Secure Techniques and Methods for Authenticating Visually Impaired Mobile Phone Users

Md Munirul Haque, Shams Zawoad, and Ragib Hasan
{mhaque, zawoad, ragib}@cis.uab.edu
Department of Computer and Information Sciences
University of Alabama at Birmingham
Birmingham, AL 35294-1170

***Abstract*—A series of new types of frauds and threats have emerged with the increased popularity of smartphones. Studies show that smartphone users are three times more likely to become the victims of identity fraud. Though researchers have developed many well known methods for user authentication in smartphone, little has been done focusing on visually impaired mobile device users. Commonly used username-password based authentication is not suitable for such users as it is cumbersome and highly susceptible to eavesdropping. In this paper, we have proposed a comprehensive algorithmic model for detecting different physical activities, such as walking, by analyzing the accelerometer sensor data from smartphones. Our proposed scheme proves that each person's gait pattern is unique and can be used as a bio-metric data for authentication. The new tool promises to provide a feasible solution for authentication, especially for visually impaired smartphone users, free from aural and visual eavesdropping.**

***Index Terms*—Blind Authentication; Gait Detection; Usable Security and privacy;**

I. Introduction

Mobile phones have become an inseparable part of modern life in all aspects. Currently, in USA, approximately half of the adults (46%) own a smartphone of some kind [1]. Though there are no exact statistics on the total number of smartphone users, who are blind or disabled; it is a reasonable assumption that the number is increasing. This technological revolution, along with relatively affordable price has attracted thousands of users with various disabilities including the visually impaired. Development of specially designed smartphones for blind users in recent times (Ray by Qualcomm, Georgie by Samsung) triggered a rapid increase in the number of blind and visually impaired users. Such users use smartphones for various purposes starting from daily activities like emails, text messages, and social networking, to more sophisticated tasks like online banking and stock market brokering. However, this rise in smartphone usage also introduces several security threats and attacks.

According to Reuters, about 12 million people in USA were victims of identity theft in 2011. The number is a significant 13% increase from 2010 [2]. This issue has been fueled by the upward trend of using smartphones and social media. Roughly 7% of all smartphone users have been victims of identity theft in 2011 [2]. It has been found that approximately 62% of the smartphone users do not use the password/PIN based home screen protection system due to various reasons including the requirement of remembering strong password and feeling of discomfort [2]. It is no wonder that a 2012 study on 13 blind smartphone users has found that none of them use the PIN based authentication system [3]. This creates the opportunity for anyone who has access to an unattended smartphone to collect personal information.

Though usable security has become a buzzword in recent years, it has hardly focused on the usability issues of disabled people. All the applications developed for blind users rely either on the Braille method or audio based instructions, both of which are vulnerable to common threats of aural-visual eavesdropping or shoulder surfing. Though any smartphone user can be a victim of these security threats, blind people are more vulnerable to these threats considering the very nature of their disability.

Smartphones have screen reader applications that echoes the user input, which could be a good feature for blind users. For example, iPhone has a screen reader application named VoiceOver [4]. However, these applications are highly susceptible to aural eavesdropping by frauds, or even bystanders since the system echoes even when a person enters a password/PIN. Blind or visually impaired smartphone users quite often prefer bigger fonts due to better visibility and usability. But this feature has a trade off since it increases the chance of visual eavesdropping. People can look at the smartphone contents from a distance and the visually impaired people might even fail to notice the eavesdropper. Unwanted access has also become a very common security threat for all smartphone users nowadays. A recent study has found that in 89% of cases, people tried to access private information of unattended smartphones [5]. People can very easily access information from lost, stolen, or unattended smartphones, if they are not locked. Moreover, the commonly used 4 bit PIN is unable to provide a strong enough protection for smartphones. Several alternative methods based on CAPCHA [6], graphical password [7], and shape drawing [8] have become available for sighted people. Unfortunately, none of these methods are viable as a solution for blind users. This analysis proves the urgent necessity of an easy to use authentication tool, which can protect the blind users from the aforementioned security threats.

Present smartphones are equipped with new sensors, such as, accelerometer and gyroscope, which can be utilized to securely authenticate a user. Based on these new features, we developed a novel blind user authentication technique that is easy to use and free from common security threats. We have proved that the gait pattern of each person is unique, and this bio-metric feature can be used for authenticating visually impaired users. The users need to simply walk for 5 steps with smartphones in their hand or pocket. The system captures the walking cycle pattern, and matches it against a pre-recorded pattern to authenticate a user.

In this paper we describe a novel authentication scheme for visually impaired mobile phone users using only the accelerometer sensors of a mobile phone. We present the results of a feasibility study in which we tested the apparatus with six subjects. The paper is organized as follows. Section II provides the authentication scheme using cell phone accelerometer data. In Section III, we present the experimental results of our gait cycle-based authentication scheme. Section IV provides the contemporary studies related to authentication for the disabled and gait detection using accelerometer sensors. Finally, we conclude in Section V with future guidelines.

II. Authentication Scheme

The availability of rich variety of on-board sensors of smartphone provides the functionality of recording bio-metric characteristics of its owner. It has a tri-axial accelerometer, gyroscope, and a microphone, which can be utilized to record gait and voice of the owner respectively.

Accelerometer. The accelerometer available in today's smartphones is a tri-axial accelerometer, i.e., there are actually three accelerometers, one working along each of the three primary axes of the device. The x-axis measures along the short side, the y-axis measures along the long side, and the z-axis is a line perpendicular to the face of the phone [9]. Values are given in terms of g, where 1g is the force of gravity.

There are three filtering modes available to isolate the data of our interest – none, low-pass filtering, and high-pass filtering. No data filtering is provided in 'none' filtering mode; applications are provided with raw data from the accelerometers. Low-pass filtering can be used to focus on the gravity and orientation aspect of the device, and to reduce the effect of instantaneous and momentary accelerations. In contrast, high-pass filtering helps to get rid of the gravitational effects, and finds out the instantaneous movement of the device. As gait is represented as the collection of instantaneous movements of the device, using high-pass filtering will serve our purpose.

Figure 1 shows the position of the three axes of smartphone's accelerometer. X, Y, and Z values are linear acceleration values. They point to the direction of gravitational force. Together, X, Y, and Z form a 3-D acceleration vector that indicates the phone's directional movement with respect to gravity [9].

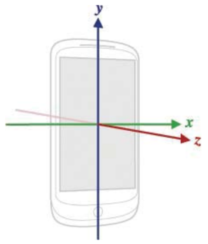


Fig. 1: Accelerometer Axes

Gait Cycle. When we walk, we put forward our left or right foot first followed by the other foot. This event occurs repeatedly, i.e., human walking is cyclic. Based on this fact, we record the accelerometer data, and find repeated occurrence of some pattern. We notice that output of any of the individual axes is more irregular than the combined output of all the three axes. For this reason we use the combined signal to extract the representative gait cycle. Among various methods of combination, the following works best in our purpose:

$$R_i = sin^{-1}(Z_i/\sqrt{X_i^2+Y_i^2+Z_i^2}), i = 1 \ldots k \qquad (1)$$

Here X_i, Y_i, Z_i, and R_i represent vertical, forward-backward, side-way, and combined acceleration at the observation number i respectively, and 'k' denotes total number of recorded observations. Gait data is a time series and we need a sophisticated algorithm for matching the gait cycles. We use Dynamic Time Warping (DTW) algorithm [10] for measuring similarity between two gait cycles, which may vary in time or speed. As the DTW algorithm allows acceleration and deceleration of signals along the time dimension, it is a suitable procedure for detecting similarity/dissimilarity between different person's walking.

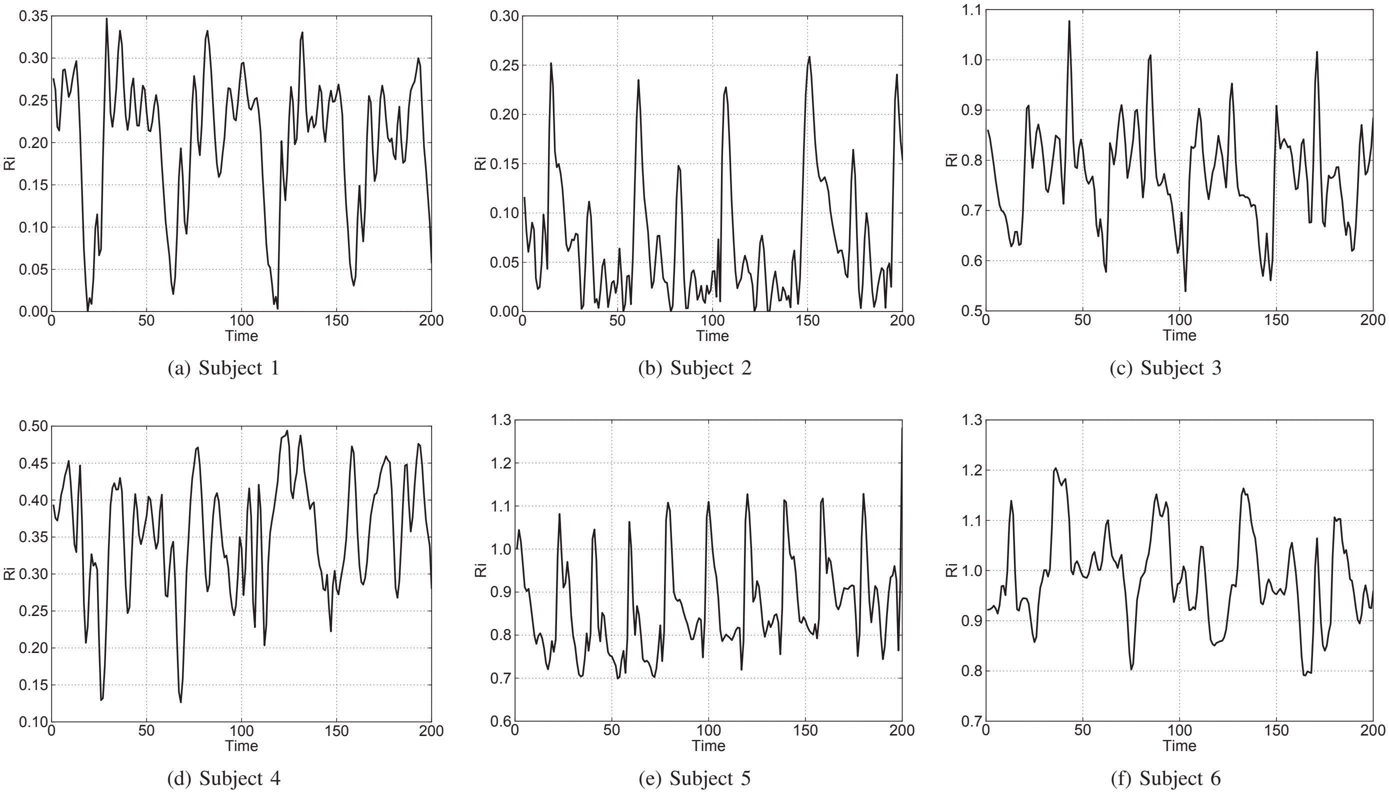
III. Experimental Results

A. Experimental Setup

We built our prototype application on the Android 2.3.3 (Gingerbread) platform. Android provides support for different types of sensors, including the accelerometer, which is needed as part of our authentication protocol. As we were not able to run the experiment with actual visually impaired people, we chose six people with normal vision as our subjects. We argue that authenticating a normal person using his walking pattern should be the same as authenticating a blind person. All of the six participants are students, age ranged from 22-30, five of whom are males, and one female. Three of them have 171 cm height, one is 183 cm, one is 162 cm, and one is 153 cm of height. The first step of any bio-metric authentication protocol is to store user's bio-metric information. In our case, the bio-metric feature is the walking pattern or the gait cycle. Hence, in our application, there are two modules, one is gait cycle collector, and the other one is the authentication module.

B. Evaluation

To evaluate our authentication protocol, we initially collected the gait cycle for our subjects, when they walked for 5 steps in an unobstructed straight path. The subjects were instructed to use the feature collection module in the



(a) Subject 1

(b) Subject 2

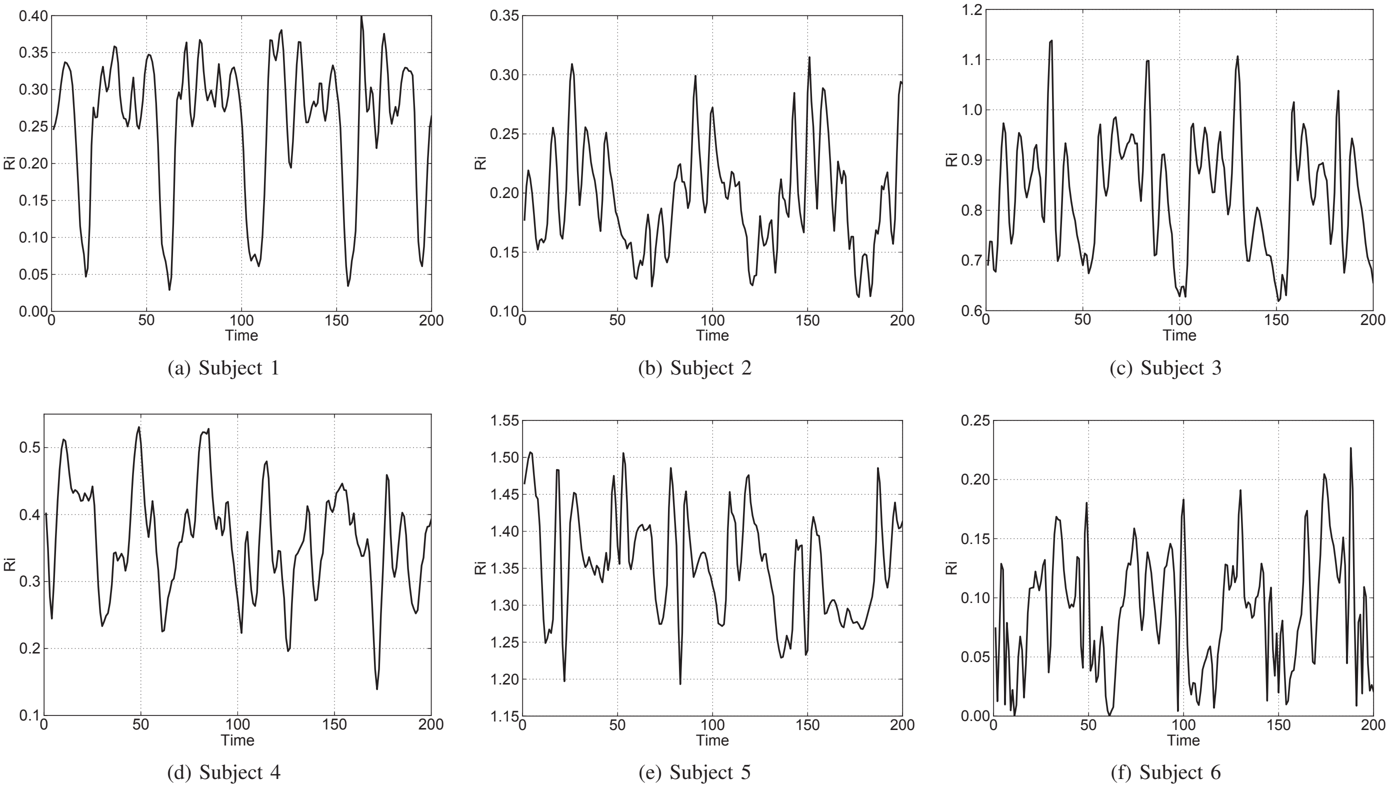
(c) Subject 3

(d) Subject 4

(e) Subject 5

(f) Subject 6

Fig. 2: Gait cycle for normal walking of 6 subjects



(a) Subject 1

(b) Subject 2

(c) Subject 3

(d) Subject 4

(e) Subject 5

(f) Subject 6

Fig. 3: Gait cycle for slow walking of 6 subjects

smartphone with appropriate instruction. Before starting the walk, they pressed a start button, and at the end of the walk, they pressed a stop button. During the walk, the phone was held in their hand. We stored the accelerometer data during the walk and according to equation 1, we calculated the R_i value and plotted this value against time. Figure 2 presents the resultant gait cycle for our six participants. The observed results reflect that the gait cycle for six different participants are significantly different. After preserving all the gait cycle data in smart phones, we instructed our subjects to run the authentication module, and walk again for the same distance. The gait cycle for the second time walking is then compared with the previously stored data using the DTW algorithm.

We noticed that for four of our subjects, the algorithm could not match the two walking pattern. Based on the time taken to complete the 5 steps, we noticed that those four subjects walked notably slow compared to their initial walking style. Hence, we again collected the gait cycle of all our subjects, while they were walking at a slow speed. Figure 3 represents the gait cycle of our six subjects for slow walking. From the figures, it is clear that for subjects 2, 4, 5, and 6, the gait cycles were different from their corresponding gait cycle of previous walking. Another important issue is that the gait cycle for slow walking of one person does not match with the gait cycle for normal walking of a different person, which is a crucial criteria for authentication.

Because of the difference in gait cycle for normal and slow walking, we stored information about both types of gait cycles for all users. At the time of authentication, we match the two different gait cycles of every user. Hence, even if a user walks a bit slowly at the time of authentication, we can successfully determine his true identity. For every subject, we tested our authentication protocol for four times. Figure 4a represents the gait cycle of feature collection step, and Figures 4b to 4e illustrate the gait cycle of four authentication trials for subject 2. In Figure 4f, we superimpose one cycle of five different attempts of a single subject, and find a close match among them. Though gait is very dependent on gender and height [11], figure 2 (a-c) and 3 (a-c), which correspond to 3 male subjects with the same height, shows that the accelerometer data is sensitive enough to distinguish them uniquely.

While authenticating subject 2, we ran the DTW algorithm to measure the distance between subject 2 and other subjects. Table I represents the result of this measurement. The lowest distance that we found is 0.00193200003992 (marked as blue). Then, we ran the DTW algorithm to measure the distance between the gait cycles collected at feature collection step, and the gait cycles collected at authentication attempts. Table II shows the comparison result. From this data, it is clear that we can successfully authenticate a person by measuring the DTW generated distance. Even the highest distance found in this step (0.001215616074997 – marked as blue) is less than the lowest distance that is found while comparing the gait cycle of different subjects. This clearly indicates that by comparing the DTW measured distance between gait cycles, we can uniquely authenticate any person.

Compare	Distance Measured by DTW
Subject 2 VS Subject 1	0.00193200003992
Subject 2 VS Subject 3	0.34221432967055
Subject 2 VS Subject 4	0.016400369870325
Subject 2 VS Subject 5	0.644525043151712
Subject 2 VS Subject 6	0.853350103141241

TABLE I: DTW measured distance between subject 2 and others

Compare	Distance Measured by DTW
Attempt 1 VS Attempt 2	0.001215616074997
Attempt 1 VS Attempt 3	0.000540532880768
Attempt 1 VS Attempt 4	0.000476056129779
Attempt 1 VS Attempt 5	0.001079208068308

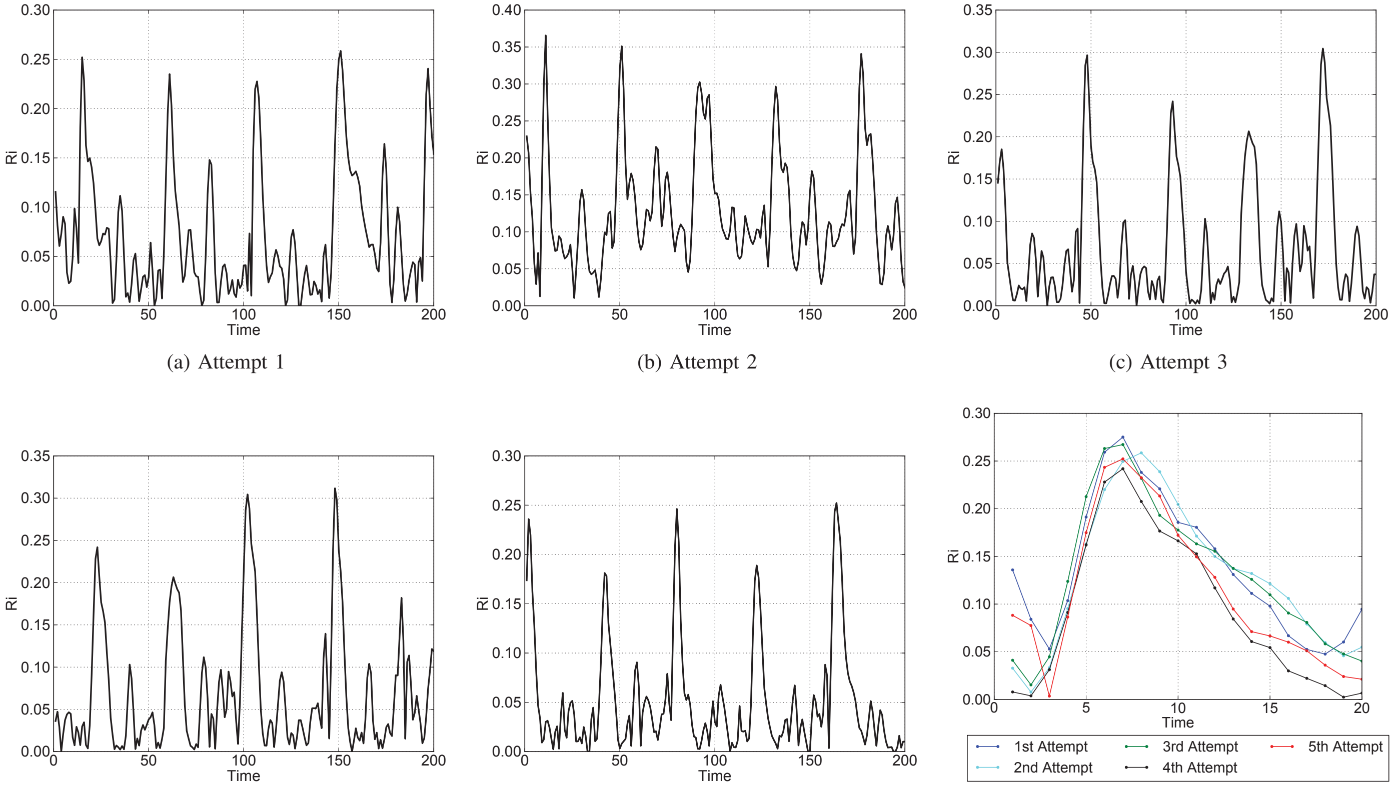
TABLE II: DTW measured distance between Attempt 1 and others

IV. Related Work

In this section, we provide the studies regarding authentication techniques for visually impaired mobile phone users. We also provide studies related with activity identification, and gait-based authentication using cell phone's accelerometer and dedicated accelerometer.

Using touch screen input, Azenkot *et al.* presented Perkinput, a text entry model for blind persons, who are familiar with Braille method [12]. In their proposed method, signals are captured through multi-point touches, where each finger represents one bit, either touching the screen or not. They used maximum likelihood and tracking algorithms to detect the fingers that touch the screen based on user-set reference points. They evaluated their text input scheme with 8 blind participants, who were proficient in Braille, and found that one-handed Perkinput was significantly faster and more accurate than iPhones VoiceOver [4]. This touch-based input scheme can be used for user name and password based authentication scheme. However, this method is vulnerable against visual eavesdropping.

Besides using traditional user name and password based authentication scheme for blind people, researchers proposed other unorthodox authentication methods. Wobbrock *et al.* proposed TapSongs [13], which enables user authentication based on a single binary sensor (e.g., button) by matching the rhythm of tap down/up events to a jingle timing model created by the user. Their proposed algorithm searches for absolute match between users' created rhythms and the input rhythm at the the time of authentication, and learns from successful login attempts. They evaluated their scheme with 10 subjects and found that after the participants created their own TapSong models from 12 examples (<2 minutes), their subsequent login attempts were 83.2% successful. However, they pointed out that aural and visual eavesdropping of the experimenter's logins resulted in 10.7% successful imposter



(a) Attempt 1

(b) Attempt 2

(c) Attempt 3

(d) Attempt 4

(e) Attempt 5

(f) Superimposed one cycle from the 5 attempts

Fig. 4: Gait cycle of 5 attempts by one subject

logins by the participants. This clearly shows that TapSongs is susceptible to visual eavesdropping.

Azenkot *et al.* proposed another authentication mechanism for disable person – PassChords [3]. This is a non-visual authentication method for touch surfaces, where users enter a PassChord by tapping several times on a touch surface with one or more fingers. The set of fingers used in each tap defines the password. They claimed that four-tap PassChord has about the same entropy, a measure of password strength, as a four-digit personal identification number (PIN) used in the iPhone's passcode lock. Though this scheme cannot be forged by aural eavesdropping, this is vulnerable to visual eavesdropping just like TapSongs.

Though no blind authentication scheme using accelerometer sensors has been proposed yet, activity and gesture detection using cell phone sensors have gained researchers' attention. Using accelerometer and gyroscope sensors, Kwapisz *et al.* showed that it is possible to identify different human activities [14]. They obtained a high level of accuracy in recognizing some basic actions, such as, walking, jogging, sitting, and standing. In addition to the above accelerometer-based activity identification, multiple sensors can simultaneously be used to identify a very precise activity. Bieber *et al.* discussed the process of recognizing human activity, and sensing the surrounding environment by using accelerometer and sound sensors [15]. They showed that only the accelerometer sensor data cannot detect office works, but the fusion of accelerometer and sound data can help to detect mouse click or keyboard typing event. Liu *et al.* showed that personal gestures can be recognized by a single three-axis accelerometer [16]. They used smartphone's sensors and got 98.6% accuracy for a single training sample for gesture recognition.

Prior to the availability of built-in sensors in mobile phones, researchers worked with dedicated sensors for gait detection. Gafurov *et al.* proposed a person recognition system based on gait data, which is collected from an accelerometer sensor attached to a person's body [17]. Rong *et al.* provided an approach for identifying users based on three dimensional gait acceleration signal characteristics acquired by a portable accelerometer attached to the center of the users' waist [18]. Bachlin *et al.* explored the effects of some real-world factors, e.g., extra load, different shoes, and natural variation over days on the gait detection [19]. They opined that these factors may affect the gait of an individual so much that false rejection may occur.

The closest work related to our work is conducted by Tanviruzzaman *et al.* [20]. They used gait cycle, and location of a person as a signature of that person. To implement their scheme, they used iPhone's accelerometer for capturing gait cycle, and A-GPS module to identify the location of a phone. The iPhone extracts the gait cycle pattern from the accelerometer data, and finds out the owner's familiar places using his location tracks. The phone periodically checks the current gait pattern with the saved gait template, and checks whether it is in a familiar place of the owner. If the phone finds out that it is in a familiar place, it accepts partial matching score for the gait cycle. Whenever the phone finds it in an unfamiliar place, it requires an exact match of the gait patterns. However, it takes a long time to build a personal profile before one can use this authentication scheme. Moreover, an exact matching of gait pattern is not practically feasible, which is clear from our experimental results. Finally, they did not conduct any usability testing of their proposed scheme.

V. Conclusion and Future Work

User friendly authentication mechanism for visually impaired people is an important issue with little focus. Our proposed gait pattern based authentication model has the potential of protecting the common security threats experienced by visually impaired people. Though we have focused on the blind user group, the usability domain of the application can be extended to other sophisticated areas. General users can switch from their usual PIN based system to gait pattern based authentication system while being at a vulnerable location at any given time. The application can also be useful for unlocking mission critical devices to ensure the physical security even if the devices fall in the hands of the enemy. Such mechanism can be especially suitable in nighttime operations where even the low light for entering password/PIN can be catastrophic. Moreover, this technique is much inexpensive compared to other biometric authentication techniques like retina or finger scan.

Building a gait pattern based authentication mechanism is the first step of our overall goal. We plan to deploy our system on 10 blind people for a week long study on usability of the designed mobile application. The study will be performed to explore and evaluate the security issues that arise from using smartphone based secure communication by blind people. We will also compare the current PIN based authentication method with our proposed method in terms of usability features including efficiency, effectiveness, and preference. Instead of identifying the usability issues based on a particular session, we will ask the participants to use the authentication tool on their smartphones over a week, and then collect their feedback. This is because there are moments in daily life when walking for authentication can be considered as a burden. We would like to incorporate all such usability issues for blind users, which will complete a much needed research for the visually impaired group of users.

Acknowledgments

This research was supported by a Google Faculty Research Award, the Office of Naval Research Grant #N000141210217, the Department of Homeland Security Grant #FA8750-12-2-0254, and by the National Science Foundation under Grant #0937060 to the Computing Research Association for the CIFellows Project.

References

[1] A. Smith, "Nearly half of american adults are smartphone owners," Online at http://pewinternet.org/Reports/2012/Smartphone-Update-2012/Findings.aspx, 2012.

[2] M. Lipka, "Rise in identity fraud tied to smartphone use," Online at http://www.reuters.com/article/2012/02/23/uk-idtheft-javelin-idUSLNE81M01H20120223, 2012.

[3] S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock, "Passchords: secure multi-touch authentication for blind people," in *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*. ACM, 2012, pp. 159–166.

[4] Apple, "Voiceover," Online at http://www.apple.com/accessibility/iphone/vision.html.

[5] streetwise-security-zone, "The honey-stick project," Online at http://www.streetwise-security-zone.com/members/streetwise/adminpages/honeystickproject, 2012.

[6] J. P. Bigham and A. C. Cavender, "Evaluating existing audio captchas and an interface optimized for non-visual use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009, pp. 1829–1838.

[7] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Proceedings of the 21st Annual Computer Security Applications Conference*. IEEE, 2005, pp. 10–pp.

[8] P. v. Oorschot and J. Thorpe, "On predictive models and user-drawn graphical passwords," *ACM Transactions on Information and system Security (TISSEC)*, vol. 10, no. 4, p. 5, 2008.

[9] wavefrontlabs.com, "Accelerometer data," http://wavefrontlabs.com/Wavefront_Labs/Accelerometer_Data.html, [Accessed May 25Th, 2013].

[10] N. Ye *et al.*, *The handbook of data mining*. Lawrence Erlbaum Associates, Publishers, 2003.

[11] S. Cho, J. Park, and O. Kwon, "Gender differences in three dimensional gait analysis data from 98 healthy korean adults," http://www.ncbi.nlm.nih.gov/pubmed/14967577, [Accessed Augutst 15Th, 2013].

[12] S. Azenkot, J. O. Wobbrock, S. Prasain, and R. E. Ladner, "Input finger detection for nonvisual touch screen text entry in perkinput," in *Proceedings of the 2012 Graphics Interface*. Canadian Information Processing Society, 2012, pp. 121–129.

[13] J. O. Wobbrock, "Tapsongs: tapping rhythm-based passwords on a single binary sensor," in *Proceedings of the 22nd annual ACM Symposium on User Interface Software and Technology*. ACM, 2009, pp. 93–96.

[14] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Activity recognition using cell phone accelerometers," *SIGKDD Explor. Newsl.*, vol. 12, no. 2, pp. 74–82, Mar. 2011.

[15] G. Bieber, A. Luthardt, C. Peter, and B. Urban, "The hearing trousers pocket: activity recognition by alternative sensors," in *Proceedings of the 4th International Conference on PErvasive Technologies Related to Assistive Environments*. ACM, 2011, p. 44.

[16] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, "uwave: Accelerometer-based personalized gesture recognition and its applications," *Pervasive and Mobile Computing*, vol. 5, no. 6, pp. 657–675, 2009.

[17] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor," *Journal of computers*, vol. 1, no. 7, pp. 51–59, 2006.

[18] L. Rong, D. Zhiguo, Z. Jianzhong, and L. Ming, "Identification of individual walking patterns using gait acceleration," in *Proceedings of the 1st International Conference on Bioinformatics and Biomedical Engineering*. IEEE, 2007, pp. 543–546.

[19] M. Bachlin, J. Schumm, D. Roggen, and G. Töster, "Quantifying gait similarity: user authentication and real-world challenge," in *Proceedings of the 3rd International Conferences Advances in Biometrics*. Springer, 2009, pp. 1040–1049.

[20] M. Tanviruzzaman, S. I. Ahamed, C. S. Hasan, and C. O'brien, "epet: when cellular phone learns to recognize its owner," in *Proceedings of the 2nd ACM workshop on Assurable and usable security configuration*. ACM, 2009, pp. 13–18.