Human-Based Fraudulent Attempts on Gait Based Profiles

Yasmeen Abdrabou
German University in Cairo
Bundeswehr University Munich
Egypt
yasmeen.abdrabou@guc.edu.eg

Omar Sherif
German University in Cairo
Egypt
omaar.sherif@gmail.com

Rana Mohamed Eisa
University of Canada in Egypt
Egypt
rana.eisa@uofcanada.edu.eg

Amr Elmougy
University of Canada in Egypt
Egypt
amr.elmougy@uofcanada.edu.eg

ABSTRACT

Recent research involves biometrics in authentication as they establish a natural way of communication. Accordingly, in this paper, we describe the implementation of an Android-based authentication application and we focus on human factor impostor attacks on gait based systems. We used the smartphone's built-in accelerometer to record gait cycles while walking. Results proved that imitating other's gait cycles is possible and can be a huge threat.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; *Usability in security and privacy*; • **Human-centered computing → HCI design and evaluation methods**;

KEYWORDS

Gait Authentication, Smartphone, Authentication, Attacks

ACM Reference Format:
Yasmeen Abdrabou, Omar Sherif, Rana Mohamed Eisa, and Amr Elmougy. 2018. Human-Based Fraudulent Attempts on Gait Based Profiles. In *2nd African Conference for Human Computer Interaction (AfriCHI '18), December 3–7, 2018, Windhoek, Namibia.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3283458.3283488

1 INTRODUCTION

Several types of authentications mechanisms have been explored in security research. The first and oldest type of authentication is knowledge-based. This is where the user has to remember a password. However, passwords are victims of several types of attacks such as shoulder surfing, video attacks [4, 9, 10], smudge attacks [2] and recently thermal attacks [1] due to the physical contact with the hardware devices. The second type is the token-based authentication. This type depends on the user owning a piece of hardware like a key or an ID. Both approaches are relatively vulnerable to hacking attempts. The last type is the biometric authentication which depends on the unique features of the body and has the highest levels of security.

Biometric-based authentication has been receiving attention over the past years for its usability, convenience and high level of security. Gait authentication is considered a type of biometric authentication. It could be implemented on smartphones without the need for any additional hardware. However, there exist many challenges concerning gait authentication. These challenges include environmental as well as internal factors, in addition to the fact that the walking patterns of many individuals can be similar. Through the past years, no one used human-based impostors attempts to attack the gait systems. Therefore the following question arises, what will happen if another user tried to imitate the gait cycle of another? Will the system still be able to differentiate between them?

Accordingly, in this paper, we investigate the human-based impostor attempts on user profiles. Where we will invite participants to watch and simulate other user's gait profiles and try to attack them using our proposed Android-based application. The application implements a gait detection and authentication system that utilizes the built-in accelerometer data as well as optimized cycle detection algorithms.

2 RELATED WORK

Using smartphones as a wearable sensor has been the study field of different experiments [6, 8, 11]. Using the accelerometer embedded in smartphones, we can read data on three axes. Forward-backward, up-and-down, and side-to-side[6]. This provides raw acceleration data on X, Y, and Z axes. Wearable Sensors describe the method of attaching sensor devices to points on an individual‘s body in order to capture gait characteristics from the motion of body parts during walking[12]. There have been numerous related experiments done in this field. Different technologies were used in detecting gait features and attempting to authenticate subjects based solely on their walking patterns. Here, we will discuss a couple of them.

A research done by Thang et al.[11] used acceleration data in the time domain to construct gait templates and DTW to evaluate the similarity score. Features in the frequency domain are classified using Support Vector Machine, achieving the accuracy of 79.1% and 92.7%, respectively. The data collected was from the accelerometer in the Google Nexus One phone. The phone position was fixed at the pocket location. A total of 11 volunteers participated in data collection. Each volunteer was asked to walk as naturally as possible

AfriCHI '18, December 3–7, 2018, Windhoek, Namibia

ACM ISBN 978-1-4503-6558-1/18/12…$15.00
https://doi.org/10.1145/3283458.3283488

on the ground floor. They walked for an overall of 12 laps with 36 seconds on each lap. 5 out of 12 lap data were picked randomly for the training phase and the other 7 lap data were used to predict.

Kobayashi et al.[7] constructed a feature extraction model based on Fourier transform features derived from 58 subjects who held the phone in a hand while walking. The experiments were conducted on gait identification by using the accelerometer embedded in the "iPhone". Signal data was collected at 33Hz sampling rate from 58 persons who freely walk in daily life withholding the cellular phone in hand. The model resulted in accuracy between 45% and 50%.

Another research done by Hoang et al.[5] used the gait template matching approach to compare data collected from 38 subjects on four consecutive gait cycles and reported EER of 3.5%. They examined the impacts of the sampling rate on constructing an adaptive gait recognition model with two different mobile phones. The most suitable sampling rate of 32-36 Hz, was considered for constructing an effective gait recognition mechanism. This type of sampling rate is rather low, which could be very useful for saving energy on a mobile. Moreover, a cross-device for gait recognition was also discovered, based on analyzing the level of the agreements of extracted features. In this study, interpolation was used only as a simple method for down/up-sampling. Therefore, accuracy could still be improved.

Derawi and Bours[3] proposed a feature extraction method that used time interpolation to find the average cycle of a subject for authentication. The result of this study was an EER of 20.1% for a dataset of 10 subjects. The Manhattan distance metric was implemented in this gait recognition.

The biggest drawback in many of the previous work is the fact that the system was not tested under serious attacker attempts. Also, the signal processing was done on computers in many cases accordingly, it doesn't give real-time feedback. We attempt to create an application which independently performs the gait authentication task, gives real-time feedback and test it against human-based impostors.

3 CONCEPT AND IMPLEMENTATION

In order to test the gait authentication against the impostors, we implemented a real-time feedback android based app. Figure 1 shows the different phases of the application starting from filtering to differentiate between impostor and actual user.

3.1 Implementation Phases

The first phase is removing the noise recorded alongside the data from the accelerometer. We used a low pass filter with an alpha variable chosen according to the sampling rate. We calculate the alpha every time a new sample is received from the accelerometer. This is done by measuring the time between consecutive samples and depending on this interval the alpha is computed. This way we ensure the highest accuracy possible, which is superior to the static one.

In the second phase, the magnitude of acceleration is computed from individual axis data of each sample as given in equation 1 in which the x,y, and z represent the acceleration alongside the main 3 axes. This is done to avoid change in readings in case the phone's orientation is changed inside the users pocket. In other words, the magnitude of acceleration is not affected by the orientation of the phone as long as it remains in the same body area.

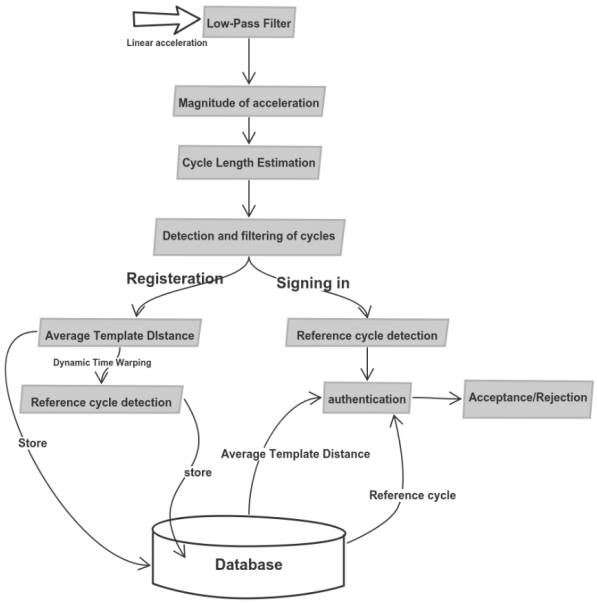

Figure 1: Flow diagram of the steps taken until registration/authentication is complete

$$a = \sqrt{x^2 + y^2 + z^2} \tag{1}$$

The third phase focuses on detecting the cycle length. Through experimentation, we discovered that in almost all cases a cycle length takes 90-160 samples per cycle. Therefore, we extract 30 samples from the middle of the data and compute the absolute difference between these 30 samples and every consecutive 30 samples. The local minimas are calculated and the difference between every two consecutive elements out of the indices of the local minimas are calculated. Lastly, the mode of the array of differences is multiplied by the originally chosen window size, which is 30 in our case. The result is an estimation of the length of cycles and will be a multiple of 30. Different window sizes were tested, the size of 30 had the best-estimated results.

The fourth phase is dedicated to detecting user cycles. Dynamic Time Warping (DTW) was used in this phase for comparing cycles. The Dynamic Time Warping algorithm lies at the core of our system. It is the main method of comparing cycles with each other and find similar cycles. To detect the full cycle we start by searching for the minimum point in the middle of the samples in the range of twice the length of the estimated cycle. From this point, we add the length of the estimated cycle. Normally the end of a cycle is the start of the next but this is not always the case. Also, due to the fact that our estimated length is not exact, we perform a small search around the end point of the cycle, looking at the beginning of the next. This is repeated until the end of the samples is reached. The previous process is again performed but this time in the backward direction. The next step is to remove outlier cycles, we did so by computing the distance for each cycle to all other cycles and taking the average

of these distances. Any cycle having an average of more than 20% different from the total average is removed. The previous process is repeated until no cycles are omitted. The reason 20% was chosen as the limit is due to the fact that it provided the best results through experimentation.

In the fifth phase, we compute the average of average distances from each cycle to all other cycles and save it under the user's name. It represents the average transformation cost of which a genuine signal should have to the average (reference) cycle. This brings us to the next phase which is calculating the reference cycle for the user, which is done by choosing the cycle with the lowest average distance to all the other cycles.

Finally, for authentication, the detected cycle is compared to the reference cycle stored and the distance between them is computed. This distance is divided by the average template distance computed earlier when the user registered as seen in equation 2. This ratio should give a number between 0 and 1.3 for genuine attempts, with 0 being a perfect match between both cycles while 1.3 is borderline acceptable. The idea behind this proposed ratio lies in trying to transform one signal to the other using Dynamic Time Warping. If the cost of transformation is 0, which is unrealistic, this means both time series being compared are identical and the ratio will equal 0. While if the cost of transformation is equal to the average template distance saved in the database, then the ratio equals one. The selection of 1.3 as the upper bound limit for acceptance is based on experimentation by which the genuine attempts almost always remain below this upper bound. While on the other hand, impostor attempts usually ended up around 1.4 to 1.8 when the impostor tried to imitate one's gait. These kinds of experimentation were carried before the actual assessment of the system in order to be able to decide on the best settings.

$$Similarityscore = \frac{DTW(Template1, Template2)}{AverageTemplateDistance(Template1)} \quad (2)$$

4 EXPERIMENTAL DESIGN

The goal of this study is to experiment with the system against human impostor attacks. In order to evaluate the application, we had three phases, registration, genuine attempts, and impostors. We invited 30 participants in both registration and sign-in phases, 25 males and 5 females between the age of 19 and 25(mean = 22; SD=0.9097). Participants were from different backgrounds.

4.1 Apparatus

To detect gait and record walking patterns of users, a smartphone 3, 2 cameras 4and a tablet5 were used. To detect gait and record the user's walking pattern, minimal equipment was used. Besides the smartphone, 2 cameras [1] with 30 fps and a tablet[2] with a resolution of 800 x 1280 were used simultaneously to record the user's walking pattern to simulate the attacks afterward.

[1]https://www.logitech.com/en-us/product/d-webcam-c310
[2]Galaxy tab E smt561

4.2 Experiment Procedure

Registration Phase After the participants arrived at the lab, we explained the purpose of the study, gave them the smartphone [3], then a consent form along with demographics was signed and collected. Each Participant was instructed to stand in 1 end of the hallway. Then, the participant press "register" and put the phone in their right pocket before starting to walk. They were instructed to walk naturally until they hear a notification from the smartphone indicating that the recording has ended. Out of These subjects, 10 also registered a second profile in which they carried a 5 kg bag.

Genuine Attempts The participants were asked to log in to the system. They were requested to write their name and press "login", then keep walking until they hear a notification sound. This process is repeated 3 times for each user to simulate normal authentication mechanisms. In addition, another 3 times with the bags for whom who registered with one.

Impostor Attempts In order to test the system's security, another 15 participants were invited to represent attackers. Each participant watched the recorded videos from 3 angles for a single user during their walking session. They were free to re-watch the videos as much as needed and were asked to analyze the exact walking pattern of the user they're watching. Then they were given the same instructions as the past participants but were asked to imitate that specific walking pattern they just saw. This process was also repeated 3 times for each attacker. The attackers were chosen specifically to match the user they are trying to imitate in regard to height and body shape. This was to ensure the system being evaluated under the most extreme conditions.

5 RESULTS

Each participant tried to sign-in to their profile 3 times following the same instructions. The reason why we chose 3 times is to simulate a real system with 3 sign-in attempts and then it blocks the user. The sign-in attempts were conducted in a different time slot than the registration one. This was done to ensure the integrity of the upcoming results. We received a False Rejection Rate (FRR) of 22.3%. Regarding the 10 users who had a second profile in which they registered in the system while carrying a bag. The results have shown that carrying a bag had little to no effect on the gait cycle. In the upper right graph in Figure 2 is the cycle of a user walking normally. While in the lower right graph is the same, except the user was carrying a 5kg bag. As seen, the cycles are almost identical. The other participants gave the same result. It is worth noting that cycles are not supposed to always be identical. Even if the same user had 2 normal walking sessions, the reference cycles from the 2 walks could be slightly different in some areas of the signal.

For fraudulent attempts, the same experimental flow was conducted for the attacks. Following the same calculations, we had a 37.8% False Acceptance Rate (FAR).

[3]https://www.htc.com/us/smartphones/htc-10/

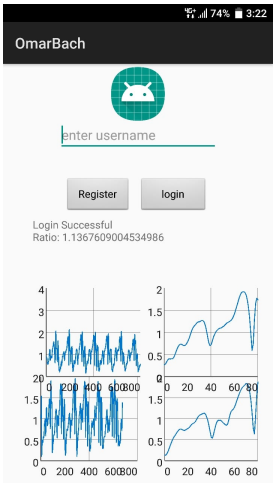

Figure 2: A user tried registering without a bag then logging in while carrying a 5kg bag.

5.1 Discussion

We received an FRR of 22.3% for the genuine attempts. For the 10 users who had a second profile in which they registered while carrying a bag, the results show that carrying a bag had no effect on the gait cycle. In the upper right graph in Figure 2 is the cycle of a user walking normally. While in the lower right graph is the same, except the user was carrying a 5kg bag. As seen, the cycles are almost identical. For the fraudulent attempts, the same experimental flow was conducted for the attacks. Following the same calculations, we had a 37.8% False Acceptance Rate (FAR). As we can see, the application shows a great potential. At 77.7% rightful acceptance rate, we could say that the application is not far from being user-friendly. In regard to the application's security, only 37.8% of attackers were able to impersonate genuine users. Keeping in mind that each attacker analyzed high-quality videos showing 3 different angles in which the victim was walking. In addition to the fact that attackers were chosen to attempt impersonating users who had very similar height and body shape. So 37.8% of fraudulent attempts being accepted in these extreme conditions is acceptable as the system still has a potential for improvement. The main limitation is that the user has to walk in a straight line and this doesn't simulate real behavior.

6 CONCLUSION AND FUTURE WORK

In this paper, we simulated human impostors on existing gait profiles by imitating other gait cycles. We developed an Android-based application to compare gait profiles. In the experiment, both attacking and attacked participants were chosen to have similar height and body shape. We received a FAR of 37.8% and an FRR of 22.3%. The system results were satisfactory as we did not use any machine learning algorithms. Future recommendations involve testing the system in different movements rather than straight path i.e circular paths. The experiment proved that with further optimization for the system accuracy, it could rival modern biometric authentication technologies.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

[2] Adam J Aviv, Katherine L Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge Attacks on Smartphone Touch Screens. *Woot* 10 (2010), 1–7.

[3] Mohammad Derawi and Patrick Bours. 2013. Gait and activity recognition using commercial phones. *computers & security* 39 (2013), 137–144.

[4] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 11.

[5] Thang Hoang, Thuc Dinh Nguyen, Chuyen Luong, Son Do, and Deokjai Choi. 2013. Adaptive Cross-Device Gait Recognition Using a Mobile Accelerometer. *JIPS* 9, 2 (2013), 333.

[6] Felix Juefei-Xu, Chandrasekhar Bhagavatula, Aaron Jaech, Unni Prasad, and Marios Savvides. 2012. Gait-id on the move: Pace independent human identification using cell phone accelerometer dynamics. In *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on*. IEEE, 8–15.

[7] Takumi Kobayashi, Koiti Hasida, and Nobuyuki Otsu. 2011. Rotation invariant feature extraction from 3-D acceleration signals. In *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 3684–3687.

[8] Jennifer R Kwapisz, Gary M Weiss, and Samuel A Moore. 2010. Cell phone-based biometric identification. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*. IEEE, 1–7.

[9] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the Design Space of Graphical Passwords on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, Article 11, 14 pages. https://doi.org/10.1145/2501604.2501615

[10] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, New York, NY, USA, 56–66. https://doi.org/10.1145/1143120.1143128

[11] Hoang Minh Thang, Vo Quang Viet, Nguyen Dinh Thuc, and Deokjai Choi. 2012. Gait identification using accelerometer on mobile phone. In *Control, Automation and Information Sciences (ICCAIS), 2012 International Conference on*. IEEE, 344–348.

[12] Liang Wang, Tieniu Tan, Weiming Hu, and Huazhong Ning. 2003. Automatic gait recognition based on statistical shape analysis. *IEEE transactions on image processing* 12, 9 (2003), 1120–1131.