"User Authentication Method and Implementation Using a Three-Axis Accelerometer"

Alexandros Zaharis, Adamantini Martini, Panayotis Kikiras, and George Stamoulis

Department of Computer & Communication Engineering,
University of Thessaly
Greece, Volos
{alzahari,admartin,kikirasp,georges}@inf.uth.gr
http://wssl.inf.uth.gr

Abstract. The rapid growth of accelerometer use on consumer electronics has brought an opportunity for unique user authentication. We present an efficient recognition algorithm for such interaction using a single three-axis accelerometer. Unlike common user authentication methods which require memorizing complex phrases and are prone to physical attacks, our method requires a single training sample for a gesture pattern which allows users to authenticate themselves in a fast and secure manner. Our work imitates the use of physical handwritten signatures, which are a common authentication technique and tries to integrate them in a digital form. The presented method aims at providing easy to remember personalized gesture passwords through the muscle memory ability of the human body. An implementation using the wii remote sensor, along with identification results for different users is presented as a proof of concept.

Keywords: gesture recognition, three axis accelerometer sensor, user authentication.

1 Introduction

An increasing number of home electronic devices and mobile phones are equipped with accelerometers, enabling a device to "sense" how it is physically manipulated by the user. In our work, we use the word "gesture" to refer to the physical interaction of the user with the device and the word "signature" to refer to a three dimensional movement which produces easily identifiable results that can authenticate a user.

In the literature there are a lot of studies regarding the use of accelerometers as a tool for recognizing gestures [5-8]. Within this paper we will try to demonstrate that the recognition of a single, easy to remember three dimensional signature-like gestures for user authentication is feasible.

For example, a user can "shake" a phone in a special way to log in or a wii remote to load personalized data for a game. While many paradigms exist for user authentication, including password [9], biometrics [10-12], speech [13], and handwriting [14], accelerometer - based signature recognition has its unique value for user authentication because of its low cost, high efficiency, and no form factor change. These properties make it highly suitable for implementation on resource constrained devices, such as mobile phones and TV remotes or handheld game consoles.

P. Chatzimisios et al. (Eds.): MobiLight 2010, LNICST 45, pp. 192–202, 2010.

The goal of our work is to investigate the feasibility and usability of a three dimensional signature recognition based on a single tri-axis accelerometer[5], because either it is privacy-insensitive data, like personalized configurations on a game, or privacy-sensitive data like personal contacts stored in a mobile phone, the resilience to attacks and usability are dominating concerns.

In order to succeed in the aforementioned goal, a unique method and implementation is presented in *Section 4*. In *Section 5*, a series of tests and experiments is presented in order to prove the usability, security and effectiveness of the proposed method. Finally, the paper concludes with some useful remarks and our envisioned future research.

2 Related Work

Most user authentication methods are based on either what properties the user has, e.g. fingerprint [10], face [11] and iris [12], or what the user knows, e.g. password [9], or both, e.g. speaker verification [13] and handwritten signature recognition [14]. The work in [15-17] considers gesture as behavioural biometrics where the user has and attempts to verify or recognize the user identity based on a fixed gesture performed, e.g. a simple arm swing in [15]. Others allow the user to create any physical manipulation of the device as the authenticating gesture [5], with an error rate close to 3% and a single training sample. Notably, the basic method in [17] has over 14% equal error rate when not as many training samples are used. Moreover, the authors did not investigate how robust their methods are against attackers imitating the user, which is an important issue for every authentication method.

The goal of [16] is targeted on recognizing a user out of a small number of users sharing a device. The work achieved an accuracy of about 95% with a large number of training samples while the user had to perform a given gesture in a highly constrained manner, e.g. exact timing with real-time visual feedback. Related to our use of accelerometers, the work in [18] employed accelerometers to recognize the user with the gait pattern as behavioural biometrics.

What is unique about our proposed authentication method and implementation is the fact that a single 3D accelerometer device is used in order to authenticate the user with only three training samples. The notion of muscle memory, along with the physical signature, (a familiar motion to the user) lead to high identification rates while at the same time provide the user with an easy to remember, unique identifier. The identification algorithm digitalizes physical signature forensic techniques in order to distinguish unique marks and patterns on the performed signature in order to safely identify a user.

3 Muscle Memory and Handwritten Signature

This paragraph presents the two main principles/practices that facilitating the use of data produced by a 3D- axis accelerometer in a user authentication method.

3.1 Muscle Memory

When an active person repeatedly trains movement, often of the same activity, in an effort to stimulate the mind's adaptation process, the outcome is to induce physiological

changes which attain increased levels of accuracy through repetition. Even though the process is really brain-muscle memory or motor memory, the colloquial expression "muscle memory" is commonly used. Individuals rely upon the mind's ability to assimilate a given activity and adapt to the training. As the brain and muscle adapts to training, the subsequent changes are a form or representation of its muscle memory. There are two types of motor skills involved in muscle memory: fine and gross. Fine motor skills are very minute and small skills similar to those that we perform with our hands such as brushing teeth, combing hair, using a pencil or pen to write or sign, touch typing, playing some musical instruments, or even playing video games. Gross motor skills are those actions that require large body parts and large body movements as in sports such as bowling, baseball, rowing, basketball, golf, martial arts, and tennis, and activities such as driving a car (especially one with a manual transmission), piloting aircraft, playing some musical instruments, and marksmanship. Muscle memory is fashioned over time through repetition of a given suite of motor skills and the ability through brain activity to inculcate and instil it until they become automatic. To the beginner, activities such as signing are not as easy as they look. As one reinforces those movements through repetition, the neural system learns those fine and gross motor skills to the degree that one no longer needs to think about them, but merely to react and perform appropriately. In this sense, the muscle memory process is an example of automating an O.O.D.A [1] loop insofar as one learns to Observe, Orient, Decide, and Act.

When one picks up a pen to sign, automatically has a certain motion, style, number of strokes without requiring conscious thought about each movement. Other forms of rather elaborate actions that have become automatic include speech. It is said that it takes about 740 [1-2] of the same motions for your muscles to "memorize" the movements almost perfectly. Our method uses the already trained muscle memory of an individual performing a physical signature in order to achieve user authentication. The user has to use the 3- axis accelerometer as a pen in order to form his unique signature. As it will be demonstrated, due to user's previous training to the same movement in the real world the results are very accurate and can be used for user authentication.

3.2 Handwriting Forensics

The examination of handwriting to assess potential authorship proceeds from the principle of identification which can be expressed as: "Two writings are the product of one person if the handwriting characteristics, when taken in combination, are sufficiently individual and there are no fundamental unexplainable differences."

Generally, there are three stages in the process of examination [4]. In brief, they are:

1. Analysis: The questioned and the known items are analyzed and broken down to directly perceptible characteristics.
2. Comparison: The characteristics of the questioned item are then compared against the known standard.
3. Evaluation: Similarities and/or differences in the compared properties are evaluated and this determines which ones are valuable for a conclusion. This depends on the uniqueness and frequency of occurrence in the items.
4. Optionally, the procedure may involve a fourth step consisting of verification/validation or peer review.

Our method combines the knowledge of anthropology and document forensics science in order to produce an accurate user authentication method with a single 3D axis accelerometer.

4 Proposed Signature Recognition Method Based On a 3-Axis Accelerometer

The proposed Signature Recognition Method consists of two phases. In the first phase the user trains / registers his signature. The second phase consists of the user authentication module, where the user forms the signature and asks for validation after providing his username.

4.1 Phase 1: Training / User Registration

The first step in every user authentication process is registering the user. This phase is crucial for the success of a user authentication technique, as it must be robust, easy to understand by every user, fast (complete in a few steps) and accurate. The proposed method satisfies all the abovementioned aspects of a successful authentication method with an intuitive utilization of a single low-cost sensor.

Figure 1 illustrates the user registration process which correlates unique username chosen by the user with a gesture password (3D Signature). During this process a textual password is also generated along with a unique hash value that can act as a digital signature:

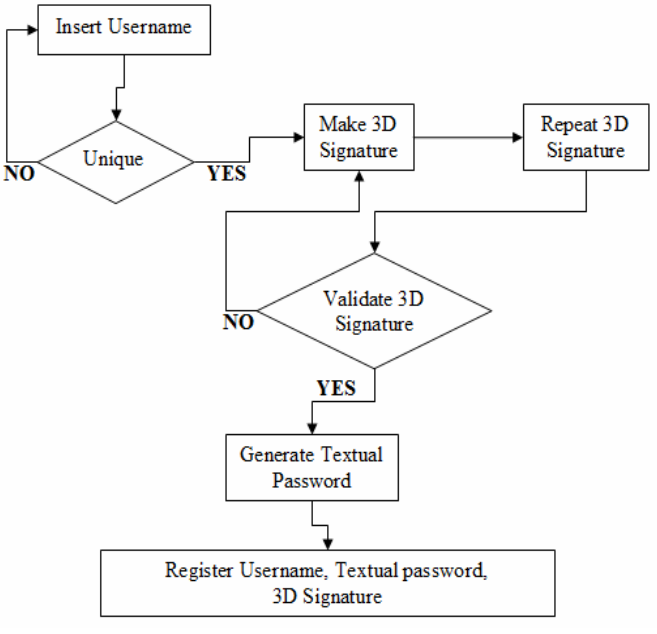

Fig. 1. User registration process

Step 1 – The user registration process begins by choosing a unique username.

Step 2 – After the username is chosen the user is asked to perform a 3D signature movement in a form of waving gesture in the three dimensional space. The capturing of the motion begins and ends with the sensor staying still for a few seconds. Three sets of acceleration values are collected, representing the x, y, z axis acceleration during the gesture. The gesture is then further analyzed in order to provide data that can be stored and compared to authenticate a user.

The data used for authentication are:

1. Elapsed time for the completion of the gesture.
2. The gesture is divided in smaller equal duration parts (time slots) for which the maximum and minimum acceleration values per axis is collected.
3. Starting sensor position (pitch, roll values)
4. Ending sensor position (pitch, roll values)
5. Total maximum and minimum acceleration value per axis is collected.

Step 3 – The user is asked to repeat the 3D signature in order to be validated. The above mentioned characteristics are compared to the newly acquired. If there is a match (with some tolerance) then the signature is validated.

Step 4 – After the validation has taken place a textual password along with a digital signature is being generated. The textual password is an 8 digit phrase (not random) created by numbers and characters which are directly seeded by the results acquired due to the 3D signature movement.

Step 5 – The username, textual password generated and 3D signature characteristics are stored and the user is registered.

4.2 Phase 2: User Authentication

In order to authenticate a user, his/her username and password must be provided. The password might be something the user "knows" (ex. text passwords) or something the user "has" (ex. biometry). Our users must provide a username and then form his/her personal 3D signature in order to be authenticated. The user is given three attempts to achieve authentication or his/her account else her account will be temporarily blocked. Optionally the user can login with the textual password generated after three failed 3D password attempts.

Step 1 – The user provides his/her username.

Step 2 – After the username is provided the user is asked to perform his 3D signature movement. The 3D signature characteristics are collected in order to be validated.

1. The data used for validation are:
2. Elapsed time for the completion of the gesture.
3. The gesture is divided in smaller equal duration parts (time slots) for which the maximum and minimum acceleration values per axis is collected.
4. Starting sensor position (pitch, roll values)
5. Ending sensor position (pitch, roll values)
6. Total maximum and minimum acceleration value per axis is collected.

This step can be repeated up to three times. If the process is completed correctly then proceed to ***Step 5.***

If all three attempts fail then proceed to ***Step 4*** or optionally ***Step 3***.

Step 3 – Textual password is needed in order to authenticate the user. If this step fails once, proceed to ***Step 4,*** else proceed to ***Step 5.***

Step 4 – The user is banned and the account is suspended. Further actions can be taken that are out of the scope of this paper.

Step 5 – The user is successfully authenticated

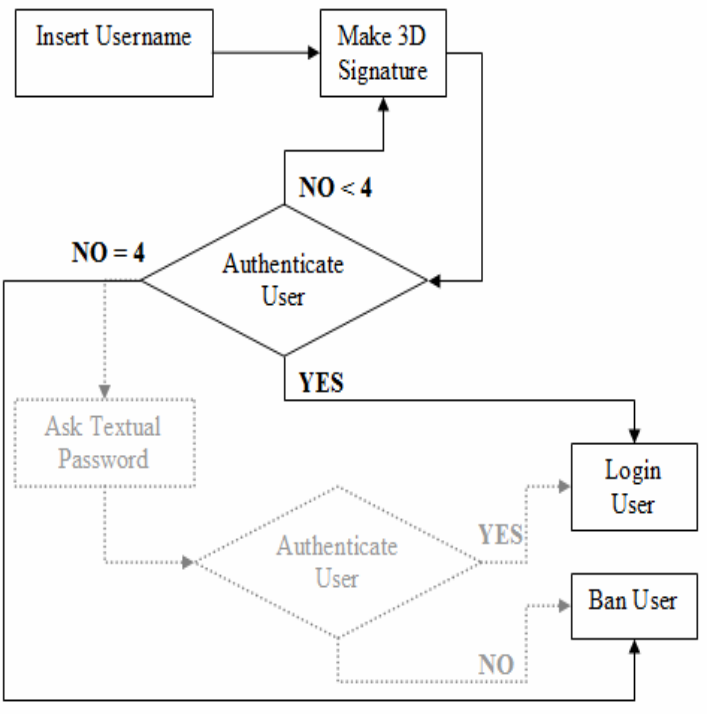

Fig. 2. User authentication process

4.3 Advantages

The advantages of the proposed authentication method are covering both practical and security issues.

Besides the fact that the proposed authentication method is innovative and intriguing for the user in relation to textual passwords, it has some other major advantages that must be pointed out, which are as follows:

1. The 3D signature password created is easier to remember than a "secure" 8 digit password.
2. The 3D signature password is faster and easier to perform than typing a secure 8 digit password.
3. The 3D signature password is difficult to steal; shoulder surfing attacks are difficult to succeed.

4. The 3D signature password cannot be written down, or given away to be performed by someone else.
5. It's cheaper to implement in many different devices (e.g. mobile phones), where biometrics would be difficult to implement.

5 User Authentication Implementation

In order to prove the validity of the proposed authentication method an implementation was designed, utilizing a simple commercial 3D accelerometer sensor and the use of a java library to capture acceleration data. The *WiiuseJ* [19] is an opensource java API which facilitates the use of *wii remote* on any computer.

5.1 Wii Remote

The *Wii Remote*, sometimes unofficially nicknamed "*Wiimote*", is the primary controller for Nintendo's Wii console. A main feature of the Wii Remote is its motion sensing capability, which allows the user to interact with and manipulate items on screen via gesture recognition and pointing through the use of accelerometer and optical sensor technology. The controller communicates wirelessly with the console or a personal computer via short-range Bluetooth radio, with which it is possible to operate up to 10 meters away from the console. The controller's symmetrical design allows it to be used in either hand. The Wii Remote has the ability to sense acceleration along three axes through the use of an ADXL330 accelerometer.

5.2 SquWiigle v1.0 Concept

SquWiiggle, derives from the word *squiggle* which means, a mark or movement in the form of a wavy line and the word *Wii* (Nintendo Game Console). While our prototype is based on the Wii remote hardware, the proposed authentication technique can be implemented to any device with a three-axis accelerometer similar to those found in most consumer electronics and mobile devices.

5.2.1 Implementation Specifications

The most important part of the implementation was the analysis of the 3D password gesture. In order to collect enough data to authenticate a user, different parameters must be stored:

Parameter 1: Elapsed time for signature completion

The elapsed time is the time duration between starting the capturing procedure of the 3D signature up to ending it. Time is calculated in milliseconds (ms)

Parameter 2: Maximum and minimum acceleration values per axis for segments

The 3D signature performed is divided in equal time segments. The number of segments depends on the elapsed time and is usually equal to:

$$\text{Segment Number} = 0.3 * \text{ElapsedTime(sec)}$$

For each segment the maximum and minimum acceleration values per axis (x, y, z) are calculated and stored.

Parameter 3: Starting sensor position

Starting sensor position is the position in which the user holds the acceleration sensor in order to start performing the password gesture.

The position can be described by the roll and pitch values that can be easily calculated using the following equations (1), (2).

$$\textbf{roll} = \arctan2(a_z, a_x) \quad (1)$$

$$\textbf{pitch} = \arctan2(a_z, a_y) \quad (2)$$

a_x = x axis acceleration, a_y = y axis acceleration, a_z = y axis acceleration

The *ArcTan2* function calculates ArcTan(Y/X), and returns an angle in the correct quadrant. The values of *X* and *Y* must be between -264 and 264. *X* can not be 0. The return value will fall in the range from -Pi to Pi radians.

Parameter 4: Ending sensor position

Ending sensor position is the position in which the user holds the acceleration sensor when he has finished performing the password gesture.

The position can be described by the roll and pitch values that can be easily calculated using the equations (1), (2).

Parameter 5: Total maximum and minimum acceleration value per axis

The total maximum and minimum acceleration per axis is calculated by simple storing the biggest and the smallest value per axis calculated on step 2.

6 Security Tests and Results

The Security tests where designed in order to prove both the validity of the proposed authentication method and the robustness of the algorithm in security attacks. The four users where divided in two categories experienced and inexperienced of different ages ranging from 16 to 51 years of age.

In the first test performed, the users had to register themselves in the system and then authenticate themselves for a three weeks period.

The following table depicts the authentication results along with failed attempts over time. The success rate is high with an average of 98.2% of successful authentication.

Table 1. User Authentication Attempts Results

User	Week 1			Week 2			Week 3		
	Success	Fail	Total	Success	Fail	Total	Success	Fail	Total
User 1	25	0	25	5	0	5	25	0	25
User 2	25	0	25	5	0	5	25	0	25
User 3	24	1	25	5	0	5	25	0	25
User 4	23	2	25	4	1	5	25	0	25

The following table depicts the time needed for each process along with the equivalent time for textual authentication using a strong 8 digit password for the first time. The 3D signature registration process is relatively slower than textual, but the authentication process is faster. Results were retrieved after ten attempts per user.

Table 2. User Registration – Authentication Timing

User	3D Signature, Registration	Textual Password, Registration	3D Signature, Authentication	Textual Password, Authentication
User 1	35 sec	29 sec	6 sec	6 sec
User 2	39 sec	30 sec	6 sec	7 sec
User 3	49 sec	55 sec	7 sec	10 sec
User 4	55 sec	58 sec	9 sec	12 sec

In order to test the security robustness of the proposed authentication algorithm we performed our secret gestures publicly in order for other users to try them for us, as a form of shoulder surfing attack. The following results indicate why the rest of the users could not imitate our private 3D gesture password. No unauthorized user could use our 3D signature in order to authenticate himself on behalf of us.

Table 3. Shoulder surfing attacks results for five authentication parameters, (X: fail, √: success)

User	User 1					User 2					User 3					User 4				
	Par 1	Par 2	Par 3	Par 4	Par 5	Par 1	Par 2	Par 3	Par 4	Par 5	Par 1	Par 2	Par 3	Par 4	Par 5	Par 1	Par 2	Par 3	Par 4	Par 5
User 1						X	X	X	√	X	X	X	√	√	X	√	X	√	√	X
User 2	X	X	X	√	X						X	X	X	√	X	X	X	√	X	X
User 3	X	X	√	X	X	X	X	√	X	X						X	X	√	X	X
User 4	X	X	X	X	X	X	X	X	X	X	√	X	X	X	X					

With the help of this test interesting conclusions where made as far as which parameter of the authentication algorithm was more prone to attacks. The starting sensor position (*Parameter 3*) and ending sensor position (*Parameter 4*) where imitated in more than one occasions by unauthorized user, while non static parameters in terms of motion were not imitated due to lack of muscle memory. Elapsed time for signature completion (*Parameter 1*) was also imitated more than one occasion as it can be easily calculated. Although parts of the authentication algorithm were imitated by unauthorized users the algorithm can be considered robust to shoulder surfing attacks in comparison to textual authentication techniques which would have surely failed.

7 (Re)-Usability Tests and Results

The (Re)-Usability tests where designed in order to prove that the proposed authentication method can be user friendly and at the same time provide a sufficient substitute

for textual passwords but without their drawbacks. Great effort was made in order to prove that user can remember a 3D password after a sufficient period of time and tested the results against a strong 8 digit textual password.

In the first test the users chose a never used before 3D password and a strong textual password. They authenticated themselves one time per day for five days in a row. After that period they stopped using their passwords for two weeks and then were asked to authenticate once more.

The results on *Table 4* depict a slightly better hit ratio when using a 3D password.

Table 4. Easier to remember, (X: no, √: yes)

User	3D Signature	Textual Password
User 1	√	√
User 2	√	√
User 3	√	X
User 4	X	X

8 Conclusions and Future Work

In this paper, we have proposed a unique user authentication technique based on gesture recognition and a tri-axis accelerometer and presented basic usability results thought our SquWiigle implementation. With the proliferation of low power, low cost accelerometers, we believe that accelerometer and gesture-based user authentication has the potential to enable personalized services on resource constrained mobile devices, and to that direction we are investigating a variety of applications such us mobile payments, serious games and in gaming in general. Considering existing open research issues, we believe that further feature analysis of 3D axis acceleration along with more sophisticated solutions in handwritten signature forensics, and adaptive solutions to personalize the rejection threshold can help achieve more effective and usable gesture-based authentication. To this direction we are planning a thorough series of experiments with more users evaluating the proposed method in order to get safer results considering the usability and robustness of the method.

References

1. Haghighi, A.P., McCabe, B.D., Fetter, R.D., Palmer, J.E., Hom, S., Goodman, C.S.: Retrograde control of synaptic transmission by postsynaptic CaMKII at the Drosophila neuromuscular junction. Neuron 39, 255–267 (2003)
2. McCabe, B.D., Marques, G., Haghighi, A.P., Fetter, R.D., Crotty, M.L., Haerry, T.E., Goodman, C.S., O'Connor, M.B.: The BMP homolog Gbb provides a retrograde signal that regulates synaptic growth at the Drosophila neuromuscular junction. Neuron 39, 241–254 (2003)
3. Muscle Memory, Dow 207 (1), 11, Journal of Experimental Biology, http://jeb.biologists.org/cgi/content/full/207/1/11

4. Osborn, A.S.: Questioned Documents, 2nd edn. Boyd Printing Company, New York (1929) (Reprinted Nelson-Hall Co., Chicago)
5. Liu, J., Wang, Z., Zhong, L., Wickramasuriya, J., Vasudevan, V.: uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications. In: Proc. IEEE Int. Conf. Pervasive Computing and Communication, PerCom (2009)
6. Hofmann, F.G., Heyer, P., Hommel, G.: Velocity Profile Based Recognition of Dynamic Gestures with Discrete Hidden Markov Models. In: Proc. Int. Wrkshp. Gesture and Sign Language in Human-Computer Interaction (1997)
7. Jang, I.J., Park, W.B.: Signal Processing of the Accelerometer for Gesture Awareness on Handheld Devices. In: Park, W.B. (ed.) Proc. IEEE Int. Wkshp. Robot and Human Interactive Communication, pp. 139–144 (2003)
8. Kela, J., Korpipää, P., Mäntyjärvi, J., Kallio, S., Savino, G., Jozzo, L., Marca, D.: Accelerometer-based gesture control for a design environment. Personal Ubiquitous Computing 10, 285–299 (2006)
9. Payne, B.D., Edwards, W.K.: A Brief Introduction to Usable Security. IEEE Internet Computing 12, 13–21 (2008)
10. Maltoni, D.: Handbook of fingerprint recognition. Springer, Heidelberg (2003)
11. Zhao, W., Chellappa, R., Phillips, P.J., Rosenfeld, A.: Face recognition: A literature survey. ACM Computing Surveys 35, 399–458 (2003)
12. Wildes, R.P.: Iris Recognition: an Emerging Biometric Technology. Proc. IEEE 85, 1348–1363 (1997)
13. Campbell Jr., J.P.: Speaker Recognition: a Tutorial. Proc. of the IEEE 85, 1437–1462 (1997)
14. Impedovo, D., Pirlo, G.: Automatic signature verification: the state of the art. IEEE Trans. on Systems, Man, and Cybernetics, Part C: Applications and Reviews 38, 609–635 (2008)
15. Okumura, F., Kubota, A., Hatori, Y., Matsuo, K., Hashimoto, M., Koike, A.: A Study on Biometric Authentication Based on Arm Sweep Action with Acceleration Sensor. In: Proc. Int. Symp. Intelligent Signal Processing and Communications (2006)
16. Farella, E., O'Modhrain, S., Benini, L., Riccó, B.: Gesture Signature for Ambient Intelligence Applications: A Feasibility Study. In: Fishkin, K.P., Schiele, B., Nixon, P., Quigley, A. (eds.) PERVASIVE 2006. LNCS, vol. 3968, pp. 288–304. Springer, Heidelberg (2006)
17. Matsuo, K., Okumura, F., Hashimoto, M., Sakazawa, S., Hatori, Y.: Arm Swing Identification Method with Template Update for Long Term Stability. In: Proc. Int. Biometrics (2007)
18. Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.M., Ailisto, H.A.: Identifying Users of Portable Devices from Gait Pattern with Accelerometers. In: Proc. of IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP), vol. 2, pp. ii/973–ii/976 (2005)
19. Duche, G., Wiiuse, J.: `http://code.google.com/p/wiiusej/`