2022 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2022, Virtual, December 12-15, 2022

# Biometric Authentication based on Unconscious Arm Swing Action with Acceleration Sensor

Motoharu Nakajima†, Jousuke Kuroiwa†, Tomohiro Odaka† and Izumi Suwa‡

†Graduate School of Engineering, University of Fukui
3–9–1 Bunkyo, Fukui, 910-8507, Japan
‡School of Life Science, Women's College of Jin-ai
43–1–1 Amaikecho, Fukui, 910-0124, Japan
Email:jou@u-fukui.ac.jp

**Abstract**—
In this paper, we investigate a simple and robust personal authentication method for smartphone applications. In conventional authentication method of smartphone, PIN with 4 or 8 digits, facial image or fingerprint, or pattern lock is employed. Unfortunately, these authentication is not robust. Therefore, we focus on arm swing actions which are unconscious. The purposes of this paper are (i) to present a novel authentication method based on their characteristic features, and (ii) to show the authentication ability of the method. From the computer evaluations, in the case of the best accuracy, both the false acceptance rate (FAR) and the false rejection rate (FRR) are 0%. In the worst cases, the FAR was 6% and all the FRRs are less than or equal to 10%. The results suggest that the proposed personal authentication method based on arm swing actions is quite robust and practical.

## 1. Introduction

Smartphones enrich our lives by providing services in various fields. However, they are targets of malicious attacks because they store important personal information such as photos, contact lists, and bank accounts. To prevent such attacks, we have applied a secure personal authentication method for smartphones. PIN codes and passwords are often used as personal authentication. However, short and simple strings would introduce the information leakage, on the other hand, long strings are burdensome for us.

To solve this problem, biometric authentication is proposed in considering usability and security. For biometric authentication, information about the human body or human behavior is conventionally employed. However, since information about the human body, for instance, facial image, fingerprint, and so on, is static, information leakage would often happen in our lives.

In contrast, it is hard to steal unconscious dynamical characteristics latent in human behavior.

Among human behaviors, arm swing actions are suited for personal authentication methods for smartphones, and it has been shown that personal characteristics are latent in the actions [1]. Unfortunately, the usability is not so high and not applicable for smartphone authentication since the arm swing action in the paper is indicated. A scheme for unlocking of a smartphone by simply shaking the phone with a Supporting Vector Machines (SVM) classifier allows customized shakes and single-hand operations [2]. However, it is unable to eliminate spoof authentication completely.

In this paper, we focus on an authentication method based on arm swing actions freely. At first, we measure free arm swing action with a smartphone and construct an original data set. Based on the data set, we investigate a novel authentication method with standardized Euclidean distance among several feature values. Therefore, the purposes of this paper are (i) to present a novel authentication method based on their characteristic features, and (ii) to show the authentication ability of the method.

## 2. Authentication Method based on Unconscious Arm Swing Action

### 2.1. Acceleration Signal Collection

At the first step of the investigation, we have recorded three dimensional acceleration signals with 200 Hz sampling frequency from 6 subjects' right arm swing actions by using acceleration sensors built into a certain smartphone. The model of the smartphone is Xperia XZ2 (SO-03K) of Sony's product with Android version of 10.

At the time of recording, we specified how many times subjects swing their own right arm. The times is 2, 3, 4, or 5, and we record the signals with 20 trials per person for each specified number of times. As a result, we gained $20(\text{trials}) \times 6(\text{person}) \times 4(\text{kind}) = 480$ acceleration signals. In this paper, we divide the signal data set into the training set with the even number and test set with the odd number.

### 2.2. Data Preprocessing

The acceleration signals are too disturbed to analyze their feature points. We have performed several noise removal methods. The simple moving average method gives the best performance with the respect to the reproducing

ORCID iDs Motoharu Nakajima: 0000-0001-7825-8018, Jousuke Kuroiwa: 0000-0002-6307-5603, Tomohiro Odaka: 0000-0003-4288-5460, Izumi Suwa: 0000-0002-4625-2911

error rate. In this paper, therefore, we employ the simple moving average method to remove noise from the original acceleration signals as a preprocessing of the data.

The simple moving average method is denoted as follows:

$$\hat{s}^{(a)}(k) = \frac{1}{5}\sum_{\tau=-2}^{2} s^{(a)}(k+\tau), \tag{1}$$

where $s^{(a)}(k)$ is the acceleration signal in the $a$th direction at $k$ steps and $\hat{s}^{(a)}(k)$ is its resultant value of the simple moving average method. The window size of 5 is determined by trying various values in searching the smallest reproducing error rate. Note that $a$ takes 1, 2 and 3, indicating $x$, $y$ and $z$ direction, respectively.

### 2.3. Feature Values

In this paper, we employ two types of characteristic feature values as shown in Figure 1:

1. The first is the maximum and minimum value of each acceleration signal.
2. The last is the duration steps between the maximum and minimum values.

The $t$th extreme value of the acceleration signal for the $a$th direction denotes $m^{(a)}(t)$ $(a = 1, 2, 3)$, and the duration steps between the $t$th extreme value and $(t+1)$th one for the $a$th direction represents $m^{(3+a)}(t)$. Note that $m^{(4)}(t)$ describes between the $t$th extreme value and $(t+1)$th one of the signals for the $x$ direction.

### 2.4. Personal Authentication Methods

In this paper, we employ the standardized Euclidean distance based on the six kinds of characteristic feature values. The standardized Euclidean distance is written as follows:

$$d_{(\beta;\alpha)} = \sum_{t=1}^{n}\sum_{a=1}^{6} \frac{(m^{(a);(\beta)}(t) - \mu^{(a);(\alpha)}(t))^2}{(\sigma^{(a);(\alpha)}(t))^2}, \tag{2}$$

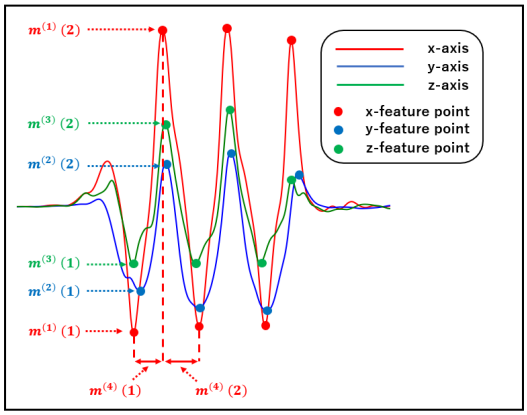



Figure 1: feature points of acceleration signals

where $m^{(a);(\beta)}(t)$ describes the $a$th feature value for the $t$th extreme value for the user of $\beta$, $\mu^{(a);(\alpha)}(t)$ represents its mean value for the user of $\alpha$, and $(\sigma^{(a);(\alpha)}(t))^2$ denotes its variance.

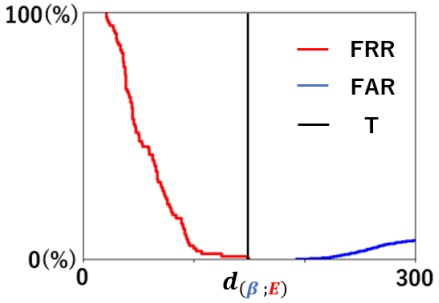
### 2.5. Determination of Threshold Value by Cross Validation

In this paper, we determine threshold values for each subject from the training data with the $k$-fold cross validation method. In the $k$-fold cross validation method, we divide the training data set into 80% of the training to evaluate threshold values and 20% for the validation. The number of the training data for each user is 10, and the possible pairs of the training and the validation data are $k = {}_{10}C_8 = 45$.

According to the $k$-fold cross validation method, we evaluate FRR (False Rejection Rate) and the FAR (False Acceptance Rate). The FRR represents the ratio that a correct user was regarded as incorrect. The FAR denotes the ratio that an incorrect user was regarded as correct. In the evaluation, we apply the signal data set with the even number for each user, which corresponds to the training set.

Figure 2(a) is the result for the user E and Figure 2(b) for the user F. In the case of Figure 2(a), the region of the distance of $d(\beta;\mathrm{E})$ where both FRR and FAR take zero is larger. In this case, we set the threshold value to be the smallest value of FRR which becomes zero. On the other hand, in the case of Figure 2(b), FRR and FAR cross each other. In this case, we set the threshold value to be the largest value of FAR which becomes zero. The rea-

(a) Result for the user E.




(b) Result of the user F.

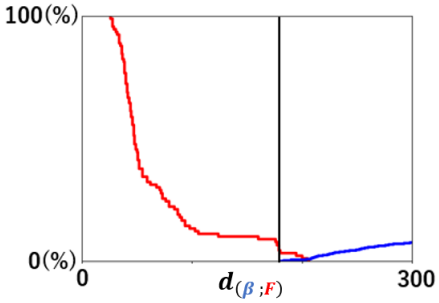



Figure 2: Results of the $k$-fold cross validation method

Table 1: Threshold values of each user.

| | 2 times | 3 | 4 | 5 |
|---|---|---|---|---|
| A | 84 | 156 | 144 | 307 |
| B | 169 | 290 | 169 | 324 |
| C | 82 | 305 | 167 | 321 |
| D | 78 | 227 | 405 | 296 |
| E | 55 | 149 | 119 | 249 |
| F | 91 | 180 | 178 | 254 |

Table 2: Authentication Results(%).

| | 2 times | | 3 times | | 4 times | | 5 times | |
|---|---|---|---|---|---|---|---|---|
| | FRR | FAR | FRR | FAR | FRR | FAR | FRR | FAR |
| A | 0 | 0 | 0 | 0 | 10 | 0 | 10 | 0 |
| B | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| C | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D | 10 | 0 | 10 | 0 | 0 | 2 | 0 | 4 |
| E | 10 | 0 | 0 | 0 | 0 | 2 | 0 | 0 |
| F | 10 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |

son is that it should avoid permitting an intruder to access to a smartphone as possible, revealing that FAR should be smaller.

## 3. Personal Authentication Experiments

### 3.1. Experiment Procedure

In the authentication experiments, the training data set is the even numbered signal and the test data set the odd numbered signal. At first, we determine the threshold value by $k$-fold cross validation method for the training data set. The threshold value for each user is given in Table 1. At the second, we evaluate the mean value of $m^{(a);(\alpha)}(t)$ and the variance of $(\sigma^{(a);(\alpha)}(t))^2$ for the $t$th extreme value and each user. At the third, we calculate the standardized Euclidean distance given by Eq.2 for all the test data. At the fourth, we classify a user whether the user is correct or not according to the threshold value. At last, we evaluate FRR and FAR according to the classification results.

### 3.2. Experiment Results

The authentication results are given in Table 2, where FRR and FAR are presented. Table 2 shows our experimental results. In the case of the swing times of 3, all the authentications by the imposters are impossible because all the FARs take zero. In the other cases, the values of FAR is sufficiently small for the authentication. All the FRR take less than or equal to 10%. Therefore, the proposed authentication method is robust and practical.

## 4. Discussions

From the viewpoint of the authentication system, the number of swing times of 3 is the most suitable because the results of FAR are important for the personal authentication. However, the worst case of FAR is 6% for the times of 2 and the user B. The value is sufficiently small however it is desirable to achieve a zero value of FAR for the authentication system of a smartphone. This point is our further problem.

At last, we consider the reason why FRR and FAR take non-zero value. We depicted the FRR-FAR curve for the test data set. The characteristical results are given in Figure 3, where the threshold value is depicted with a black straight line. In all the cases, the threshold value is inappropriate, suggesting the difficulty of the determination of the threshold value. Possibly, the difficulty comes from the definition of the standardized Euclidean distance of Eq. 2, where we do not consider the contribution ratio for each feature value except for the variance of $(\sigma^{(a);(\alpha)}(t))^2$. Then, the problem becomes impossible to linearly separate among the space of our feature values. In order to solve the problem, it is one possibility to apply SVM. Therefore, in the near future, we investigate the authentication ability with SVM.

## 5. Conclusions

In this paper, we investigate a simple and robust personal authentication method for smartphone application with unconscious dynamical characteristic features latent in human behavior. The results are as follows:

- We employ the maximum and minimum value of each acceleration signal, and the duration steps between the values as characteristic feature values.
- We present a novel authentication method with the arm swing action, where for the authentication we employ the standardized Euclidean distance based on the feature values.
- From the computer evaluations, in the case of the best accuracy, both the false acceptance rate (FAR) and the false rejection rate (FRR) are 0%. In the worst cases, the FAR was 6% and all the FRRs are less than or equal to 10%.
- The proposed personal authentication method based on arm swing actions is quite robust and practical.

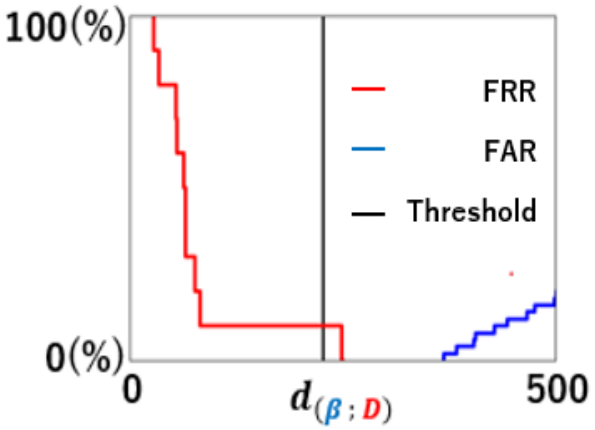
In the present experiments, we have recorded the signals in a day. The characteristic features would change after a few days. Therefore, it is a further problem to investigate the authentication ability for the signals with several intervals of days or weeks.

## References

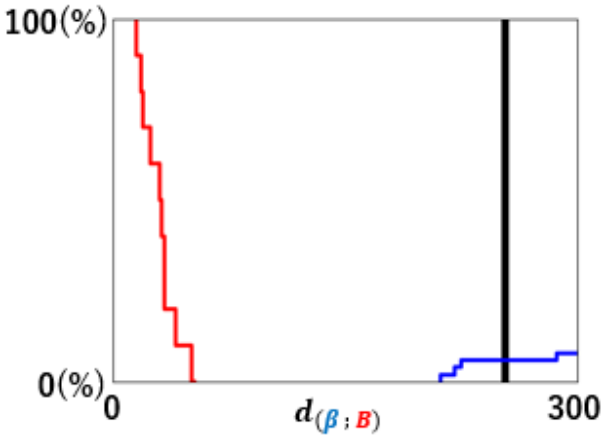

[1] O. Fuminori, K. Akira, H. Yoshinori, M. Kenji, H. Masayuki, K. Atsushi, "A study on biometric authentication based on arm sweep action with acceleration sensor," *Proc. of 2006 ISPACS*, pp.219–222, 2006.

[2] Z. Hongzi, H. Jingmei, C. Shan, L. Li, "ShakeIn: secure user authentication of smartphones with single-handed shakes," *IEEE transactions on mobile computing*, vol.16, pp.2901–2912, 2017.

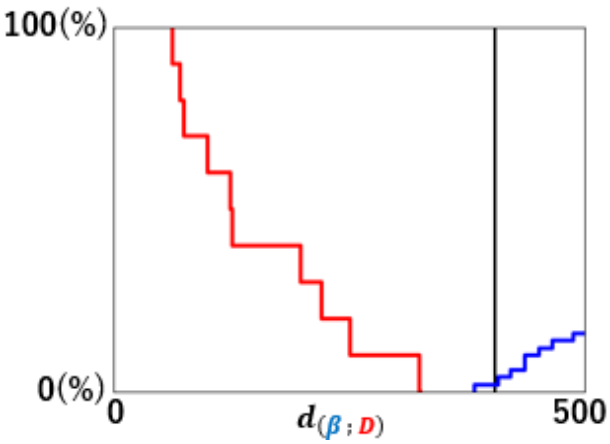
(a) Swing times of 3 and the user D.



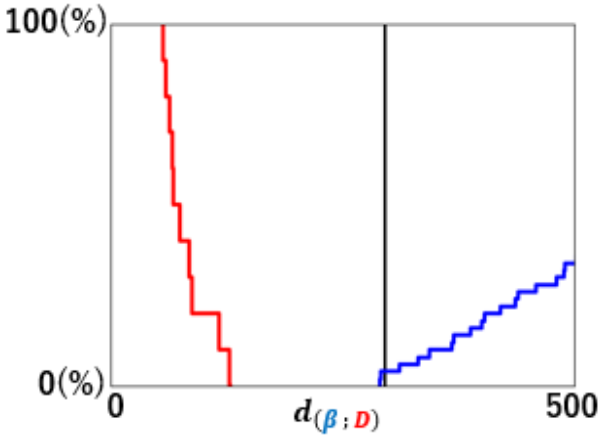

(b) Swing times of 2 and the user B.



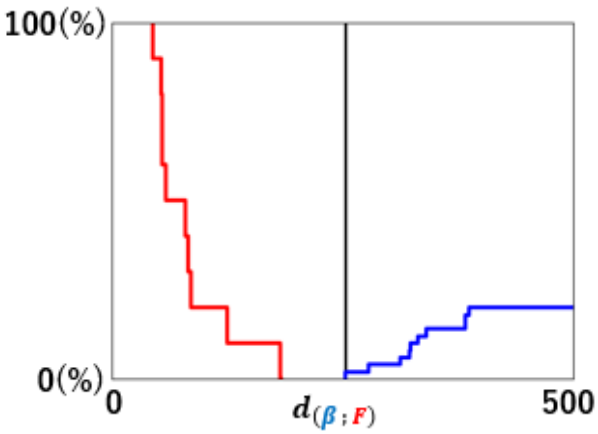

(c) Swing times of 4 and the user D.




(d) Swing times of 5 and the user D.




(e) Swing times of 5 and the user F.




(f) Swing times of 4 and the user E.

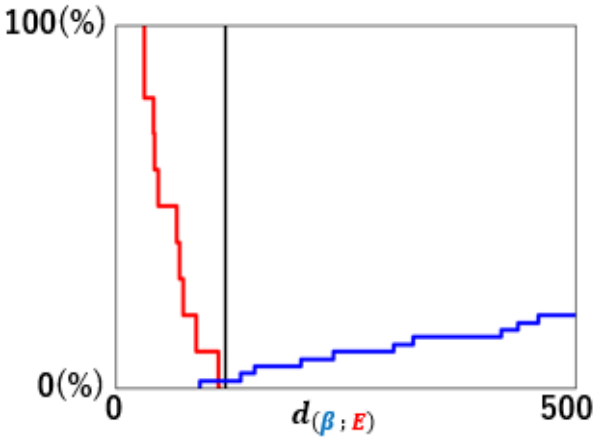



Figure 3: Characteristical FRR-FAR curve.