Analysis of Head and Torso movements for Authentication

Gayathri Manogna Parimi
Syracuse University
Syracuse, USA
gparimi@syr.edu

Partha Pratim Kundu
Nanyang Technological University
Singapore, Singapore
partha@ntu.edu.sg

Vir V. Phoha
Syracuse University
Syracuse, USA
vvphoha@syr.edu

Abstract

Wearable computing devices have become increasingly popular and while these devices promise to improve our lives, they come with new challenges. One such device is the Google Glass from which data can be stolen easily as the touch gestures can be intercepted from a head-mounted device. This paper focuses on analyzing and combining two behavioral metrics, namely, head movement (captured through glass) and torso movement (captured through smartphone) to build a continuous authentication system that can be used on Google Glass alone or by pairing it with a smartphone. We performed a correlation analysis among the features on these two metrics and found that very little correlation exists between the features extracted from head and torso movements in most scenarios (set of activities). This led us to combine the two metrics to perform authentication. We built an authentication system using these metrics and compared the performance among different scenarios. We got EER less than 6% when authenticating a user using only the head movements in one scenario whereas the EER is less than 5% when authenticating a user using both head and torso movements in general.

1. Introduction

People often carry multiple devices such as smartphones and smartwatches to access different applications and personal data and most wearable devices in the market have different sensors that can be used to capture behavioral metrics of a user [1]. Google Glass (GG) is one such device gaining prominence as a light-weight head mounted device [2]. This paper focuses on authenticating a user to improve the security of GG by analyzing the accelerometer and gyroscope data from glass and smartphones.

2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)
978-1-5386-2248-3/18/$31.00 © 2018 IEEE

Google Glass is a wearable device, worn on the head like normal glasses, with a small display near the eye in the wearer's line of vision. However, being a head mounted device, it is easily prone to thefts; for example, passwords can be easily intercepted, and device can be stolen easily [1]. The voice commands used for unlocking the glass can also be easily overheard. The other authentication mechanism for the glass is either a PIN or Password given using swipe and tap gestures, which can be easily observed for a head mount device [3]. This calls for better security measures in GG. A continuous authentication on GG will provide one such better authentication mechanism.

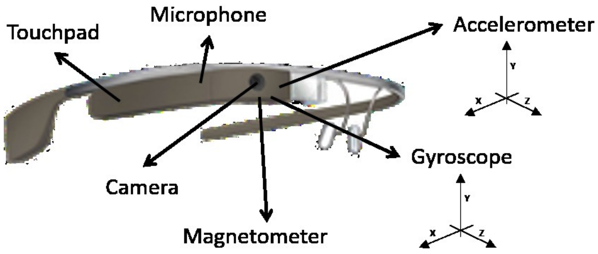


Figure 1: Google Glass (GG) with the location of some of the main sensors

A relevant question is, why 'continuous' authentication on GG? GG is used only by pairing it with an email account or with a smartphone. This makes the user's data more vulnerable, as losing account information to an imposter or the login information of the paired smartphone compromises the GG and vice versa. So, a continuous authentication mechanism will add an additional layer of security to prevent an imposter from accessing sensitive information on GG. Also, continuous authentication helps users have a higher level of security on GG as they need not depend on voice commands or touch gestures to unlock the device.

Being a head mount device, glass provides an opportunity to capture head movements using the sensors on the GG [4]; some of the sensors locations on GG are shown in Figure 1. This gives us an opportunity to compare head movements with the torso movements captured by smartphones [5]. In this paper, we consider Linear Accelerometer- we will refer it as Accelerometer in rest of the paper - and Gyroscope data captured in GG and a smartphone. Our main contributions are as follows:

- We perform a correlation analysis of the head and torso movements captured through GG and smartphone respectively. The analysis shows that there are very few feature pairs between the head and torso movements with a correlation coefficient above 0.3 and a p-value < 0.001. These results motivated us to use a combination of head and torso movements to authenticate a user.
- We propose a continuous authentication system on GG for generic scenarios. Authentication performances are shown for a different set of activity scenarios using state-of-the-art classifiers. Our results show that the EER is less than 6% in one scenario using only the head movements and less than 5% in all the scenarios when a combination of head and torso movements are used.

The rest of the paper is organized as follows: Section 2 describes the related work; section 3 discusses our methodology in detail for both the correlation analysis and authentication system, and section 4 concludes the paper.

2. Related Work

Behavioral metrics for continuous authentication has been a challenge for researchers in computing for several years now [6, 7]. Different sensors on the wearable devices are still being explored to capture user behavior to perform authentication. These sensors include but are not limited to Accelerometer, Gyroscope, keystroke pattern, Touch, etc. [8, 9, 10, 11, 12]. Google Glass with its positioning to wear on the head gives us a different focus area to capture head movements and verify if they can be used for authentication. Since the release of Google Glass, its sensors are used in different medical applications. Some such medical applications include capturing Heart rate, Respiration rate [13], and delivering social cues to autism patients [14].

There are different applications that propose to increase the one-time authentication on Google Glass i.e., increase the PIN Password protection. PIN is not secure enough as it can be inferred through various side channels [15]. Although, such attacks can be stopped by using random PIN pad [3], they pose usability issues.

Another system for authenticating Google Glass is by Pan Chan and team is scanning a QR Code Key and storing the private key in the Glass and use it for sub-sequent scans of OTP [1]. However, the private key may be vulnerable to theft if the glass or the linked Gmail account gets compromised, as it is stored on the Google Glass itself.

There are some biometric user identification mechanisms for Google Glass using the Bone Conductance sensor and music Cues [16, 17]. The Skull Conduct system uses bone conduction of sound through the user's skull and the microphone. When sound passes through the skull the frequency generated will be unique to every user, The Skull Conductance system uses these frequencies when the user is listening to audio tracks and capture them through the microphone to record it in the glass [16]. Another biometric authentication system, which is close to our work, identifies user using the accelerometer and Gyroscope data when the user is listening to set of music cues [17]. Here, the users head movements are captured while sitting and a certain set of music cues are played to the user. The study states that each user reacts differently to the music being played and hence the sensor readings are different for each user enabling the system to identify the users. Both these systems, however, cannot be used effectively for continuous authentication as they involve playing music clips which reduces usability for the user and even consumes additional resources on the glass.

A continuous authentication using the in-built sensors will be a better form to identify the user and increase the privacy and security of the data [6]. Fusion of accelerometer and gyroscope data from different devices can be used for this purpose [18, 19, 20]. In this paper, we propose one such continuous authentication using the behavioral data collected from the Accelerometer and Gyroscope of the Google Glass and smartphone.

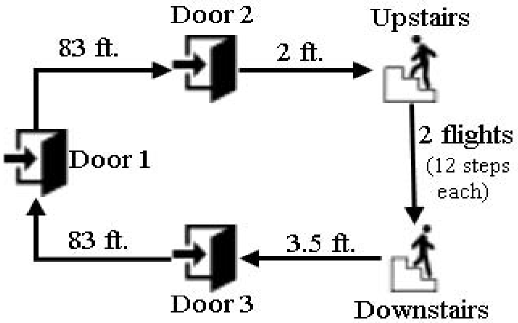


Figure 2: Series of activities performed by the users while wearing GG and carrying the SF and SB

3. Methodology

In our approach, we leverage the Accelerometer and Gyroscope sensors in the GG and on two smartphones, one placed in the participant's front trouser pocket (SF) and one placed in the participant's back trouser pocket (SB), to collect data from users while they are performing activities mentioned in Figure 2. The two smartphones are used to make the system independent of the placement of the phone. As the Accelerometer and Gyroscope are running on the devices continuously, this approach does not use any additional resources, which is an advantage in GG as it has limited resources.

We use multiple devices for our experiment and consider the following combinations for analyzing data and to authenticate the user.

1. data from Only GG
2. combining the data from GG with SF
3. combining the data from GG with SB

We perform a correlation analysis for the above combinations to see whether there exists a correlation between the head and torso movements captured by GG and smartphones (SF and SB) respectively. Both the correlation analysis and authentication are performed on all the activities and a subset of activities.

Scenarios	**Mean**	**Std.**
#1 All activities	97.89	12.74
#2 Climbing up and down Stairs	36.42	14.58
#3 Activities with no stairs	61.47	20.43

Table 1: Average mean and standard deviation of time taken to perform the activities (in seconds)

3.1. Experiment Design

We designed the experiment considering that users may place their phones either in the front pocket or back pocket. To satisfy this requirement, we used two smartphones along with one GG for collecting data. The activities mentioned in Figure 2 are designed to represent the general walking patterns of a user.

3.2. Data Collection

We collected data from 17 participants, after obtaining approval from the Institutional Review Board (IRB). After the volunteers were explained the experiment, they were asked to walk at their usual pace. The data was collected in two sessions for each participant; one session for training and one session for testing. These sessions were spread across 28 days, depending on the availability of the participants.

Each participant walked for 85-120 seconds, depending on their pace, performing a series of activities in the same sequence: - opening a door, walking on a flat surface for 83 feet, opening another door, climbing up 2 flights of stairs with 12 steps per flight, climbing down the same 2 flights of stairs with 12 steps per flight, then opening another door and walking on a flat surface for 83 feet (Figure 2). Participants performed two types of activities: 1) walking on flat surface with door opening i.e., activities with no stairs 2) climbing up and down stairs. Distance covered and average time consumed by each of the activities are mentioned in Figure 2 and Table 1 respectively. The activities were same for training and testing sessions.

We developed two Android applications to collect data from glass and smartphones. We used the default sensor delay for capturing the sensors' data in the GG because GG gets overheated for higher delay times and we used the fastest sensor delay for the smartphones. The sampling rate for GG is 5Hz and for smartphones it is 48Hz; this varies because of the in-built hardware settings. The camera in the GG is used to record the activity being performed to map the timing for each activity [21].

Features Extracted			
Accelerometer (1-48)		**Gyroscope (49-96)**	
1-4	Mean	49-52	Mean
5-8	Standard Deviation	53-56	Standard Deviation
9-12	Band Power	57-60	Band Power
13-16	Energy	61-64	Energy
17-20	Median Frequency	65-68	Median Frequency
21-24	IQR	69-72	IQR [22]
25-28	Range	73-76	Range
29-32	Signal to Noise Ratio	77-80	Signal to Noise Ratio
33-36	Spectral Entropy	81-84	Spectral Entropy
37-39	DTW	85-87	DTW [23]
40-45	Mutual Information	88-93	Mutual Information [24]
46-48	Correlation	94-96	Correlation [24]

Table 2: Features extracted from the accelerometer and gyroscope data for each device, GG, SF and SB

3.3. Feature Description

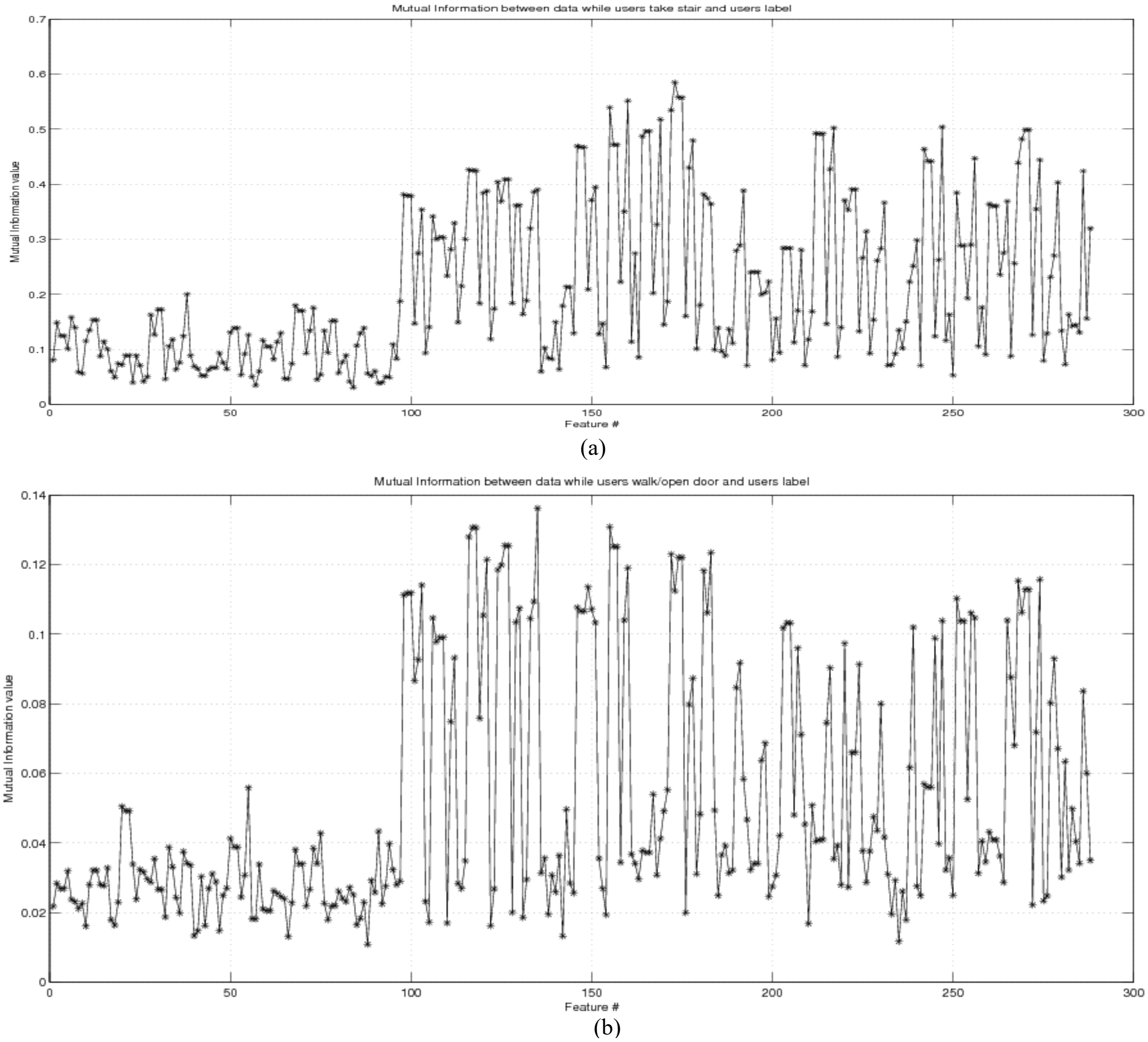
The data collected from the Accelerometer and Gyroscope have three dimensions each (X-axis, Y-axis, Z-axis). We preprocess the data by removing noise using median filtering and smoothing. We computed the magnitude (M) for the sensors and used it as a fourth dimension. We extracted 48 features using the four dimensions, each for Accelerometer and Gyroscope for all three devices, giving 96 features per device. The features were extracted with a sliding window of two seconds, with a 50% overlap between the windows, as found this time window to be the best. A detailed list of features extracted can be seen in Table 2. The description of the features is available in Appendix.

We extracted basic features like Mean and Standard Deviation; we also extracted other features like Band

Power, Mutual Information, and Spectral Entropy to get more insight into the data collected from the GG and both SF and SB. Band Power is the average power in the range of each frequencies calculated for each pair of the dimensions. We extracted the Mutual Information between the dimensions to see the change of each dimension with respect to the other. We extracted Signal to Noise ratio for each user to be able to differentiate the correlated feature pairs depending on the noise ratio. We are calculating Inter Quartile Range (IQR) to find the span of the signals from GG, SF and SB [7, 18, 19, 25].

Features #1-36 are computed using all the four dimensions (X, Y, Z, M) of the Accelerometer. These features are computed as Mean of X and Y, Mean of Y and Z, Mean of Z and M and, Mean of X and M, similarly for other features. The features #37-39 (Dynamic Time Wrapping) and #46-48 (Correlation) are computed by comparing only three X, Y, Z. Features #40-45 are computed by doing a comparison among the three dimensions (X, Y, Z) and between the X, Y, Z and M. Then we repeated the same process to extract features #49-96 from Gyroscope data. The Accelerometer and Gyroscope data are combined at feature level and then fed as inputs to the classifiers for authentication.

The Mutual Information between the features in all the three devices - GG, SF and SB - is shown in Figure 3. The x-axis of the graphs in figure 3 represent the features, the features #1-96 correspond to GG, #97-192 represent the features from SB and #193-288 represent the features from SF. The first graph represents the Mutual Information of the features for user labels while the participants are climbing up or down stairs.



(a)

(b)

Figure 3: Mutual Information among features and class labels of GG, SB and SF, X-axis: Feature # 1-96 are for GG, 97-192 are for SB and 193-288 are for SF. (a) while user is climbing up or down stairs. (b) while user is not using stairs.

The second graph in figure 3 represents the mutual Information of the features for user labels for the data collected during the activities that does not involve climbing up or down stairs.

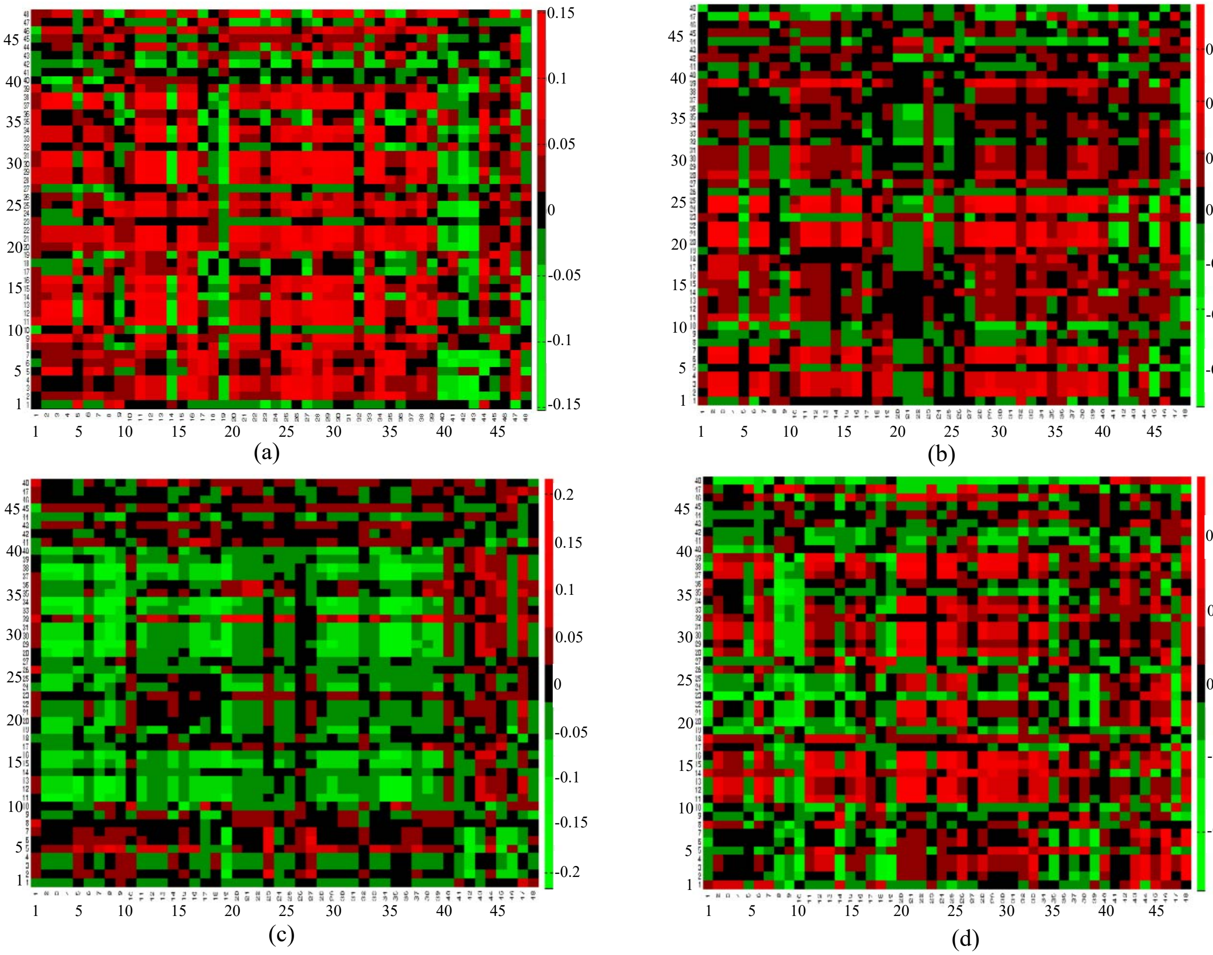
The patterns in Figure 3 indicate that the mutual information between the features of GG and the class labels is significantly less than those of SF and SB. This suggests that the features of GG alone form poorer indicators for authenticating a user. So, we proceeded to combine the features from GG, SF and SB to authenticate a user.

3.4. Correlation Analysis

We performed a correlation analysis on the training data for three combinations: correlation between Accelerometer and Gyroscope of GG; correlation between features of GG and SF; correlation between features of GG and SB. The correlation coefficient below 0.3 (absolute value) is considered as weak correlations [26].

Scenarios	CT	GG	GG with SF		GG with SB	
			Acce	Gyro	Acce	Gyro
All activities	0.15	238	1	14	2	0
	0.2	172	0	0	1	0
	0.3	97	0	0	0	0
Stairs	0.15	243	286	142	33	2
	0.2	193	207	109	3	0
	0.3	114	49	49	0	0
Activities with no stairs	0.15	723	20	0	0	0
	0.2	575	0	0	0	0
	0.3	350	0	0	0	0

Table 3: Comparison of number of feature pairs with correlation coefficient > CT and p-value < 0.001 for all activities data, data collected from climbing up and down stairs activities, data collected from activities other than climbing up and down stairs (Acce is Accelerometer, Gyro is Gyroscope)



(a)

(b)

(c)

(d)

Figure 4: Heatmap of correlation coefficient between feature pairs of (a) Accelerometer of GG and SF (b) Gyroscope of GG and SF (c) Accelerometer of GG and SB (d) Gyroscope of GG and SB

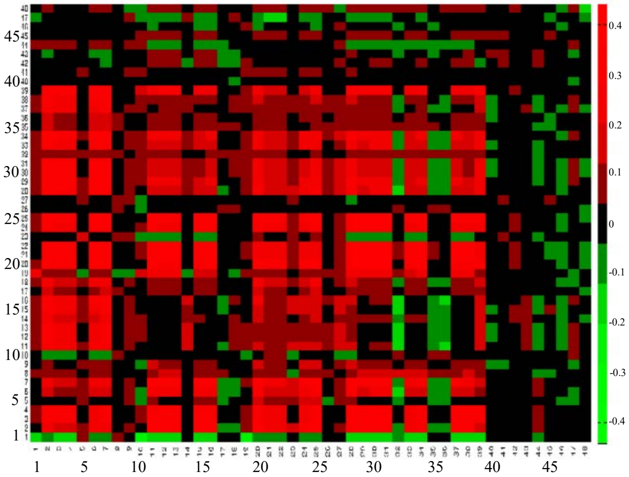


Figure 5: Heatmap of correlation coefficients between feature pairs of accelerometer and gyroscope in GG

We varied the Correlation Threshold (CT) values to check the number of correlated feature pairs. We also computed the p-values for the correlation coefficients to check their significance. Table 3 shows the number of pairs of features with a correlation coefficient > CT and with p-value < 0.001 for each CT value. The results show that the number of feature pairs with correlation > CT reduced as the CT is increased for any activity.

When all activities are considered, there are a few correlated feature pairs between GG and SF when CT=0.15 (1 feature pair for accelerometer and 14 pairs for Gyroscope) whereas there are no correlated feature pairs between GG and SF with CT >= 0.2. Similarly, for GG and SB, there are no correlated feature pairs for Gyroscope, while there are 1 and 2 correlated feature pairs for accelerometer when CT=0.2 and 0.15, respectively. However, the number of correlated feature pairs between GG and SF and, GG and SB are higher when the participant is climbing up or down stairs. The number of feature pairs that are correlated between GG and SF are higher when the users are climbing up and down the stairs but the features are very weakly correlated when the user is performing other activities or all the activities.

We found that, for GG, the accelerometer and gyroscope have more feature pairs with correlation coefficient (CC) greater than CT while there are very few correlated features between GG and SF and GG and SB for any set of activities. The heatmaps for the correlation coefficients can be seen in Figures 4 and 5. It can be seen from the heatmaps in figures 4 and 5 that the correlation between GG and SF for both Accelerometer and Gyroscope is very low, and, the correlation between GG and SB is much lower. This motivated us to use a combination of devices to perform the authentication because this provides us a safeguard against using one set of features to mimic other set of features. The intrinsic characteristics of this mechanism prevent attacks like spoof-forge-replay.

3.5. Discussion on Authentication Performance

We implemented four different classifiers, Support Vector Machine (SVM), Linear Discriminant Analysis (LDA), Logistic Regression (LR) and Random Forest (RF) for authenticating a user using publicly available R packages. We measured authentication performance on each of the scenarios discussed in Figure 2. We considered three combinations of data, as mentioned earlier, only GG, GG with SF and GG with SB, on each of these scenarios.

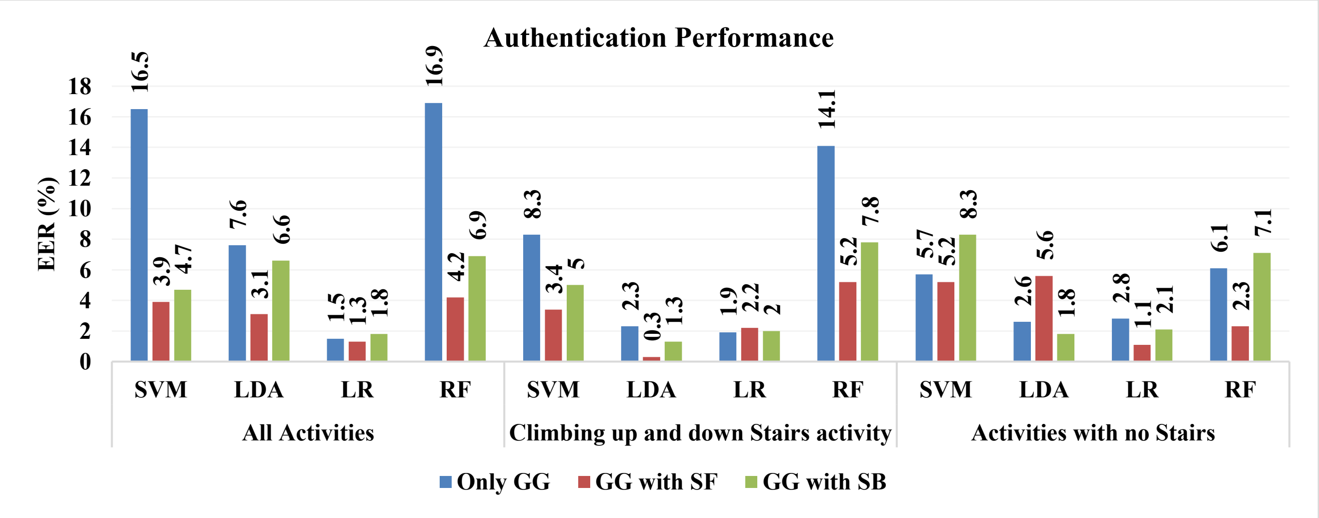


Figure 6: Authentication Performance in terms of EER (%) for combinations: only GG, GG with SF and GG with SB; for the classifiers used and different activities: including all activities, climbing up and down stairs, activities with no staircase

We used all the extracted features (refer Table 2) for each case. The performance results are shown in Figure 6. The values on top of each bar represent the percentage of EER value. For each classifier group, each bar represents the combinations in order of only GG, GG with SF and GG with SB. It can be inferred from the graph that GG with SF has a better performance compared with other combinations in most of the classifiers and scenarios. GG with SB also produced low EER value in most classifiers. GG alone performed well in scenario #3 (refer Table 1) with an EER value less than 6% for all the classifiers. The authentication performance is higher for all the activities when features of GG are combined with any of the mobile phones SF and SB in comparison with stairs and no stairs activities.

From these observations, it can be said that GG alone is sufficient to authenticate a user for scenario #3 that does not include any stairs while a combination of GG with smartphone works better in scenarios #1 and #2. So, in general, a combination of GG with smartphone (SF or SB) i.e., head and torso movements will provide a better authentication in a generic scenario.

4. Conclusion

In this paper, we are using head and torso movements using GG and two smartphones (SF and SB). The smartphones are placed in two different places, user's front pocket and back pocket of the trouser to collect the data, which gives a more generic scenario of usage of the device. We performed an analysis to check if correlations exist between these behavioral metrics. We observed from the analysis results that there exists very little correlation between these two-behavioral metrics in most scenarios. This characteristic prevents imposter to mimic one set of features using the other set. This motivated us to build an authentication system by combining these two metrics.

We performed user authentication using state-of-the-art classifiers. From the results, we observed that combination of these two-behavioral metrics successfully authenticated a user with EER value less than 5% and when the only the head movements are used, the authentication system gave an EER value less than 6% for one of the scenarios.

5. Acknowledgement

We thank the anonymous reviewers for their insightful feedback. This research was supported in part by National Science Foundation Award SaTC Number: 1527795. The second author Pratha Pratim Kundu was at Syracuse University while this work was done.

6. References

[1] P. Chan, T. Halevi and N. Memon, "Glass OTP: Secure and Convenient User Authentication on Google Glass," in *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2015.

[2] Google, "Glass," Google, [Online]. Available: https://developers.google.com/glass/.

[3] D. K. Yadav, B. Ionascu, S. V. K. Ongole, A. Roy and N. Memon, "Design and Analysis of Shoulder Surfing Resistant PIN Based Authentication Mechanisms on Google Glass," in *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2015.

[4] Google, "Google Developers, Glass, Locations and Sensors," [Online]. Available: https://developers.google.com/glass/develop/gdk/location-sensors.

[5] M. Ellamil, J. Berson, J. Wong, L. Buckley and D. S. Margulies, "One in the Dance: Musical Correlates of Group Synchrony in a Real-World Club Environment}," *PloS one,* vol. 11, p. e0164783, 2016.

[6] V. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," in *IEEE Signal Processing Magazine 33 (4), 49-61.*

[7] R. Kumar, P. Kundu, D. Shukla and V. Phoha, "Continuous Authentication via Unlabeled Phone Movement Patterns," in *IEEE International Joint Conference on Biometrics - (IJCB'17)*, 2017.

[8] R. Kumar, V. Phoha and A. Serwadda, "Continuous Authentication of Smartphone Users by Fusing Typing, Swiping, and Phone Movement Patterns," in *IEEE-BTAS*, 2016.

[9] C. Cornelius, R. Peterson, J. Skinner, R. Halter and D. Kotz, "A wearable system that knows who wears it," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services, ACM*, 2014.

[10] R. Walters, "Continuous Authentication: The future of Identity and Access Management," SVP of security products, Intermedia, 2016. [Online]. Available: http://www.networkworld.com/article/3121240/security/continuous-authentication-the-future-of-identity-and-access-management-iam.html.

[11] F. Monrose and A. D. Rubin, "Keystroke Dynamics as Biometrics for Authentication," *Future Generation computer systems,* vol. 16, 2000.

[12] I. C. Stylios, O. Thanou, I. Androulidakis and E. Zaitseva, "A Review of Continuous Authentication Using Behavioral Biometrics," in *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference. ACM, 2016*, 2016.

[13] J. Hernandez, Y. Li, J. M. Rehg and R. W. Picard, "Bioglass: Physiological parameter estimation using a head-mounted wearable device," in *EAI 4th International*

Conference on Wireless Mobile Communication and Healthcare (Mobihealth), IEEE, 2014.

[14] P. Washington, C. Voss, N. Haber, S. Tanaka, J. Daniels, C. Feinstein, T. Winograd and D. Wall, "A Wearable Social Interaction Aid for Children with Autism," in *ACM*, New York, NY, USA, 2016.

[15] D. Shukla, R. Kumar, A. Serwadda and V. Phoha, "Beware, Your Hands Reveal Your Secrets!," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications*, 2014.

[16] S. Schneegass, Y. Oualil and A. Bulling, "SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM*, 2016.

[17] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist and M. Gruteser, "Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns," in *IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE*, 2016.

[18] R. Kumar, V. Phoha and A. Jain, "Treadmill Attack on Gait-based Authentication Systems," in *IEEE-BTAS*, 2015.

[19] R. Kumar, V. Phoha and R. Raina, "Authenticating Users through their Arm Movement Patterns," in *CoRR 2016, https://arxiv.org/abs/1603.02211v1*.

[20] B. Shrestha, M. Mohamed and N. Saxena, "Walk-Unlock: Zero-Interaction Authentication Protected with Multi-Modal," in *CoRR*, 2016.

[21] U. e. r. u. G. Glass, "Rahman, Shah Atiqur; Merck, Christopher; Huang, Yuxiao; Kleinberg, Samantha," in *IEEE*, 2015.

[22] G. Upton and I. Cook, Understanding statistics, Oxford University Press, 1996.

[23] A. Akl and S. Valaee, "Accelerometer-based gesture recognition via dynamic-time warping, affinity propagation, \& compressive sensing," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, 2010.

[24] Y. Anzai, Pattern recognition and machine learning, Elsevier, 2012.

[25] J. R. Kwapisz, G. M. Weiss and S. A. Moore, "Cell phone-based biometric identification," in *IEEE-BTAS*, 2010.

[26] Calkins, "Correlation Coefficients," [Online]. Available: https://www.andrews.edu/~calkins/math/edrm611/edrm05.htm.

7. Appendix

Description for the features extracted is given in Table I.

Feature Name	Description
Mean	The mean value of x, y, z-axis and m within a time window. It constitutes 4 features.
Standard Deviation	The standard deviation within x, y, z-axis and m within a time window.
Band Power	The average power in the given frequency range (0 to Fs/2). This feature depends on the sampling frequency (Fs) of the signal.
Energy	The energy of x, y, z-axis and m within a time window.
Median Frequency	A frequency that divides the power spectrum into two regions with equal amplitude is known as the median frequency. This feature depends on the sampling frequency (Fs) of the signal.
IQR	Inter Quartile Range (IQR) is the difference between signal quarter 3 (Q_3) and quarter 1 (Q1).
Range	The difference between maximum and minimum value within x, y, z-axis and m within a time window.
Signal to Noise Ratio	Measure to compare actual signal to background Noise. Ratio of signal power to noise.
Spectral Entropy	It describes the complexity of the signal and is directly proportional to the peak of the signal power spectrum and similar to Shannon's entropy. With the use of the power spectral density as a probability density.
DTW	Dynamic Time Wrapping (DTW) distance is computed between pair of signals to find the best mapping for minimum distance.
Mutual Information	Mutual information is computed between pair of signals.
Correlation	Pearson correlation coefficient is computed between pair of signals.

Table I: Description for the features extracted.