A Study on Biometric Authentication based on Arm Sweep Action with Acceleration Sensor

Fuminori Okumura*, Akira Kubota*, Yoshinori Hatori*,
Kenji Matsuo†, Masayuki Hashimoto†, Atsushi Koike†
*Department of Information Processing,
Tokyo Institute of Technology, Yokohama, 226-8502, Japan
E-mail: {fuminori.okumura, kubota, hatori}@ip.titech.ac.jp
†Visual Communication Laboratory,
KDDI R&D Laboratories Inc., Kamifukuoka, 356-8502, Japan
E-mail: {matsuo, masayuki, koike}@kddilabs.jp

Abstract— **A new biometrics authentication method for cellular phones which has an advantage of simple and natural operation is proposed. The proposed method authenticates owner using acceleration signals obtained by an acceleration sensor embedded in the cellular phones during his arm sweep action. When the owner wants to unlock its security, he just needs to grasp and shake his cellular phone. The proposed method verifies owner's acceleration signals by using a DP-matching algorithm which can adapt fluctuations caused by different grip. Simulation results show that the proposed method can achieve the best equal error rate 5.0% for 22 testers.**

I. Introduction

Cellular phones are indispensable to our daily life. Its security systems to verify the owner are playing an important role, because the devices contain private data. The private data include the owner name and phone numbers, personal schedules. In addition, recently cellular phones are used in various applications such as online shopping and stock trading (especially in Japan, paying in prepaid using non-contact type IC chip). The most popular method for user authentication is a simple way of inputting 4-digit PIN-code. This system is not robust, because we can break its security by inputting PIN-code 10,000 times at the most. Actually, it would be possible with much fewer trials, when PIN-codes are set to the numbers related to their personal information (e.g. their birthday, birth year, or a part of their phone number).

Currently there are some cellular phones with new authentication systems using 8-digit PIN-code and biometrics authentications based on fingerprints or face images. Such systems are much robuster than the conventional system using 4-digit PIN-code. However these security systems are not always convenient to use; for the 8-digit PIN-code system, we have to memorize and input longer and complex numbers; for biometrics authentications systems, we need to sweep our finger on the sensor or to take our face images with camera every time when we want to unlock the security. Most existing security systems require such inconvenient operations.

In this paper, we propose a new biometrics authentication method with easier and more natural (convenient) operation for cellular phones. Our method verifies the owners by analyzing their simple arm sweep actions.

II. Authentication based on Arm Sweep Action

There are various kinds of authentication methods shown in Table I. Compared with others, our authentication method has a great advantage in following points.

First, its operation is especially simple and easy. Most security systems require complex operations and/or specific devices to verify the users. For example, PIN-code needs to be

Table I Type of Authentications

	Accuracy of Authentication	Convenience of Operation	Resistance for Authentication	Danger of Imitation	Harmful Effect of Leakage	Device
non-Biometric Authentication						
PIN-code (4-digit)	HIGH	middle	LOW	high	NONE	keyboard
Biometric Authentication (using physical feature)						
Fingerprint	HIGH	middle	high	high	LOW	sensor
Face Image	low	middle	high	middle	high	camera
Retina	HIGH	low	high	LOW	high	camera, sensor
DNA	HIGH	low	high	high	high	large device
Biometric Authentication (using behavioral feature)						
Voice	low	HIGH	LOW	middle	LOW	mic
Signature	low	middle	LOW	LOW	LOW	tablet, sensor
Arm Sweep Action	low	HIGH	LOW	LOW	LOW	acceelation sensor

0-7803-9733-9/06/$20.00©2006 IEEE

input by hitting keyboards several times. Fingerprint authentication needs finger sweep action on the sensor, and we have to take our face photos in face images authentication. In our proposed system, we just need to grasp and shake cellular phones. This advantage is especially important for cellular phones. This is because, in the conventional system, even if all devices have a PIN-code security, most people do not lock their cellular phones due to inconvenient (troublesome) operations.

The second advantage of our authentication is that there is no risk of leaking out our personal features or information. Biometric authentications generally use personal features, for example, fingerprints, face images, voices, retinas, DNA, and shapes of hands. In case of leakage of data from DNA security system for instance, our blood type, color of skins and eyes, and medical history are revealed. In contrast, arm sweep actions offer no personal important features in our authentication system.

In addition, it seems that people have less resistance in our authentication than in other biometric authentications. For example, some people have a strong resistance against face images authentication, because they have to consciously take our face photos every time.

Finally, this authentication is strong against injustice and malicious imitation. It is well known that we can counterfeit someone else using artificial finger made of gelatin in fingerprint authentication [1] or using someone's hair in DNA certification. In our research, we confirmed that although all of testers just shake sensors in the same arm sweep action, their actions were distinguishable with 5% of the best equal error rate.

Our authentication method verifies owners using acceleration signals obtained with an acceleration sensor embedded in the cellular phones during their arm sweep action. There are only a few research works in this biometric authentication field using acceleration sensors related to our work [2]. Our research work is quite different from other works in the simplicity of the verifying action. The action used in Ishihara's work [3] is a complex action of writing a signature in the air. In contrast, the action needed in our method is just shaking the sensor up and down, as described in next chapter.

III. Experimental setup and preprocessing

Let us first explain the experimental setup we performed. We used an acceleration sensor which size is almost the same size of cellular phone, so that we can grasp it just as we usually hold cellular phones (see Figure. I). The acceleration sensor can record a three-dimensional acceleration signal in x, y, and z-axis defined in this sensor. The acceleration signals are recorded with 100 Hz sampling frequency. Testers shake this device in wireless without physical constraints because it works with electric batteries and records acceleration signals in its own memory. The acceleration data can be taken out to PC through USB cable and analyzed. The specification of the acceleration sensor is shown in Table II.

TABLE II SPEC OF ACCELERATION SENSOR

size of device	75(h) * 60(w) * 32(d) mm
weight of device	115 g
channel of sensor	3 axes (x, y, and z-axis)
range of sensor	-10G~+10G
sampling rate	100Hz
measurement error	±10%

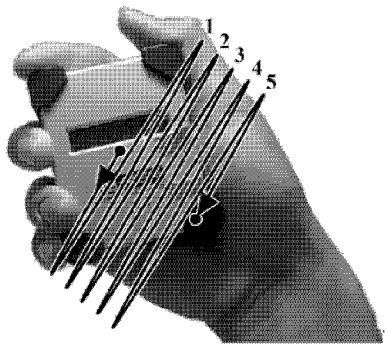

FIGURE I THE ARM SWEEP ACTION IN EXPERIMENTS

The number of testers was 22, all are adults and right-handed. Testers had a following trial; grasp the device in the same way and shake it simply up and down in the direction of y-axis 5 times continuously. The way of shaking is shown in Figure I. We instructed them how to shake but didn't prescribe the time length of the action. This trial was repeated 5 times for each tester. As a result we acquired 110 series of acceleration signals.

The following three preprocessing steps are required.

- Extracting signal in sweep action

We extract signal between the first and the last (fifth) minimum value of the obtained acceleration signals in y-axis, shown in Figure II. Because the acceleration sensor records signals all the time, and the time length of each action is severally different. Hence, we need to extract the exact motion period. Testers shake the device almost along y-axis, so that the acceleration signals of y-axis significantly changed compared with other two signals.

In the process of finding minimum values, we had to pay attention to some minimum values which are close to each other. Accordingly, we ignored the minimum values which came after another one within 0.1 ms.

As a result, the length of extracted data was around 2~3 sec.

- Normalization of the acceleration signal

In the next step, we normalized the acceleration signals. The signals are always affected by gravity. The direction of gravity affect the signals are always changing, because the axes of the sensor are always changing during the arm sweep action.

To remove the influence of gravity, we calculate

$$\boldsymbol{a}_i' = \boldsymbol{a}_i - \hat{\boldsymbol{a}}, \qquad (1)$$

where $\boldsymbol{a}_i$ and $\boldsymbol{a}_i'$ are acceleration signals before and after the normalization respectively, and $\hat{\boldsymbol{a}}$ is an average of $\boldsymbol{a}_i$.

- Normalization of the data length

Finally, we normalized the time length of data so that we can compare all data having different time length. In this process, we used a simple normalization based on linear interpolation. We normalized the time length to be 300 frames (the original data lengths ranged 200-300 frames).

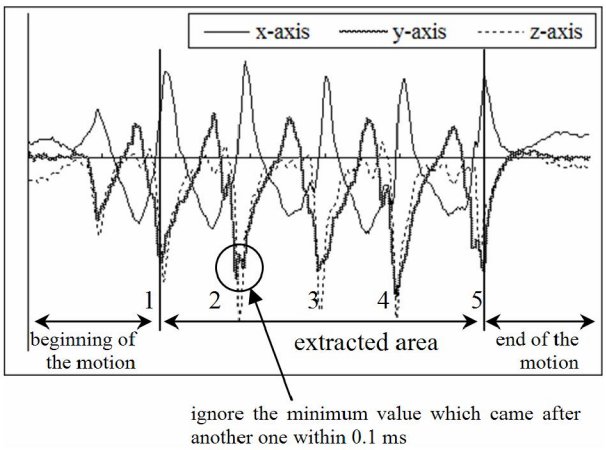

FIGURE II PREPROCESSING : EXTRACTION OF MOTION PERIOD

IV. VERIFYING METHODS AND RESULTS

After preprocessing steps, we analyzed the acceleration data using squared error of Euclidean distance, error of angle, and DP-matching with the error of angle. The last analysis is our proposed method. We chose one data as registration data (owner's data) and verified it with all other data: owner's other 4 data and 21 others' 5 data. We processed these verifying methods for all data, i.e., 11990 (= 109 * 110) pairs of comparison.

A. *Squared Error of Euclidean Distance*

In this process, we verified the similarity between acceleration data using a sum of squared error of Euclidean distance frame by frame (see Figure III):

$$e_{ab} = \sum_i d_i^2 = \sum_i \|\boldsymbol{a}_i - \boldsymbol{b}_i\|^2 \qquad (2)$$

If e_{ab}, a difference between acceleration signals $\boldsymbol{a}$ and $\boldsymbol{b}$, was less than predetermined threshold, we decide the acceleration signals $\boldsymbol{a}$ and $\boldsymbol{b}$ were from the same person's trials.

Applying this method, we achieved the best equal error rate (EER) 24.1%, which is very high and cannot be used for authentication.

B. *Error of Angle*

Instead of error of distance, we used error of angle between acceleration vectors (see Figure IV):

$$e_{ab} = \sum_i \omega_i = \sum_i \left| \arccos\left(\frac{\langle \boldsymbol{a}_i, \boldsymbol{b}_i \rangle}{\|\boldsymbol{a}_i\| \|\boldsymbol{b}_i\|} \right) \right| \qquad (3)$$

The motivation for using error of angle is based on our assumption that personal feature appears more significantly in the direction of sweep action than in the intensity. The achieved the best EER was 15.6% and lower than the above verification EER. However it is not low enough for better authentication.

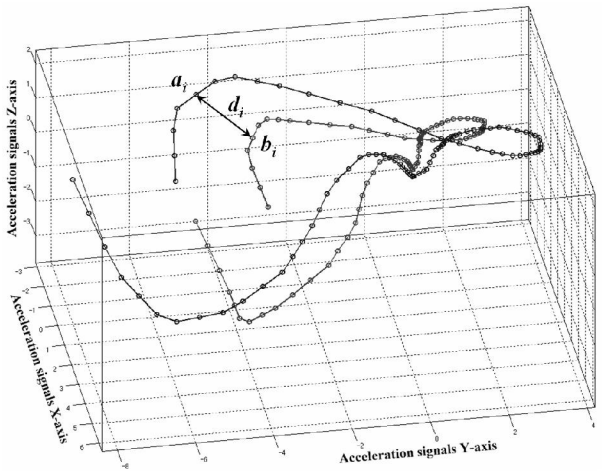

FIGURE III SQUARED ERROR OF EUCLIDEAN DISTANCE

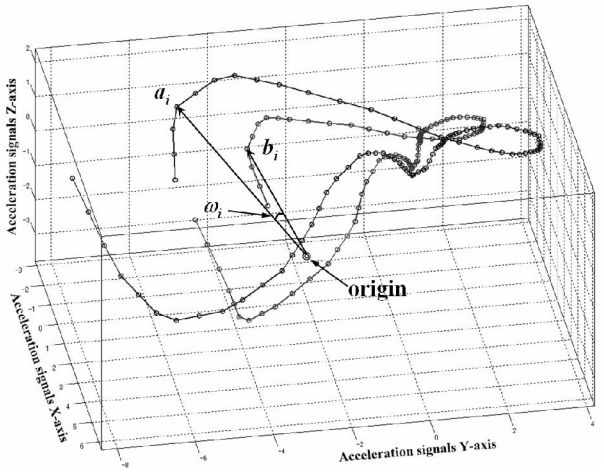

FIGURE IV ERROR OF ANGLE

C. *DP-matching using Error of Angle*

We adopted a DP-matching, Dynamic Programming-matching, which is a well-known matching algorithm for computing similarity between series of data using a route searching [4]. There are two parameters in this algorithm, an entrance penalty and a toll penalty. An entrance penalty is a similarity of two signals at each matching point, and a toll

penalty is a weight of route searching. Our method uses error of angle as an entrance penalty. The toll penalty was set to 0.65, which was the best value we found through many trials.

$$e_{ab} = score(I-1, J-1) \tag{4}$$

$$score(i,j) = min\begin{bmatrix} score(i-1,j-1)+err(i,j) \\ score(i,j-1)+err(i,j)+toll \\ score(i-1,j)+err(i,j)+toll \end{bmatrix} \tag{6}$$

$$score(0,0) = err(0,0)$$

$$score(0,j) = score(0,j-1)+err(0,j)+toll$$

$$score(i,0) = score(i-1,0)+err(i,0)+toll$$

$$err(i,j) = \left| arccos\left(\frac{\langle \boldsymbol{a}_i, \boldsymbol{b}_j \rangle}{\|\boldsymbol{a}_i\| \|\boldsymbol{b}_j\|} \right) \right| \tag{5}$$

$$0 \le i < I, 0 \le j < J$$

where I and J is the number of frames in acceleration signals $\boldsymbol{a}$ and $\boldsymbol{b}$, and $toll$ is toll penalty.

The achieved the best EER was 5.0%, much improved compared with above two methods. Although this rate is not still enough for accurate authentication; however it should be noted that this rate was achieved from data of simple and same sweep actions, showing a possibility to achieve lower rate when introducing other type of sweep actions.

V. Conclusions and Future work

The results of our experiments with 22 testers showed that our biometric authentication based on arm sweep action with acceleration sensor is possible and promising to be a new type of authentication system. It also showed that the personal differences typically appear in the direction of the action rather than in the intensity. We consider this result is mainly due to our physical differences of a wrist snap and an arm length. Although there were differences in timing of sweep action even if the same person tried, we could deal with this problem using DP-matching.

As future work, we would develop more robust algorithm to achieve EER of 1%. To evaluate such reliable algorithm, we need perform experiment with at least 300 testers, according to the "Rule of 3". We also want to take into account other feature quantities such as velocity and the frequency domain features.

Acknowledgment

The three authors with Tokyo Institute of Technology thank to the Telecommunication Advancement Foundation (TAF) in Japan for the support.

References

[1] M. Une, T. Matsumoto, IMES Discussion Paper Series No.2005-J-2, Institute for Monetary and Economic Studies Bank of Japan.

[2] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S. Mäkelä, H. Ailisto, "IDENTIFYING USERS OF PORTABLE DEVICES FROM GAIT PATTERN WITH ACCELEROMETERS", ICASSP '05, Vol.2, March 18-23, 2005. Vol.2 (2005), pp. 973-976, Oulu / Finland.

[3] M. Ohta, E. Namikata, S. Ishihara, T. Mizuno, "Individual Authentication for Portable Devices using Motion Features", *proc. of the 1st International Conference on Mobile computing and Ubiquitous networking (ICMU2004)*, pp. 100-105, 2004-1, Yokosuka / Japan.

[4] S. Hangai, S. Yamanaka, T. Hamamoto, "ON-LINE SIGNATURE VERIFICATION BASED ON ALTITUDE AND DIRECTION OF PEN MOVEMENT", Proc. of IEEE ICME, vol.1, pp.489-492, (2000) 34.