Analysis of Smartphone Sensor Data for Continuous Biometric Authentication

Shahir Ghani

Rutgers University
sag315@scarletmail.rutgers.edu

December 20, 2022

Abstract

Previously there has been work done to continuously authenticate smartphone users using sensor data. The initial Hand Movement, Orientation, and Grasp paper introduced a set of behavioral features to continuously authenticate smartphone users. In this paper I look to analyze how Orientation data plays a part in the classification of users.

I. Introduction

Smartphones have become an integral part of society as we see that everyone around us has them and is constantly interacting with them. Smartphones have become a tool to store and interact with information about a user which includes their passwords, photos, social networks, and banking tools. These are sensitive pieces of information that need to be adequately secured.

The current state of smartphone authentication primarily uses facial recognition and fingerprint scans as primary methods, with PINS and passwords being secondary if the out bio-metric scans fail. One of the main issues with these forms of authentication is that they are susceptible to attacks in various forms. Additionally, these are only one-time forms of authentication that once bypassed give the user full access to the device or inconvenience the user by asking for authentication again. For example, within the iOS operating system if you were to go under the Recently Deleted Photos album it prompts for authentication again. In order to address this problem we look into continuous authentication using sensor data from the smartphone.

Regarding the logistics of continuous smartphone authentication, it follows a would follow a similar process as that of reCAPTCHA v3. reCAPTCHA v3 is the latest version in bot detection in which the algorithm returns a score for the user with no user friction. The algorithm runs in the background and gives a score based on how a user is interacting with the site. If the user is deemed abusive then the site owners can set up appropriate actions to respond. Similarly, setting something similar for smartphone authentication is what I plan to look into.

II. Related Work

Introduction of Hand Movement, Orientation and Grasp (HMOG). The HMOG paper was published in 2016 and introduced a set of behavioral feature to continuously authenticate smartphone users [1]. In this paper they evaluated authentication and biometric key generation on the HMOG features. They also performed analysis of the energy consumption in extracting the features from the smartphone and the computation. From this paper they were able to achieve 8.53% authentication EER while walking and 11.41% [1].

Biometric-based continuous authentication scheme with HMM prehensile movements

modeling. This was a paper that built on the existing work discussed in the HMOG paper and it was published in September of 2020. This paper looked into how gravity data impacted the authentication scheme. The movements were modeled through a Hidden Markov Model-Universal Background Model (HMM-UBM) with continuous observations based on Gaussian Mixture Model (GMM) [2].

III. Problem Statement

I look to analyze three main questions as a part of this paper. Can we continuously authenticate a user using sensors built into the smartphone? What sensors do we need in order to successfully authenticate a user and which sensors provide the most information? Lastly, I plan to look at if device orientation plays an important role in identifying a user.

IV. Data Description

For this project, I will be looking at data from three main sources. The first of which is the Hand Movement, Orientation and Grasp (HMOG) Dataset. The second is the Presensile Movement Dataset. Lastly, data collected will also be analyzed

i. HMOG Dataset

HMOG at the time it was published was presented as a new set of behavioral biometric features for continuous authentication of smartphone users [1]. HMOG used accelerometer, gyroscope and magnetometer readings captured from the smartphone, as well as raw touch data. Touch data included touch gestures, key presses, and key release latencies. In order to collect touch and key presses a virtual keyboard was required due to the smartphone operating system's security limitations. The sensor data was collected with a sampling rate of 100 Hz. The data that was collected was from 100 smartphone users (53 male, 47 female). This data was collected during eight text typing sessions. Four of these sessions had the user sitting, and the other four had the user walking in a controlled environment.

ii. Prehensile Movement Dataset

The second dataset is the Prehensile Movement Dataset [2]. It contains data from multiple 3-dimensional inertial sensors of the smartphone. These sensors include the accelerometer, gyroscope, and gravity sensor. The data was collected from seven volunteers aged 19 to 56 with an Android smartphone (Sony Xperia P). The users had no predefined tasks to perform in order to represent natural user behavior.

iii. Data Collection

Moving on to the data that was collected as a part of this project. The data that was collected included accelerometer, gyroscope, gravity, and orientation data. Orientation data included the pitch, roll, and yaw of the smartphone as shown in Figure 1.

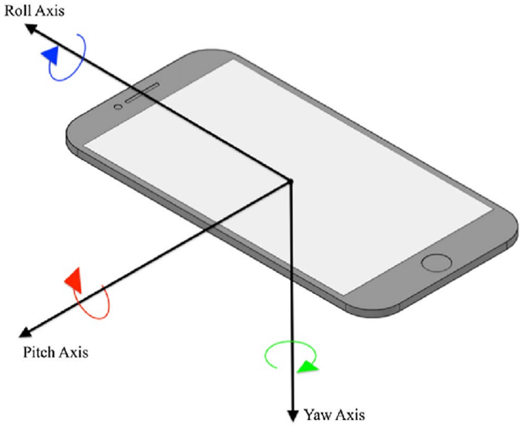

Figure 1: *Orientation Axes of Smartphone*

The data was collected using the Sensor Logger smartphone app available on Android and iOS. The sampling rate can be adjusted for the various sensors. For this project, the sampling rate was set to 100 Hz. The app allows for a user to export the data or send it via HTTP requests. For this project that data was exported directly from the phone. The data comes in a zip file which contains a CSV file for each sensor. The data collection process is to have a user casually interact with common social media and messaging apps. Users were primarily stationary but were free to adjust their posture and position as they would with normal usage. Figure 2 and Figure 3 show sample data that was collected using the sensor logger app. These plots were not from the app it self, but they were generated using matplotlib.

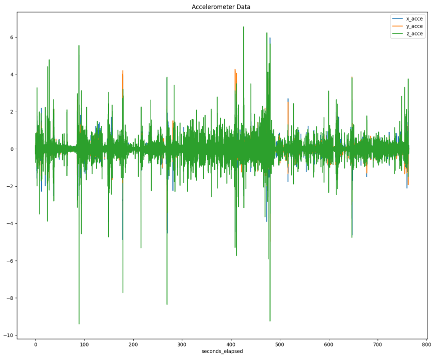

Figure 2: *Accelerometer Data From Sensor Logger App*

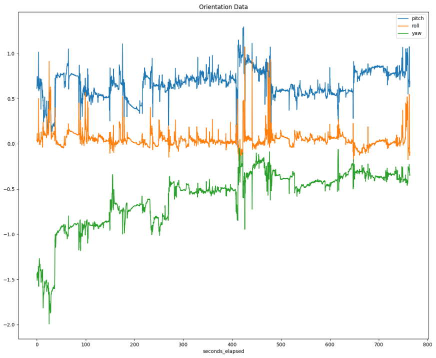

Figure 3: *Orientation Data from Sensor Logger App*

V. Methodology

There will be two main points covered in the methodology which include the data exploration for the collected data and the training and testing models to compare with the existing data and work that has been completed.

i. Feature Extraction and Data Exploration

As mentioned above regarding the data that was collected, the data from each sensor was split into different CSV files. The first step was to combine these into a single data frame and make sure all the timestamps corresponded correctly. Since all the data was collected from one application and the sampling rate was set to 100 Hz for all the sensors, there was no need for any interpolation. This was done for each of the different user's data. All of the different user data was then compiled into one data frame with a column to indicate which user the row corresponded to. Since there is still limited data collected I will be looking at data from three different users. Moving on to PCA. The data was first preprocessed using the StandardScalar from the sklearn preprocessing library. With all of the sensor data, there was a total of 16 different components so PCA was initially run with 16 different components to measure how much of the feature space was covered by each component. This is done by looking at the explained variance for each component. Then the top two and top three components are plotted in order to visualize the component space and see if there are any patterns that can be observed. These PCA plots are created for comparisons between different users as well to compare the smartphone usage patterns between different users.

ii. Training and Testing Models

In order to evaluate the performance of the authentication accuracy using the datasets and collected data I used a convolutional neural network to process the data. The plan is to compare results accuracy results from the different datasets to determine which sensors provide the best results. The first step was to collect the HMOG data. For this neural network, the touch data was excluded since it is not a feasible data source for practical implementations. The data set was then split into training and testing data. The training set included 102,000 samples and the testing set contained 25,000 samples. For the prehensile movement data there was a total of approximately 50,000 samples which was split into training and testing sets based on the user id.

VI. Results

For the results I will first look at the results from feature extraction using PCA. Then I will cover the results from the neural network model and cover some of the issues that came up .

i. Feature Extraction Results

For PCA I will first look at the explained variance table and the elbow plot. The elbow plot in Figure 4 shows the show much of the feature space is covered by the number of components that are chosen when performing PCA. From Table 1 we can see that six components accounts for 90% of the feature space and seven components results in almost 95% of the feature space covered.

Table 1: *Explained Variance*

Components	Percent
1	52.56%
2	61.69%
3	70.32%
4	77.64%
5	84.34%
6	90.12%
7	94.75%
9	99.32%
15	100%

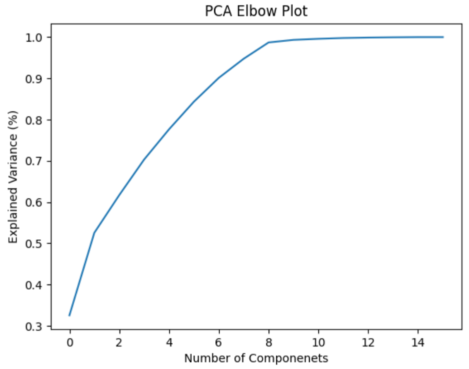

Figure 4: *Elbow Plot for PCA with 16 Components*

After calculating how much of the feature space is covered by each component we then look at the PCA plots for the first two components and then the first three components. These results can be found in Figure 5 and Figure 6. From these two plots we can see a clear separation of the two users across the first principal components axis. There is some overlap

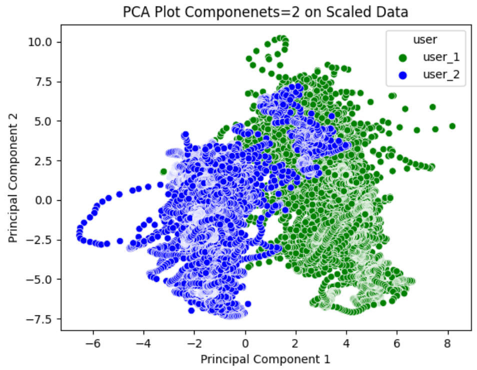

Figure 5: *PCA plot for first two Principal Components*

When comparing the PCA plots between users one and three as well as users two and three similar results were generated.

ii. Model Evaluation

Moving on to the results from the neural network. The initial results for the HMOG dataset being inputted was extremely promising. The network was yielding 80% validation accuracy

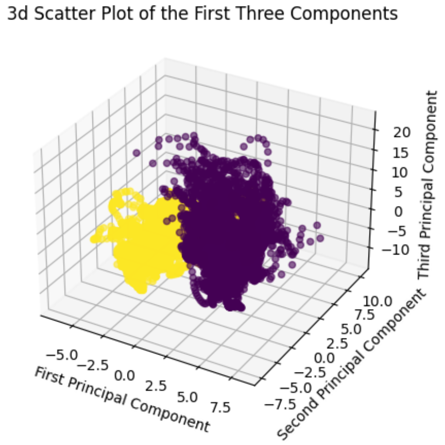

Figure 6: *3d PCA Scatter Plot for first Three Principal Components*

after around 12 epochs as shown in Figure 7 and in Figure 8 we can see the training and validation loss across the epochs.

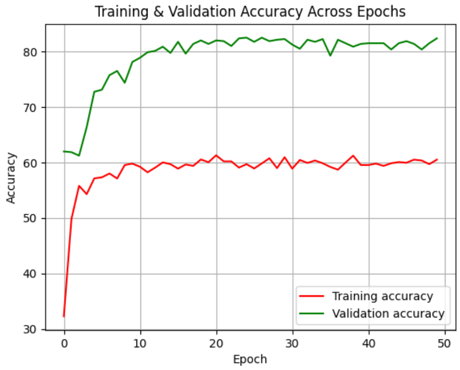

Figure 7: *Training and Validation Accuracy for HMOG Dataset Sample*

However, when moving onto the prehensile movement dataset the accuracy of the model dropped significantly as shown in Figure 9. This can possibly be because there were not as many different users in the prehensile movement dataset. The HMOG dataset contained sample from over 100 different users, but the prehensile movement dataset only had samples from seven different users.

In order to run the model on the data that I collected with orientation data, many more user samples would need to be collected. As of right now there is not enough data to make an appropriate decision on the impact of the orientation data.

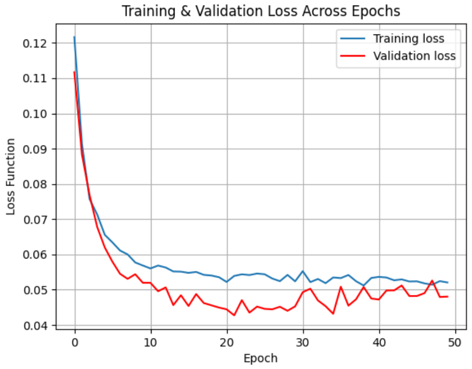

Figure 8: *Training and Validation Loss for HMOG Dataset Sample*

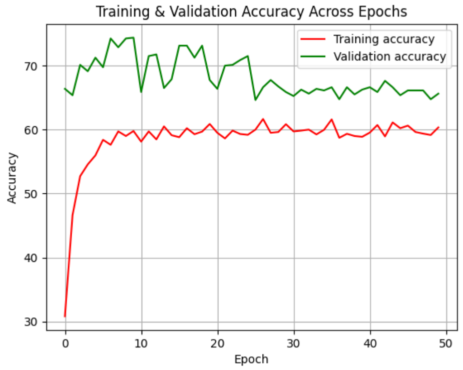

Figure 9: *Training and Validation Accuracy for Prehensile Dataset*

VII. Future Work

One of the main challenges that was faced throughout this project was the limited data. Collecting additional data would allow for better neural network performance since the networks do not perform that well with limited data as talked about previously. The plan would be to set up an HTTP server to receive data from the sensor logger application. This would allow for the data to be more easily collected instead of manually extracting it from each user. All the user would have to do is enter the address of the server and start the recording in order for the data to be collected.

Another avenue to look at would be data filtering and cleaning. A lot of this sensor data is extremely noisy so filtering this data should in theory increase the performance of the networks.

I had also wanted to look into computing the Matrix Profile for the sensor data that was collected from the smartphone to explore what motifs and discords appear. However, time was a limiting factor and this was put to the side, but it is an extremely interesting avenue to possibly explore common habits in smartphone usage.

The end goal of this work would be to have the real-time sensor data streamed to a server that calculates a score for the user. This score would then be sent back to a smartphone application and could be used to perform checks on the user. For Example, if the user were to fail it could prompt the user to input their password again. However, this would need to be tuned properly which is where False Accept Rate and False Reject Rates come into play. False Acceptance Rate is the percentage of identification instances in which unauthorised persons are incorrectly accepted. False Rejection Rate is the percentage of identification instances in which authorised persons are incorrectly rejected. If you try to reduce the FAR to the lowest possible level, the FRR is likely to rise sharply. In other words, the more secure your access control, the less convenient it will be, as users are falsely rejected by the system[3].

VIII. Conclusion

From the results shown in we can see that the initial results are promising. When comparing the two users there was a clear separation across the first principle component axis when performing PCA. This indicates a significant difference in the smartphone usage patterns between the users that the data was collected from. Additionally, this bodes well for future work when there is more data collected. Once more data is collected a proper model can be for the evaluation of the continuous authentication scheme using smartphone sensor data. The current model shows promising results on the HMOG dataset which included largest sample of users.

References

[1] Zdeňka Sitová, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, Kiran S. Balagani. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. In IEEE Transactions on Information Forensics and Security, vol.11, no.5, pp.877-892, May 2016. DOI: 10.1109/TIFS.2015.2506542

[2] Feriel Cherifi, Mawloud Omar, Kamal Amroun. An efficient biometricbased continuous authentication scheme with HMM prehensile movements modeling. Journal of information security and applications, 2021, 57, pp.102739. ff10.1016/j.jisa.2020.102739ff. ffhal-03091925

[3] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. 2017. Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). Association for Computing Machinery, New York, NY, USA, 386–399. https://doi.org/10.1145/3052973.3053032

[4] Natalia Neverova, Christian Wolf, Lacey Griffin, Lex Fridman, Deepak Chandra, et al.. Learning Human Identity from Motion Patterns. IEEE Access, 2016, 4, pp.1810-1820. ⟨10.1109/ACCESS.2016.2557846⟩. ⟨hal-01281946⟩