A STUDY ON USER AUTHENTICATION BASED ON ARM MOVEMENTS USING AN ACCELERATION SENSOR

Madoka Hasegawa, Daisuke Someya, Yuichi Tanaka, Shigeo Kato

Dept. of Information Systems Science,
Graduate School of Engineering, Utsunomiya University

E-mail: {madoka@, someya@mclaren., tanaka@, kato@}is.utsunomiya-u.ac.jp

ABSTRACT

In this paper, we study a user authentication method using a handy controller with a built-in acceleration sensor. For the authentication, a user draws a figure in the air with holding the controller. If the captured data by the acceleration sensor during moves of his/her arm are matched with user's data stored in the system, the user can access the system. Although drawing a figure in the air is easy and convenient for logging on to video games and applications in mobile terminals, this method is vulnerable against observation attack because user's movement is observable. Attackers may success in impersonating the movement.

To solve this problem, we utilize both of log data of the acceleration sensor while drawing a mark and movement to press/release a button behind the controller. Observing the motion to press/release the button is difficult for attackers. This method is expected to be stronger than the former method against the impersonation attack.

Index Terms— user authentication, acceleration sensor, behavior-based approach, security.

1. INTRODUCTION

Recently, various personal data are stored in user's mobile terminals such as mobile phones and PDAs. If a user loses his/her terminal on the street, his/her personal information stored in it may be easily stolen and abused by a third person. Although passwords or PINs are used for protecting the data, typing them with small buttons is not usable and sometimes user needs to switch language input method to type secure password with numbers, alphabets, and symbols. Some mobile phones have biometrics recognition [1], such as finger print and face recognition. However, Matsumoto reported finger print is not safe enough [2]. Face recognition takes time for starting and operating camera. A more secure and usable authentication method for portable devices is still desired.

An authentication method using user's arm movement captured by an acceleration sensor is one of the good candidates as an authentication method which is suitable for the mobile terminal because the method is quicker and easier than typing PINs or passwords. This method can be classified into the behavior-based authentication as shown in Figure 1. Recent Japanese mobile phones have a motion sensor and several researchers have started studies on the authentication method based on users' arm movements [3], [4]. In their authentication, a user is verified by matching his/her pre-registered acceleration data of his/her motion with the captured acceleration data. It is not easy to correctly imitate other person's motion, and it makes impersonation difficult. However, there are some possibilities that the user fails the authentication because the pre-registered motion was too complicated or a third person succeeds the authentication due to too simple pre-registered motions. A secure and usable behavior-based authentication method with a simple user interface is desired.

To solve this problem, we study on a behavior-based authentication method which combines log data of the acceleration sensor and movement to press/release a button on the mobile device. Observing the motion to press/release the button is difficult for attackers. We built a prototype system of our method using a Nintendo's Wii Remote controller. This paper reports on a user study to evaluate false rejection rate (FRR) and false acceptance rate (FAR) of this system.

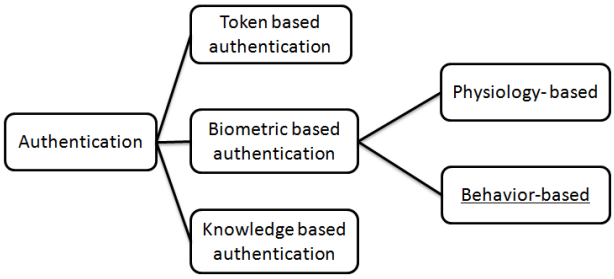


Figure 1. Classification of Authentication Method

2. SYSTEM OVERVIEW

Figure 2 shows overview of our system. Our authentication system is installed in a PC and a Wii remote controller is connected via Bluetooth. When a user draws a figure with

holding the controller, its acceleration data are transmitted to the system in real time.

Figure 2. System Overview

The acceleration sensor in the controller is a 3-axis sensor and its coordinate system is shown in Figure 3. Sampling rate of the sensor is 100Hz.

On the back side of the controller, there is a button called B-button (Figure 4). We used this button to control duration for capturing acceleration data.

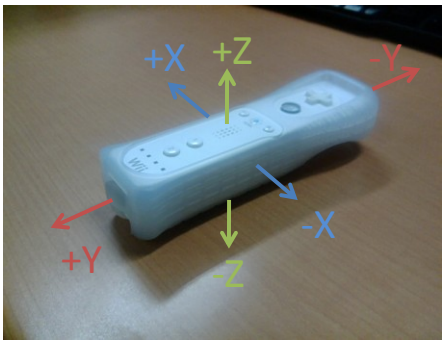


Figure 3. Coordinate System of Acceleration Sensor

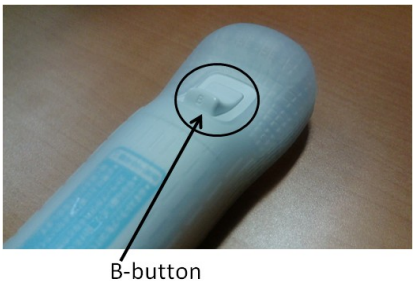


Figure 4. Back side of controller

Figure 5 shows examples of acceleration data of drawing a triangle. As shown in Figure 5 (b), if a user released the B-button in the middle of the path, data are not captured and data become different from Figure 5 (a). Unless precisely imitating the timing of pressing/releasing this button, attacker cannot success the authentication. In addition, the button is too small to notice if the user is pressing/releasing it when the controller is moved for drawing a figure.

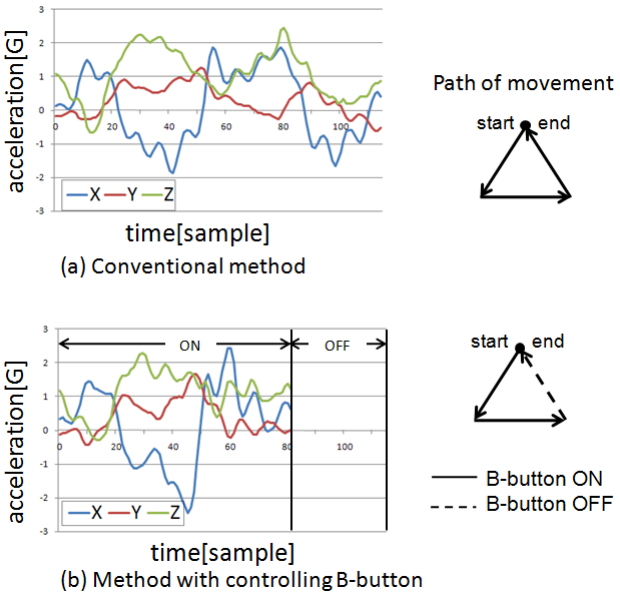


Figure 5. Examples of Acceleration Data
(Top: User kept pressing B-button while drawing a triangle, Bottom: User released B-button while drawing the last side of a triangle.)

3. ALGORITHM OF AUTHENTICATION USING ACCELERATION DATA

3.1. DP matching of Acceleration Data

In our system, DP matching scheme is used to compare two sequences of different length based on dynamic programming algorithm which solves complex problems by breaking them down into several simpler steps. Captured acceleration data is a sequence of three-dimensional signals of (X, Y, Z) coordinates. The acceleration sensor can measure force of ± 3G for each axis. Length of the sequence slightly varies in each authentication, even if a user tries to draw same figures. Therefore, the DP matching is suitable for evaluating difference of sequences of acceleration data.

Assume $\mathbf{A} = \{A_1, A_2, ..., A_i, ..., A_I\}$ and $\mathbf{B} = \{B_1, B_2, ..., B_j, ..., B_J\}$ are sequences of acceleration data where A_i is the i-th three-dimensional signal in the sequence $\mathbf{A}$. A_i consists of (A_{ix}, A_{iy}, A_{iz}). In the same way, B_j means the j-th signal in the sequence $\mathbf{B}$. Length of each sequence is denoted as I and J, respectively.

Difference $D(\mathbf{A}, \mathbf{B})$ between $\mathbf{A}$ and $\mathbf{B}$ is calculated by following steps:

Step1: Normalization

Normalize acceleration data by dividing by the maximum absolute value in the sequence. For example, if the absolute value of the z-axis of 5-th data $|A_{5z}|$ is the maximum in the sequence A, all data is divided by $|A_{5z}|$. Therefore, the nor-

malized value of the acceleration data is always mapped within the range from -1 to +1 after the normalization.

Step2: DP matching

Apply DP matching for Euclidean distance between two acceleration vectors. The Euclidean distance between i-th vector in the sequence **A** and j-th vector in the sequence **B** is defined by equation (1).

$$d(i,j)=\sqrt{(A_{ix}-B_{jx})^2+(A_{iy}-B_{jy})^2+(A_{iz}-B_{jz})^2} \quad (1)$$

As an initial value for DP matching, set

$$g(1,1)=2d(1,1) \quad (2)$$

where $g(i, j)$ is the minimum cost to align first i data of the sequence **A** with the first j data of the sequence **B**. This initial value means the lowest cost of the starting point is twice the distance between the two first elements.

Then, calculate $g(i, j)$ successively for each i and j.

$$g(i,j)=\min\begin{bmatrix} g(i-1,j)+d(i,j) \\ g(i-1,j-1)+2d(i,j) \\ g(i,j-1)+d(i,j) \end{bmatrix} \quad (3)$$

Finally, difference D(**A**, **B**) is obtained by dividing $g(I, J)$ with sum of length of two sequences.

$$D(A,B)=\frac{g(I,J)}{I+J} \quad (4)$$

3.2. Procedure of Authentication

Prior to the authentication, a user draws his/her key figure N times and these acceleration data are registered as his/her master data M_i in the system (i = 1, .., N). The system computes sum of squared difference between k-th master data and others by equation (5).

$$S_k=\sum_{l=1}^{N} D^2(M_k,M_l) \qquad (for \quad l\neq k) \quad (5)$$

where $D(M_k, M_l)$ is difference between M_k and M_l obtained by the DP matching after normalizing amplitude of M_k and M_l. One of M_i's which gives the minimum S_k is set as the typical master data M_m for the user.

For the authentication, the user tries to draw the same figure as his/her key figure once and its acceleration data A is recorded. Figure 6 and Figure 7 show an overview of the authentication procedure and its flow diagram. The amplitude of data A is normalized to compare with the master data M_m. Then, the DP matching is applied to the normalized A and M_m for calculating difference $D(A, M_m)$. If $D(A, M_m)$ is smaller than a threshold T, the user is accepted as a legitimate user. The threshold T is defined by following equation.

$$T=\mu+a\sigma \quad (6)$$

where μ is the average and σ is the standard deviation of $D(M_m, M_l)$ ($l\neq m$) which is difference between the typical master data M_m and other master data. The parameter "a" is used for controlling sensitivity of the system. For smaller a, FRR will be greater and FAR will be smaller.

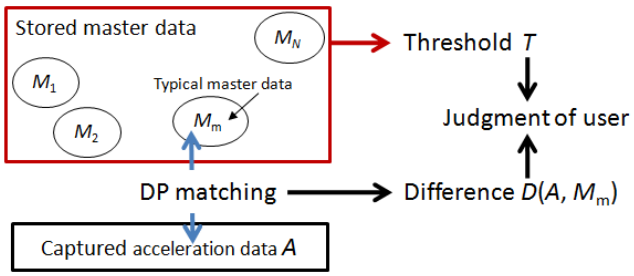


Figure 6. Overview of Authentication

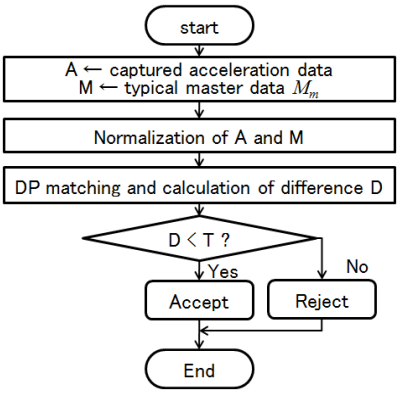


Figure 7. Flow Diagram of Authentication

4. USER STUDY AND ITS RESULT

4.1. Environment and Conditions

We conducted a user study to evaluate FRR and FAR of our system. The number of participants is 17. All participants are 20's male students. The participants held the controller with their dominant hand for drawing their key figures. There are 15 right-handed participants and 2 left-handed ones.

Prior to the authentication, experimenter gave participants instruction on the procedure of the user test and the usage of the controller. Then, participants arbitrary decided a figure and registered it as their key. After that, they tried logging-in using the key figure 5 times to evaluate FRR. We recorded movements on video from in front of the participants during the authentication. The environment of the user test room is shown in Figure 8.

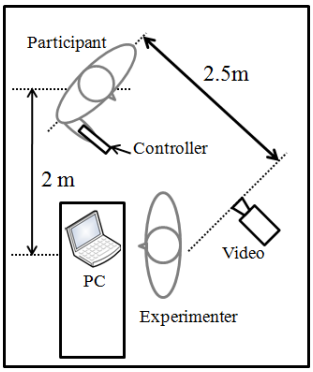


Figure 8. Environment of User Test

To evaluate FAR, participants tried to impersonate one of other participants which is decided by the experimenter. In advance of the trial, participants repeatedly watch movements of a target user on video until they can imitate the movements. After that, they tried logging-in 5 times to impersonate the target user.

4.2. Result

Figure 9 shows result of the user study. The range of the sensitivity parameter a is [0.0:9.9]. FFR and FAR are the average values for all participants.

The equal error rate (EER), which is the cross-point of FFR and FAR, is about 3.5% for a = 4.7. EERs of other behavior-based authentications are around 2 to 8 % [4]. Therefore, our system is very comparable to these methods.

After the test, we asked the participants to fill out the questionnaire about the impersonation test. All of them answered they could not know when the B-button was pressed/released from the video; therefore, they conjectured the timing to control the B-button.

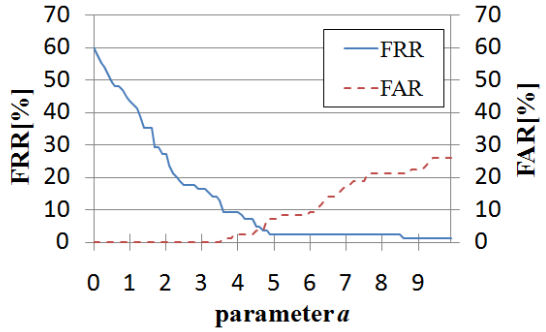
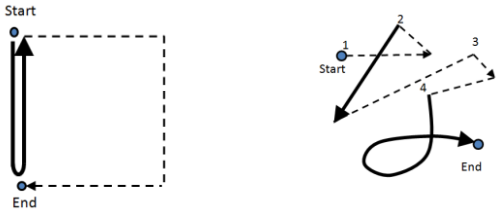


Figure 9. FRR and FAR

Figure 10 shows examples of registered key figures. Both of FFR and FAR was low for Figure 10 (a). On the contrary, FFR was high and FAR was low for Figure 10 (b). These results imply that the combination of simple key lines and complex dummy lines is suitable for authentication. However, if the key figure is too complex, it becomes difficult to reproduce the same movement even though it is the legitimate user.



(a) Sample1 (b) Sample2

Figure 10. Registered Key Figures
(Solid line: B-button on, Dotted line: B-button off)

5. CONCLUSIONS

We proposed a user authentication method using a handy controller with a built-in acceleration sensor to enhance usability of the authentication for mobile devices. The result of user study shows the security of our method is equal to the existing method.

Future works include the following issues:

- Detailed user study on usability and memorability of arm movements in the longer term tests.
- Detailed user study on impersonation with more participants.
- Study on reducing FRR by improving DP matching and updating acceleration data.
- Implementation on a mobile phone.

ACKNOWLEDGEMENT

This work was supported by the Grant-in-Aid for Scientific Research (C) 22500105 from Japan Society for the Promotion of Science.

REFERENCES

[1] Kresimir Delac, Mislav Grgic, "A Survey of Biometric Recognition Methods," *46th International Symposium Electronics in Marine*, 2004.

[2] Bruce Schneier, "Fun with Fingerprint Readers," http://www.schneier.com/crypto-gram-0205.html#5

[3] S. Ishihara, M. Ohta, E. Namikata, T. Mizuno, "Individual Authentication for Portable Devices Using Motion of the Devices," *Journal of Information Processing*, Vol.46, No.12, pp.2997-3007, Dec. 2005. (in Japanese)

[4] K. Matsuo, F. Okumura, M. Hashimoto, A. Koike, A. Kubota, Y. Hatori, "Arm Swing Identification Method with Template Update for Long Term Stability," *The transactions of IEICE*, Vol.J91-B, No.6, pp.695-705, June 2008. (in Japanese)

[5] Anil K. Jain, Ruud Bolle, Sharath Pankanti, "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.