INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 5 ISSUE 4 (2019) PAGES 4439 - 4441
RECEIVED : 12.06.2019 PUBLISHED : 16.07.2019

July 16,2019

WEARABLE SENSOR USING HUMAN GAIT MOTION DETECTION FAR AND EER IN ANDROID

[1]Harini. S, M.Phil, Research Scholar, K.M.G College Of Arts & Science, Gudiyattam.

[2]Prof.P.Anjugam, Assistant Professor, Pg & Research Department Of Computer Science & Applications, K.M.G College Of Arts & Science, Gudiyattam.

Abstract:

Biometric systems designed on wearable technology have substantial differences from traditional biometric systems. Due to their wearable nature, they generally capture noisier signals and can only be trained with signals belonging to the device user (biometric verification). In this article, we assess the feasibility of using low-cost wearable sensors—photoplethysmogram (PPG), electrocardiogram (ECG), accelerometer (ACC), and galvanic skin response (GSR)—for biometric verification. We present a prototype, built with low-cost wearable sensors, that was used to capture data from 25 subjects while seated (at resting state), walking, and seated (after a gentle stroll). We used this data to evaluate how the different combinations of signals affected the biometric verification process. Our results showed that the low-cost sensors currently being embedded in many fitness bands and smart-watches can be combined to enable biometric verification. We report and compare the results obtained by all tested configurations.

Keywords: biometrics; verification; low-cost sensors; wearables; electrocardiogram; photoplethysmogram; accelerometer.

1. INTRODUCTION

Authentication systems verify the identity of a machine or person to provide access to different services (banking, email, etc.). In general terms, an authentication system uses one or multiple factors, which can be categorised as “something you know” (i.e., passwords), “something you have” (i.e., security tokens), or “something you are” (i.e., biometrics). This is known as the authentication triad. Personal identification numbers (PINs) and passwords are routinely used to access computer systems, electronic locks, and all types of on-line accounts. Although they are probably the most widely used authentication factor, choosing good passwords is not a simple task However, their main advantage is also their main weakness—they are physical objects that can be lost, with the attendant effect of disrupting access to services. Biometric systems rely on physiological or behavioural characteristics that can be measured by a sensor and used to identify an individual. In contrast to passwords and security tokens, a biometric trait like a fingerprint or iris scan does not need to be remembered, and always goes with the user. In the last few years, wearable devices have proliferated and found wide adoption among the general population. According to some estimates, wearable sales will rise to 100 million units by . Because they are equipped with relatively cheap sensors, they capture noisier signals. In addition, due to their wearable nature, they can only be trained with data from the device user. These two issues hinder data collection in such a way that to-date, most proposals in the wearable area that use health-related signals have been developed relying on datasets captured with medical-grade equipment.

2. RELATED WORK

The EER reflects the point in the receiver operating characteristic (ROC) curve where the false positive and false negative rates are equal. Because of this, the EER is accepted as a good estimator of the quality of a biometric system. However, using the EER as a single quality metric can lead to two problems. First, it does not provide meaningful information about how the FPR and FNR may change when varying the threshold around that point (as a ROC curve does).

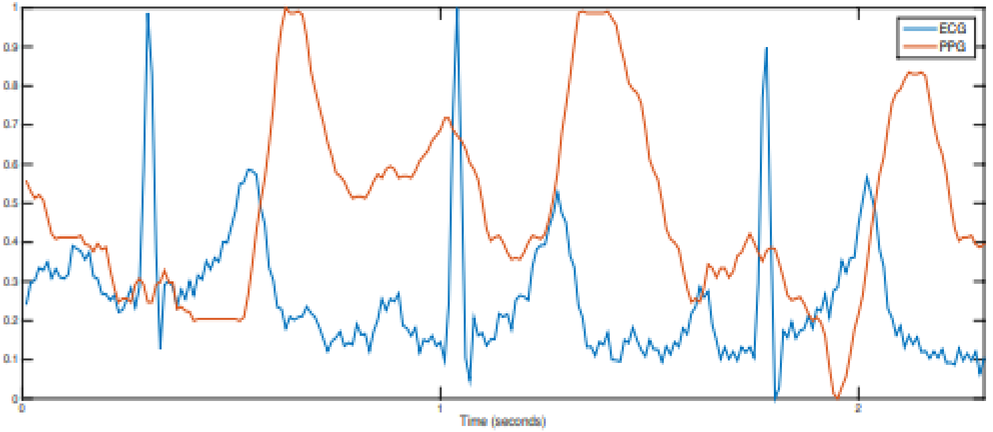

Fig.1.

For all the participants, the device was placed on their wrist, as in most fitness trackers. The PPG sensor was placed on the inner side of the wristband. One of the ECG electrodes was placed on the inner side of the wristband, while the second was placed on top of the wristband. The GSR electrodes were placed on the lower region of the palm of the hand. The accelerometer was attached to the microcontroller unit (MCU), also provided by Bitalino, where all sensors were connected. The MCU was subsequently connected to a Bluetooth block, allowing for real-time transmission of synchronised data to a smartphone. We applied the same preprocessing for cardiac (i.e., ECG and PPG) and accelerometer signals. First, the DC component is eliminated. Then, a band-pass filter is used, mainly to remove the power line noise. The lower and upper cut-off frequencies were set to 0.67 and 45 Hz, respectively. This removes the noise caused by the respiration of the subject (i.e., 0.67 Hz) and the power line noise (i.e., 45 Hz). We found the same filter to also be useful when removing noise from the ACC signal, as most of the information resides in the lower frequencies (20 Hz). Due to its simplicity, we only apply smoothing to the GSR signal.

3. ANALYSIS

The worst results were obtained in Scenarios 1b and 2, with the accelerometer (EER = 0.1071) and when training and testing on different participant states (EER = 0.0794). The variability introduced by the five-minute walk increased the average EER by 0.06, matching the results in [15]. Da Silva et al. observed an increase in the EER of 0.08 when the ECG measures were taken four months apart. These results lead us to believe that using a single user state for training is not the best strategy for ECG-based systems. To complete and generalise the dataset, as future work, users may be recorded on different days (preferably repeating it over a long period of time) for the proposed set of scenarios. In turn, for each scenario, subjects may be under different situations (relaxation, stress, fear, etc.) and places (indoor or outdoor). The set of scenarios could also be made larger by expanding the number of activities (e.g., running, cycling, or driving) that users execute during the data acquisition. In addition, another aspect to analyse in depth is related to when and how often the user credentials are validated. In the proposed system, regular time intervals were used. As a future work, credentials could also be evaluated continuously. This is the gap between a classical identification system and a continuous identification system. Data stream mining techniques may be used for this purpose. These types of systems are promising since they can cope with the concept of drift (slight variations over time), as these commonly occur in biosignals.

CONCLUSION

In this work, we analysed the feasibility of using low-cost wearable sensors to build a multi-modal biometric system to perform user verification. Our results showed that the implementation of such systems in a realistic setting is feasible, but several challenges must be considered. First, low-cost sensors that are being worn continuously by the user are subject to movement-generated noise that can reduce the quality of the captured signal. This could be mitigated by a proper fit of the device that limits its movement. Second, signals like ECG, PPG, and GSR vary over time because of changes in the user state or ageing. To avoid false negatives under these circumstances, a biometric system should allow the addition of new samples over time to keep the biometric system under acceptable metrics.

REFERENCES

1. Chiasson, S.; van Oorschot, P.C.; Biddle, R. A Usability Study and Critique of Two Password Managers. In Proceedings of the 15th conference on USENIX Security Symposium, Vancouver, BC, Canada, 31 July–4 August 2006; Volume 6, pp. 1–16.

2. Florencio, D.; Herley, C. A Large-scale Study of Web Password Habits. In Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada, 8–12 May 2007; ACM: New York, NY, USA, 2007; pp. 657–666.

3. Srinivas, S.; Balfanz, D.; Tiffany, E. FIDO Universal 2nd Factor (U2F) Overview. Available online: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/FIDO-U2F-COMPLETE-v1.2-ps-20170411.pdf (accessed on 15 August 2018).

4. Lee, P.; Stewart, D.; Barker, J. Deloitte TMT Predictions 2014; Technical Report; Deloitte: New York, NY, USA, 2014.

5. Hill, C. Wearables—The future of biometric technology? Biom. Technol. Today 2015, 2015, 5–9.