A Hand Gesture-Based Method for Biometric Authentication

Satoru Imura and Hiroshi Hosobe

Faculty of Computer and Information Sciences,
Hosei University, Tokyo, Japan
hosobe@acm.org

Abstract. With the spread of computers to ordinary people, computer security is becoming increasingly important. User authentication is one of the most important technologies for computer security. Although passwords are used in many personal computers, they are known to sometimes have problems. As an alternative to passwords, biometric authentication, such as fingerprint authentication and face recognition-based authentication, is becoming more widely used. In this paper, we propose a hand gesture-based method as a new kind of biometric authentication. It supports three-dimensional (3D) gestures that allow its user to move the user's hand without touching an input device. Using the motions of fingertips and finger joints as biometric data, the method improves the performance of authentication. Also, we propose seven 3D gestures that can be classified into three types. We implemented the method by using a 3D motion sensor called the Leap Motion controller. We present the results of an experiment that we conducted with nine participants to evaluate the method. For all the gestures, the true acceptance rates were more than 90 %, and the equal error rates were less than 4 %.

Keywords: Biometric authentication, Hand gesture, Motion sensor

1 Introduction

With the spread of computers to ordinary people, computer security is becoming increasingly important. User authentication is one of the most important technologies for computer security. Although passwords are used in many personal computers, they are known to sometimes have problems. For example, users sometimes employ passwords that are easy to memorize, which might enable dictionary attacks to succeed. Also, passwords might be stolen, e.g., by shoulder surfing.

As an alternative to passwords, *biometric authentication* [11, 21, 22] is becoming more widely used. In general, biometric authentication adopts physiological/behavioral characteristics of users (e.g., fingerprints, faces, irises, palm veins, pen pressures, keystrokes, and gaits) for user authentication. Such characteristics are contrary to passwords that users might forget and that other people might steal. Also, since such characteristics are unique to users, there

Fig. 1. Hand gesture-based biometric authentication

are no common patterns like easy-to-memorize passwords. In particular, fingerprint authentication is widely used for mobile devices such as smartphones and tablets. Also, face recognition-based authentication is lately becoming popular.

In this paper, we propose a hand gesture-based method as a new kind of biometric authentication. It supports three-dimensional (3D) gestures that allow its user to move the user's hand without touching an input device, as shown in Figure 1. Using the motions of fingertips and finger joints as biometric data, the method improves the performance of authentication. Also, we propose seven 3D gestures that can be classified into three types. We implemented the method by using a 3D motion sensor called the Leap Motion controller [14]. We present the results of an experiment that we conducted with nine participants to evaluate the method. For all the gestures, the true acceptance rates were more than 90 %, and the equal error rates were less than 4 %.

This paper is an extended version of the poster paper that we previously published as [9]. In particular, this extended paper describes how the proposed method represents 3D hand gestures (Subsection 4.2), how it registers template gestures (Subsection 4.3), and how it performs gesture authentication (Subsection 4.4).

The rest of this paper is organized as follows. After presenting related work in Section 2, we briefly describe the Leap Motion controller and performance measures for biometric authentication in Section 3. Then, in Section 4, we propose our biometric authentication method, and present its implementation in Section 5. We report the experiment that we performed to evaluate our method in Section 6, and discuss the method in Section 7. Finally, we describe conclusions and future work in Section 8.

2 Related Work

Many existing personal computers and mobile devices use text-based passwords and similar symbolic sequences such as PIN codes for user authentication. However, some users employ vulnerable passwords to easily memorize or enter the passwords. Google's Android introduced pattern lock [18], which allows users to draw patterns by connecting dots on touch screens instead of entering text passwords. However, since Android's pattern lock uses only a small number of dots, they are essentially almost as simple as passwords. In addition, Ye et al. [26] showed the possibility of attacking pattern lock; they were able to infer correct patterns by analyzing videos for the motions of fingertips even if the videos had not directly captured the screens.

As an alternative to passwords, there has been research on biometric authentication [11, 21, 22] employing characteristics of users. Methods for biometric authentication can be roughly divided into two categories, the first one using physiological characteristics and the second one using behavioral characteristics. Physiological characteristics include, for example, fingerprints, faces, irises, and palm veins. In particular, fingerprint authentication is widely used in smartphones and tablets, and face recognition-based authentication is lately becoming popular. There has also been research on the use of the physiological characteristics of hands for biometric authentication [2]. For example, Jain et al. [10] showed the possibility of identifying persons by the geometries of hands.

The method that we propose in this paper falls in the second category of biometric authentication. Behavioral characteristics used in this category include, for example, pen pressures, keystrokes, and gaits [11, 15, 21, 22, 25]. Kholmatov and Yanikoglu [12] proposed an online signature verification method that used not only the form of a signature but also the number and the order of the strokes and the velocity and the pressure of the pen. Kim et al. [13] used the pressures of fingertips as behavioral characteristics, in particular, to solve the shoulder surfing problem in the context of collaborative tabletop interfaces. Ataş [1] proposed a biometric authentication method using the tremors of hands, and implemented it by using the Leap Motion controller.

Our biometric authentication method uses hand gestures as behavioral characteristics. Such methods can be categorized into two, one using two-dimensional (2D) hand gestures, and the other using three-dimensional (3D) hand gestures [5]. Methods using 2D hand gestures for biometric authentication typically employ touch screens. Sae-Bae et al. [16] proposed multi-touch gestures using a thumb and four fingers on a multi-touch screen, and studied particular 22 gestures. Sherman et al. [19] studied the use of free-form gestures for authentication.

Biometric authentication methods using 3D hand gestures can be further categorized into sensor- and camera-based methods [5]. Sensor-based methods typically use accelerometers. Guerra-Casanova et al. [8] proposed the use of an accelerometer-embedded mobile device to capture a 3D hand gesture like an in-air signature. Sun et al. [20] developed a biometric authentication system for smartphones that used on-phone accelerometers to capture 3D hand gesture

signatures. It should be noted that such sensor-based methods do not consider the motions of fingers.

Camera-based biometric authentication methods perform image processing. Fong et al. [7] used the stationary images of 3D hand gestures that represented sequences of alphabets in a hand sign language.

Recently, there has been research on camera-based methods using the Leap Motion controllers. Chan et al. [3] used the Leap Motion controller for biometric authentication using a circle-drawing gesture with one finger. Saritha et al. [17] also used the Leap Motion controller to treat circle-drawing, swipe, screen-tap, and key-tap gestures. Xiao et al. [24] used the Leap Motion controller to handle 3D hand gesture signatures. Wong and Kang [23] proposed stationary hand gestures that used the free motions of fingers without the motions of hands, wrists, and arms; they implemented a biometric authentication method by using the Leap Motion controller.

In some sense, these camera-based methods using the Leap Motion controllers share the same motivation as our method. However, our method is more focused on the use of a wider variety of 3D hand gestures. The 3D hand gestures used by Chan et al. [3], Saritha et al. [17], and Xiao et al. [24] were relatively simple because they did not utilize gestures with the complex motions of fingers. Although stationary hand gestures proposed by Wong and Kang [23] were more complex, they still did not use the motions of hands. In this sense, our method is closer to the one proposed by Sae-Bae et al. [16] that defined and studied 22 2D hand gestures in the context of a multi-touch screen.

3 Preliminaries

This section briefly describes the Leap Motion controller and the performance measures for biometric authentication that we use in our work.

3.1 Leap Motion Controller

The Leap Motion controller [14] is a motion sensor that captures the positions of hands and fingers in a 3D space by using two infrared cameras and an infrared LED. It has an effective range of 25 to 600 mm upward, a field of view of 150 degrees in the side direction and of 120 degrees in the depth direction, a tracking rate of 120 fps, and a tracking accuracy of 1/100 mm. It internally has a standard model of human hands, and treats various motions of hands by associating sensor data with the internal model. However, it cannot accurately sense fingers that are hidden by other fingers or by palms. It is a small device of a size of $80 \times 30 \times 11$ mm, and is as low as about 100 US dollars. It is easily available, and even laptop computers with built-in Leap Motion controllers are being sold.

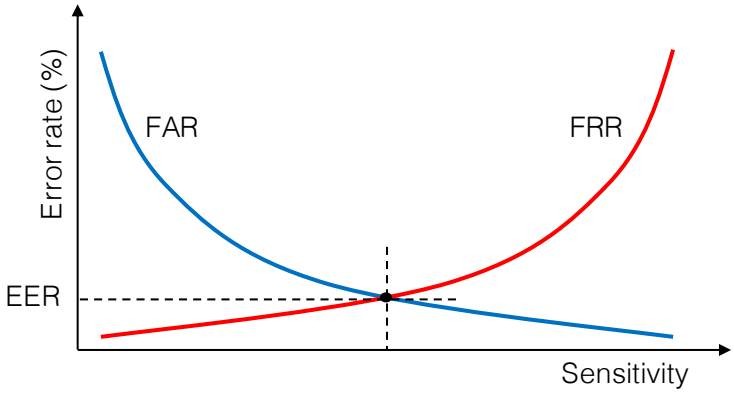

Fig. 2. The false rejection rate (FRR), the false acceptance rate (FAR), and the equal error rate (ERR)

3.2 Performance Measures for Biometric Authentication

There are various measures for evaluating the performance of biometric authentication [4, 6, 11]. In this paper, we use two performance measures. The first measure is the *true acceptance rate* (TAR, also known as the true match rate). This is a simple measure that indicates the rate of how often an input is correctly accepted.

The second measure is the *equal error rate* (EER). This is a measure commonly used to more precisely evaluate the performance of an authentication method. The EER is computed from the false rejection rate (FRR, also known as the false nonmatch rate)[1] and the false acceptance rate (FAR, also known as the false match rate) by considering an appropriate threshold. The EER is defined as the rate at which the FRR and the FAR cross (Figure 2). This is based on the following: a tighter threshold makes the authentication more sensitive by more often causing false rejection (i.e., rejecting a right input); a looser threshold makes the authentication less sensitive by more often causing false acceptance (i.e., accepting a wrong input). Thus there is a trade-off between the FRR and the FAR, and the EER is the error rate corresponding to the best threshold.

4 Proposed Method

This section proposes a hand gesture-based method for biometric authentication.

4.1 3D Hand Gestures

Our method executes biometric authentication using the geometries and the 3D gestures of a hand. It adopts a 3D motion sensor to obtain the geometry

[1] It should be noted that $FRR = 1 - TAR$ holds.

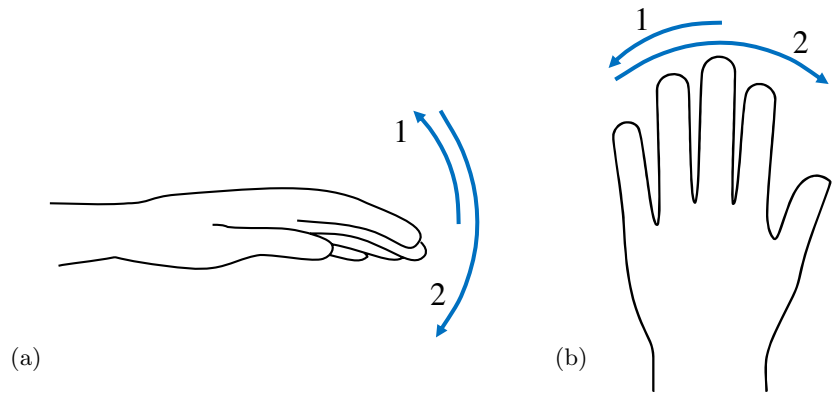

Fig. 3. 3D hand gestures called (a) WUD and (b) WLR

and the position of the hand in real time (Figure 1), from which it computes the similarities of the input gesture with the template gestures stored in its database beforehand.

We propose the following three types of 3D hand gestures, namely, the fingertip, the wrist, and the complex type.[2]

The fingertip type defines gestures that start from an open posture of fingers and then move fingers in certain directions. It consists of the following two gestures.
- **FCO:** All fingertips close and then open.
- **FBO:** Fingertips bend and extend one after another.

The wrist type defines gestures that move the hand in certain directions with the position of the wrist fixed. It consists of the following four gestures.
- **WUD:** The wrist is bended up and down (Figure 3(a)).
- **WLR:** The wrist is bended to the left and to the right (Figure 3(b)).
- **WCWY:** The hand and the forearm are rotated clockwise with the wrist as its center and along the vertical axis (which is parallel to the y-axis shown in Figure 4).
- **WTR:** The hand is turned over and back.

The complex type consists of user-defined gestures.
- **UDS:** The user writes the user's signature in the air.

We use the Leap Motion controller for 3D motion sensing. Users position their hands about 20 cm above the Leap Motion controller as shown in Figure 4. In our experiment that we report in Section 6, the users used the left hands for the gestures other than UDS. For UDS, they used their dominant hands since they needed to write their signatures.

[2] Initially, we included another gesture type called "hand" that consisted of four gestures such as moving the left hand up and down. However, we found that this type of gestures was difficult for users to precisely perform again because they needed to move their arms as well as their hands. Therefore, we excluded this type of gestures.

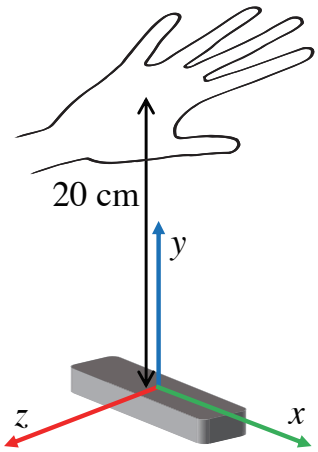

Fig. 4. Setting of the Leap Motion controller for a hand

4.2 Representation of 3D Hand Gestures

Our method internally treats a 3D hand gesture as a time-based sequence of multi-dimensional vectors. For a posture of a hand at a particular time point, it considers the 3D positions of the joints of the fingers as well as the 3D positions of the fingertips. More specifically, a posture of a hand at a time point is represented as a 75-dimensional vector that can be divided into five 15-dimensional vectors for the thumb and the four fingers.

Figure 5 shows the parts of a hand that we use for biometric authentication. The motion sensor measures the 3D positions of the fingertips and the joints of the thumb and the four fingers. For each of the four fingers, there are four joints at the ends of the bones called a distal phalange, an intermediate phalange, and a proximal phalange, and a metacarpal. For the thumb, there are three joints because one bone is missing. In the case of the Leap Motion controller, it internally generates an extra joint for the thumb by additionally considering a bone of a zero length.

Therefore, we can represent each of the thumb and the four fingers at a time point t as the following 15-dimensional vector:

$$\mathbf{f}_{i,t} = (x_{i,t}^{\mathrm{tip}}, y_{i,t}^{\mathrm{tip}}, z_{i,t}^{\mathrm{tip}}, x_{i,t}^{\mathrm{dis}}, y_{i,t}^{\mathrm{dis}}, z_{i,t}^{\mathrm{dis}}, x_{i,t}^{\mathrm{int}}, y_{i,t}^{\mathrm{int}}, z_{i,t}^{\mathrm{int}}, x_{i,t}^{\mathrm{pro}}, y_{i,t}^{\mathrm{pro}}, z_{i,t}^{\mathrm{pro}}, x_{i,t}^{\mathrm{met}}, y_{i,t}^{\mathrm{met}}, z_{i,t}^{\mathrm{met}}),$$

where $i \in \{1, 2, 3, 4, 5\}$ indicates the thumb or one of the four fingers, and each component of $\mathbf{f}_{i,t}$ represents a coordinate of the thumb or one of the four fingers. Using these vectors, we represent a hand posture at t as the following 75-dimensional vector:

$$\mathbf{h}_t = (\mathbf{f}_{1,t}, \mathbf{f}_{2,t}, \mathbf{f}_{3,t}, \mathbf{f}_{4,t}, \mathbf{f}_{5,t}).$$

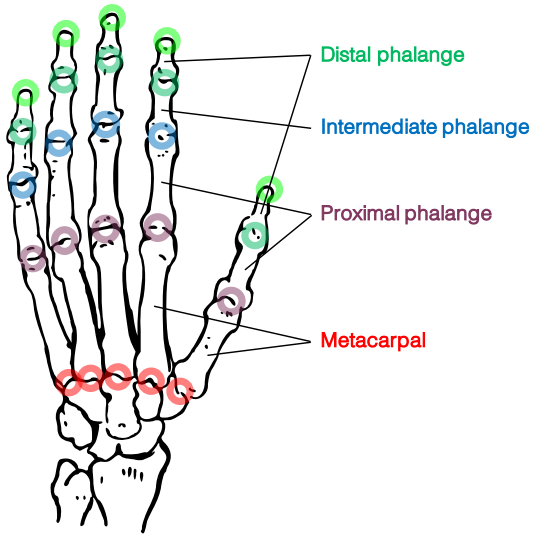

Fig. 5. Parts of a hand used for biometric authentication

Finally, we represent a gesture as the following time-based sequence G of hand postures from time point 1 to T:

$$G = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_T].$$

We use such a sequence G of 75-dimensional vectors for both an *input gesture* and a *template gesture*. An input gesture is the data that is obtained by measuring a user's actually performing a certain 3D hand gesture. A template gesture is the data that is associated with a certain 3D hand gesture of a user and that is stored in a database.

4.3 Registration of Template Gestures

Before gesture authentication, we need to construct a database of template gestures. Since it is often difficult for a user to re-perform a sufficiently similar 3D hand gesture, we use the average of multiple input gestures to obtain a template gesture. Specifically, our method requires the user to repeat a certain gesture ten times to register its template gesture on the database. The average of the ten input gestures is calculated as a template gesture, and then is stored in the database.

We also associate a *preset threshold* with a template gesture. We use it to judge whether an input gesture is sufficiently similar to the template gesture associated with the preset threshold. We obtain the preset threshold of a template gesture by computing the average similarities between this template gesture and the ten used input gestures, where the similarities are calculated as presented in the next subsection. We use such preset thresholds to compute true acceptance rates in our experiment.

4.4 Gesture Authentication

Given an input gesture, our method of gesture authentication reports whether it accepts or rejects the input. This process is performed as follows.

1. Find the template gesture that is the most similar to the input gesture.
2. Do the following:
   (a) If the similarity between the input gesture and the found template gesture is smaller than the preset threshold associated with the template gesture, it accepts the input gesture;
   (b) Otherwise, it rejects the input gesture.

To compute the similarity between an input and a template gesture, our method calculates the sum of the Euclidean distances between the corresponding 75-dimensional vectors from the sequence G_{inp} of the input gesture and the sequence G_{tem} of the template gesture. Formally, with $G_{\mathrm{inp}} = [\mathbf{h}_1^{\mathrm{inp}}, \mathbf{h}_2^{\mathrm{inp}}, \ldots, \mathbf{h}_T^{\mathrm{inp}}]$ and $G_{\mathrm{tem}} = [\mathbf{h}_1^{\mathrm{tem}}, \mathbf{h}_2^{\mathrm{tem}}, \ldots, \mathbf{h}_T^{\mathrm{tem}}]$, the similarity $S(G_{\mathrm{inp}}, G_{\mathrm{tem}})$ between G_{inp} and G_{tem} is defined as follows:

$$S(G_{\mathrm{inp}}, G_{\mathrm{tem}}) = \sum_{t=1}^{T} d(\mathbf{h}_t^{\mathrm{inp}}, \mathbf{h}_t^{\mathrm{tem}}),$$

where each $d(\mathbf{h}_t^{\mathrm{inp}}, \mathbf{h}_t^{\mathrm{tem}})$ is the Euclidean distance between 75-dimensional vectors $\mathbf{h}_t^{\mathrm{inp}}$ and $\mathbf{h}_t^{\mathrm{tem}}$.

The simple calculation of this similarity is usually impossible due to the different lengths of G_{inp} and G_{tem}, which occurs because their lengths depend on the time lengths of the gestures performed by the user. To solve this problem, we extend the shorter sequence to the length of the longer one. We use the following simple method: we first determine the appropriate locations of the shorter sequence where new 75-dimensional vectors should be inserted; then we insert each of the new vectors that we obtain by calculating the midpoint of its previous and next vectors. For example, consider two sequences of lengths 103 and 100. Then we extend the sequence of length 100 by adding new three vectors. Let this sequence be $G = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{100}]$. We insert new three vectors between $\mathbf{h}_{25}$ and $\mathbf{h}_{26}$ and between $\mathbf{h}_{50}$ and $\mathbf{h}_{51}$ and between $\mathbf{h}_{75}$ and $\mathbf{h}_{76}$. We compute the new three vectors as $(\mathbf{h}_{25} + \mathbf{h}_{26})/2$, $(\mathbf{h}_{50} + \mathbf{h}_{51})/2$, and $(\mathbf{h}_{75} + \mathbf{h}_{76})/2$.

5 Implementation

We developed a prototype hand gesture-based biometric authentication system based on the method proposed in the previous section. We used the Leap Motion controller for 3D motion sensing. We implemented the system in Java using the Leap Motion SDK. It consists of approximately 3300 lines of code.

6 Experiment

This section reports the experiment that we conducted to evaluate the proposed method.

Table 1. Results of the experiment

Type	Gesture	TAR (%)	EER (%)
Fingertip	FCO	90.4	3.8
	FBO	90.6	0.0
Wrist	WUD	94.0	2.4
	WLR	97.6	2.9
	WCWY	94.1	2.9
	WTR	93.0	2.3
Complex	UDS	100.0	0.0

6.1 Procedure

We recruited nine participants who all were male and who were 21.8 years old on average.[3] We asked them to use their left hands to perform the gestures other than UDS. In the case of UDS, the participants used their dominant hands since they needed to write their signatures. The participant pressed a key with the other hand when he started and finished a gesture.

We first constructed a database of template gestures. First, the participants practiced each gesture several times before registering its template. For the registration, each participant performed each of the seven gestures ten times (i.e., 70 times in total).

After all the participants registered their template gestures on the database, we conducted an experiment on gesture authentication. In the experiment, each participant performed each of the seven gestures ten times again. Every time after the participant performed a gesture, the system notified him whether it was accepted or rejected. For this purpose, the preset thresholds were used.

6.2 Results

To show the performance of the proposed method, we use two measures TARs and EERs that we explained in Subsection 3.2. Table 1 shows the resulting TARs and EERs for the seven gestures. The TARs were more than 90 % for all the gestures, and the average of the TARs for all the gestures was 94.2 %. The averages of the TARs for the fingertip, the wrist, and the complex type were 90.5 %, 94.7 %, and 100 % respectively.

We computed the EERs for the seven gestures by finding appropriate thresholds. All the EERs resulted in smaller than 4 %, and the average of the EERs for all the gestures was 2.0 %. The averages of the EERs for the fingertip, the wrist, and the complex type were 1.9 %, 2.6 %, and 0.0 % respectively.

[3] Since we wanted a stricter experimental setting, we did not recruit female participants; otherwise, the larger variance of the geometries of the participants' hands could have more affected the experimental results.

7 Discussion

The results of the experiment indicate that the proposed method almost always distinguished the gestures of the participants. It should be emphasized that, in the cases of the fingertip and the wrist type, the participants performed the same 3D hand gestures. This suggests that it is difficult for users to imitate the gestures of other users in such a way that the method cannot distinguish them, which is an ideal property for biometric authentication. It also should be noted that, unlike passwords, 3D hand gestures are not vulnerable to shoulder surfing because of the difficulty of gesture imitation.

Many of the participants gave comments that they had suffered hand fatigue because it had been time-consuming for them to position their hands about 20 cm above the motion sensor. To solve this problem, we need to implement the facility that automatically adjusts the vertical positions of input gestures. Also, it will be better for us to implement the facility that automatically adjusts the angles of input gestures, which can be expected to further improve the performance by reducing errors caused by hand positions.

To compute the similarity between an input and a template gesture, we used a simple definition of the similarity based on the sum of Euclidean distances between time-based sequences of 75-dimensional vectors. Also, we used a simple method for treating an input and a template gesture with different lengths. However, we can consider other alternatives. For example, we could use a distance between two high-dimensional vectors by treating a time-based sequence of 75-dimensional vectors as a single high-dimensional vector. Alternatively, we could use a cosine distance instead of an Euclidean distance. Also, we could use a more sophisticated interpolation method to handle an input and a template gesture with different lengths. We need to explore such alternatives to improve the performance of the gesture-based authentication.

As an experiment for evaluating biometric authentication, our experiment was small in the number of participants. However, the results of the experiment indicated that our method is insufficient than state-of-the-art methods such as fingerprint- and iris-based ones that obtain EERs of less than 0.1 %. Therefore, before conducting a larger experiment, we need to improve the performance of our method by doing things described above. For this purpose, there are also other directions such as the combination of multiple gestures for one trial of authentication.

8 Conclusions and Future Work

We proposed a new biometric authentication method based on 3D hand gestures. We used, as biometric data, timed-based sequences of 3D positions of fingertips and finger joints. Also, we proposed seven 3D hand gestures that are classified into three types. We implemented the method by using the Leap Motion controller as a 3D motion sensor. To evaluate it, we conducted an experiment of gesture authentication with nine participants. As a result, for all the gestures,

the TARs were more than 90 %, and the EERs were less than 4 %. This indicates that, even if different users perform the same gestures, the method can almost always distinguish such gestures. Also, this suggests that, even if a gesture is imitated by another person, the method is not likely to accept it.

Compared to state-of-the-art authentication methods such as fingerprint- and iris-based ones, our method still has room for improvement in performance. For example, we need to implement the facility that automatically adjusts the vertical positions and the angles of input gestures. Also, we could improve the performance by combining multiple gestures for one trial of authentication. We believe that we should pursue a biometric authentication method that is easy-to-use for ordinary people.

Acknowledgment

This work was partly supported by JSPS KAKENHI Grant Number JP15KK0016.

References

1. M. Ataş. Hand tremor based biometric recognition using Leap Motion device. *IEEE Access*, 5:23320–23326, 2017.
2. M. Bača, P. Grd, and T. Fotak. Basic principles and trends in hand geometry and hand shape biometrics. In *New Trends and Developments in Biometrics*, pages 77–99. InTech, 2012.
3. A. Chan, T. Halevi, and N. D. Memon. Leap Motion controller for authentication via hand geometry and gestures. In *Proc. HAS*, volume 9190 of *LNCS*, pages 13–22, 2015.
4. F. Cherifi, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger. Performance evaluation of behavioral biometric systems. In *Behavioral Biometrics for Human Identification: Intelligent Applications*, pages 57–74. IGI Global, 2009.
5. G. D. Clark and J. Lindqvist. Engineering gesture-based authentication systems. *IEEE Pervasive Comput.*, 14(1):18–25, 2015.
6. M. El-Abed and C. Charrier. Evaluation of biometric systems. In *New Trends and Developments in Biometrics*, pages 149–169. InTech, 2012.
7. S. Fong, Y. Zhuang, I. Fister, and I. Fister Jr. A biometric authentication model using hand gesture images. *Biomed. Eng. Online*, 12(111):1–18, 2013.
8. J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra. Authentication in mobile devices through hand gesture recognition. *Int. J. Inf. Security*, 11(2):65–83, 2012.
9. S. Imura and H. Hosobe. Biometric authentication using the motion of a hand (poster). In *Proc. ACM SUI*, page 221, 2016.
10. A. K. Jain, A. Ross, and S. Prabhakar. A prototype hand geometry-based verification system. In *Proc. Int. Conf. Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 166–171, 1999.
11. A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.*, 14(1):4–20, 2004.
12. A. Kholmatov and B. Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recogn. Lett.*, 26(15):2400–2408, 2005.

13. D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier. Multi-touch authentication on tabletops. In *Proc. ACM CHI*, pages 1093–1102, 2010.
14. Leap Motion. Leap Motion for Mac and PC. https://www.leapmotion.com/product/desktop/.
15. A. Mahfouza, T. M. Mahmouda, and A. S. Eldinc. A survey on behavioral biometric authentication on smartphones. *J. Inf. Security Appl.*, 37:28–37, 2017.
16. N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon. Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In *Proc. ACM CHI*, pages 977–986, 2012.
17. L. R. Saritha, D. Thomas, N. Mohandas, and P. Ramnath. Behavioral biometric authentication using Leap Motion sensor. *Int. J. Latest Trends Eng. Technol.*, 8(1):643–649, 2017.
18. A. Shabtai, Y. Fledel, and U. Kanonov. Google Android: A comprehensive security assessment. *IEEE Security & Privacy*, 8(2):35–44, 2010.
19. M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos. User-generated free-form gestures for authentication: Security and memorability. In *Proc. MobiSys*, pages 176–189. ACM, 2014.
20. Z. Sun, Y. Wang, G. Qu, and Z. Zhou. A 3-D hand gesture signature based biometric authentication system for smartphones. *Security Comm. Netw.*, 9(11):1359–1373, 2016.
21. J. Wayman, A. Jain, D. Maltoni, and D. Maio. An introduction to biometric authentication systems. In *Biometric Systems*, pages 1–20. Springer, 2005.
22. J. L. Wayman. Fundamentals of biometric authentication technologies. *Int. J. Image Gr.*, 1(1):93–113, 2001.
23. A. M. H. Wong and D.-K. Kang. Stationary hand gesture authentication using edit distance on finger pointing direction interval. *Scientific Prog.*, 2016(7427980):1–15, 2016.
24. G. Xiao, M. Milanova, and M. Xie. Secure behavioral biometric authentication with Leap Motion. In *Proc. ISDFS*, pages 112–118. IEEE, 2016.
25. R. V. Yampolskiy and V. Govindaraju. Taxonomy of behavioural biometrics. In *Behavioral Biometrics for Human Identification: Intelligent Applications*, pages 1–43. IGI Global, 2009.
26. G. Ye, Z. Tang, D. Fang, X. Chen, K. I. Kim, B. Taylor, and Z. Wang. Cracking Android pattern lock in five attempts. In *Proc. NDSS*. Internet Society, 2017.