The Impact of Segmentation and Overlapping in Biometric Human Authentication Systems

Author: Carla Andrea Varela Rosa
Advisor: Jeffrey L. Duffany
Department of Electrical & Computer Engineering and Computer Science (ECECS)

Abstract

One of the arduous challenges in Machine Learning is how to extract features with enough information that will simplify the learning process of classification models; therefore, leading to better predictions and human interpretations. We investigated the impact of segmentation and overlapping techniques used to extract features from accelerometer data to optimize the performance of Machine Learning models designed for Biometric User Authentication via walking patterns. Results showed that bigger segmentations were beneficial to the individual performance of the features and detrimental for systems fed with a set of features. Also, there was no evidence found supporting the increase in the overall performance of the system by using the method of overlapping. Finally, via a brute-force feature selection algorithm, we achieved a 71% classification accuracy (with 10/34 features) vs. 64% (with 34 features), regardless of the system's configuration meaning that key features hold more weight than mere segmentation and overlapping methods.

Introduction

Accelerometer data help in detecting changes in gravitational acceleration to determine stabilization, vibration and device orientation for several applications. In addition, accelerometers are one of the most widely used sensors on embedded devices and the most frequently accessed from applications. Research has shown how accelerometer data is enough to predict biological traits of the device's holder [1]; these findings open the door to many researchers in the pursuit of real-world applicability on cybersecurity systems. The goal of this project is to use tri-axial accelerometer data for Human Authentication by exploring the value of overlapping and windowing techniques for feature extraction. The results of this project will help to characterize the tradeoff between feature extraction methods and the performance of accelerometer-based systems.

Background

The topic of unobtrusive Biometric User Authentication is latent nowadays. Many researchers focus on the placement of the sensors [2], the selection of the best supervised learning method [3] or the improvement of the classification accuracy of the model [4]; frequently ignoring the feature extraction process and the selection of key features. This project is motivated by a publication at the 23rd International Conference on Artificial Intelligence called "Feature Optimization in Machine Learning" [5] where the authors addressed the issue of effective feature selection.

Problem

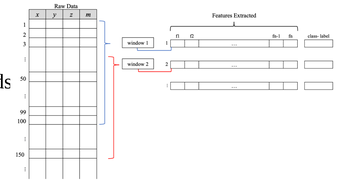
Banos et. al [6] claims that signal segmentation has been seldom and vaguely characterized. Many designs rely on datasets with features already extracted or on segmentation methods from previous works with little to no data to endorse their strategy. The goal of this project is to help characterize the tradeoff between signal segmentation methods and a system's performance.

Methodology

This research project attempted to characterize the tradeoff between segmentation/overlapping and performance accuracy of Biometric Human Authentication Systems. This was accomplished by:

1. Identifying a machine learning dataset from the UCI Machine Learning Repository that contained tri-axial accelerometer data, in the form of a time-series, of several subjects walking for a certain period.
2. Creating new datasets by segmenting the raw data into partitions (windows) of fixed size and using different overlapping percentages (process described on Figure 1).

Figure 1. Sample windowing and overlapping methods



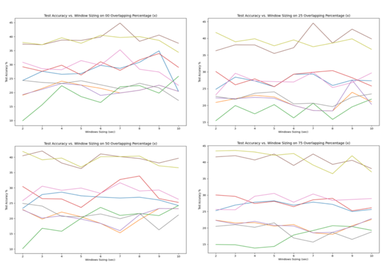
3. Exploring the impact of segmentation and overlapping on individual features extracted from the accelerometer data by creating numerous classification models via a K-Neighbors Classifier.
4. Ranking the features by their individual ability to authenticate the subjects based on their walking patterns.
5. Comparing the average feature performance of the features extracted by different configurations.
6. Comparing the performance of classification models created with all the features extracted by different configurations.
7. Comparing the performance of classification models created with a feature selection of the features extracted by different configurations.
8. Creating visualizations for the analysis of the results.

Results and Discussion (cont.)

From the three axis of the acceleration and the magnitude the following features were extracted by varying the window size [2-10sec.] and the overlapping percentages (0%, 25%, 50%, 75%): max, mean, median, min, negative count, peak count, positive count, standard deviation and variance.

Figure 2 shows the individual performance of the features extracted with different configurations of window sizes and overlapping percentages over the acceleration over the x axis. This showed how there's not a patterned behavior from overlapping and segmentation choices, the same happened for the other signals.

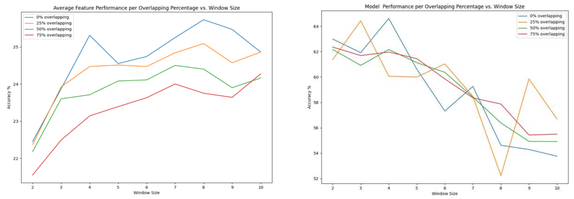
Figure 2. Individual feature performance from x-acceleration signal over various overlapping percentages



Results and Discussion (cont.)

An analysis of the top 10 ranked features (from all the combinations of window sizes and overlapping percentages) showed how the higher-ranking features were extracted from the x and the z axis. In addition, the following features ranked in the top 10 for all choices of window sizes and overlapping percentages: x_mean, x_median, y_mean, z_mean, and z_median followed by: z_pos_count, z_neg_count, x_pos_count, x_min, x_neg_count and z_min. According to the results, the mean, and the median of the acceleration contains more information about the user's walking pattern than any other of the features extracted.

Figure 3 (a) shows the average feature performance; for individual features, results showed how no overlapping and bigger windows size with 0% of overlapping were beneficial for the authentication of the subjects. On the other hand, Figure 3 (b) shows the collective feature performance with the 34 features extracted; results showed that in this case, smaller windows benefited the performance of the systems.



(a) (b)

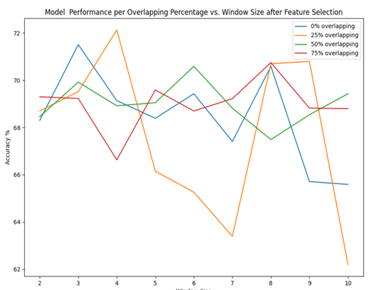
Figure 3. (a) Average feature performance, (b) Collective feature performance

Figure 4 contains the results of the models' performances after the feature selection method proposed in (Duffany, & Varela, 2021). We can see how the different overlapping percentages performed similarly except for the 25% whose plot behaves erratically meaning that it should not be considered as a design option.

In terms of the window size, with a reduced number of features there's not much change in the accuracy of classification of the models, implying that there's more weight in the quality of the features extracted than in the segmentation and overlapping configuration selected.

Lastly, after features were selected, we were able to improve the classification accuracy of the models from approximately 64% of accuracy (with 34 features) to approximately 71% of accuracy (with 10 features).

Figure 4. Comparison of model performance after feature selection



Conclusions

We explored the tradeoff between segmentation/overlapping, and the performance of Biometric Human Authentication systems based on accelerometer data. Results showed how bigger segmentations resulted in a better performance of individual features, yet detrimental for the set of the 34 features. In addition, there's not enough evidence to support the extra computation for the overlapping of windows. Finally, results showed how key features have more value in the classification performance of the systems than segmentation and overlapping. With these results, we hope to help characterize the tradeoff that exists in Biometric Human Authentication systems and to support future systems designers by providing some basis to their design choices.

Future Work

Future work can focus their efforts into investigating the impact of segmentation in smaller windows applied to other field of study, developing cleaner datasets with higher sample frequencies and more transparent positioning of the accelerometer sensor, comparing the results of this project with other classification algorithms, and/or extracting features in the frequency domain and exploring the impact of segmentation.

Acknowledgements

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) under contract/award #1563978, the National Security Agency under contract/grant number: H98230-20-1-0411, the Applied Computer Security Associates (ACSA), and the Committee on Widening Participation in Computing Research (CRA-WP) through the Scholarship for Women Studying Information Security 2021 (SWSIS).

References

[1] Kröger, Jacob & Raschke, Philip & Bhuiyan, Towhidur, "Privacy Implications of Accelerometer Data: A Review of Possible Inferences", *3rd International Conference on Cryptography, Security and Privacy*, 81-87, 2019.
[2] Cleland, I., Kikhia, B., Nugent, C., Boytsov, A., Hallberg, J., Synnes, K., … Finlay, D., "Optimal Placement of Accelerometers for the Detection of Everyday Activities", *Sensors*, 13(7), 9183–9200, 2019.
[3] Casale, Pierluigi & Pujol, Oriol & Radeva, Petia, "Personalization and user verification in wearable systems using biometric walking patterns", *Personal and Ubiquitous Computing - PUC*. 16. 1-18, 2012.
[4] Singha, Thingom & Nath, Rajsekhar & Narsimhadhan, A. "Person Recognition using Smartphones' Accelerometer Data", 2017.
[5] Duffany, J., Varela, C., "Feature Optimization for Machine Learning", *The 23rd International Conference on Artificial Intelligence*, 2021.
[6] Banos, O., Galvez, J. M., Damas, M., Pomares, H., & Rojas, I., "Window size impact in human activity recognition", *Sensors* (Basel, Switzerland), 14(4), 6474–6499, 2014.