A Hand Gesture-Based Authentication Method That Makes Forgery Difficult

Hideaki Terui and Hiroshi Hosobe$^{[0000-0002-7975-052X]}$

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

Abstract. Physiological biometric authentication methods such as fingerprint, face, vein, and iris authentication have become or are becoming popular. Although these methods are highly accurate, they still have the problem of poor authentication due to noise and other disturbance in recognition. To alleviate this problem, behavioral biometric authentication also has been being studied. Among them, hand gesture-based authentication methods adopt the geometry and motion of hands and fingers. However, such hand gesture-based methods have the problem that they require larger movements than other authentication methods and are easily seen by third persons, which enables forgery. In this paper, we propose a hand gesture-based authentication method that incorporates dummy gestures to make forgery difficult. It allows increasing the number of gesture elements by inserting dummy gestures into real gestures during authentication. We show the results of an experiment that we conducted to examine whether the participants could insert dummy gestures and whether the dummy gestures could work as a countermeasure against forgery.

Keywords: Biometric authentication · Hand gesture · Forgery prevention.

1 Introduction

Passwords are often used in authentication as a security measure. While passwords can be easily created, they have the disadvantage that they can be memorized by third persons. For this reason, physiological biometric methods such as fingerprint, face, vein, and iris authentication have become or are becoming popular. Although these methods are highly accurate, they still have the problem of poor authentication due to noise and other disturbance in recognition.

To alleviate this problem, behavioral biometric authentication also has been being studied. Along this line, researchers proposed hand gesture-based authentication methods adopting the geometry and motion of hands and fingers [2, 4, 5, 7–10, 17, 22, 25, 27, 30, 31, 34]. However, such hand gesture-based methods have the problem that they require larger movements than other authentication methods and are easily seen by third persons (sometimes called shoulder surfing [2]), which enables forgery.

In this paper, we propose a hand gesture-based authentication method that incorporates dummy gestures to make forgery difficult. It allows increasing the number of gesture elements by inserting dummy gestures into real gestures during authentication. In the experiment, we examined whether the participants could insert dummy gestures and whether the dummy gestures could work as a countermeasure against forgery. As a result, we found that it was not difficult to authenticate with dummy gestures. We also found that adding the average of 1.8 dummy gestures to four real gestures made it difficult to memorize the entire gestures.

The rest of this paper is organized as follows. Section 2 describes previous work related to our method, and Section 3 briefly explains preliminaries to our method. Section 4 proposes our method, and Section 5 gives its implementation. Section 6 presents the results of the experiment, and Section 7 discusses our method. Finally, Section 8 provides conclusions and future work.

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 [23], which allows users to draw patterns by connecting dots on touch screens instead of entering text passwords. 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. [33] showed the possibility of attacking pattern lock; they were able to infer correct patterns by analyzing videos for the motion of fingertips even if the videos had not directly captured the screens.

As an alternative to passwords, there has been research on biometric authentication [12, 28, 29] 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 has lately become popular. There has also been research on the use of the physiological characteristics of hands for biometric authentication [3]. For example, Jain et al. [11] showed the possibility of identifying persons by the geometry 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 [12, 15, 28, 29, 32]. Kholmatov and Yanikoglu [13] 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. [14] 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 [6]. Methods using 2D hand gestures for biometric authentication typically employ touch screens. Niu and Chen [18] proposed the use of gestures with taps on a touch screen for authentication. Sae-Bae et al. [20] proposed multi-touch gestures using a thumb and four fingers on a multi-touch screen, and studied particular 22 gestures. Sherman et al. [24] 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 [6]. 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. [25] 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 motion 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. Aumi and Kratz [2] used a depth camera for authentication with 3D hand gestures for diagrammatic shapes such as a star and a spiral.

More recently, there has been research on camera-based methods using the Leap Motion Controller (LMC). We previously proposed an authentication method using three types of 3D hand gestures [9, 10]. We particularly studied the use of the motion of fingertips and wrists for 3D gestures. We implemented the method by using LMC to capture 3D gestures.

Other researchers also used LMC for hand gesture-based authentication. Nigam et al. [17] used LMC to capture in-air signatures for authentication. Xiao et al. [31] also used LMC to handle in-air signatures. Chahar et al. [4] proposed "Leap password" consisting of six gestures using one of 10 fingers at a time. Chan et al. [5] used LMC for authentication using a circle-drawing gesture with one finger. Saritha et al. [22] also used LMC to treat circle-drawing, swipe, screen-tap, and key-tap gestures. Wong and Kang [30] proposed stationary hand gestures that used the free motion of fingers without the motion of hands, wrists, and arms; they implemented a biometric authentication method by using LMC. Zhao and Tanaka [34] proposed a hand gesture-based authentication method using LMC; it was capable of updating gesture templates to make it work for a long period. Wang and Tanaka [27] proposed a hand gesture-based authentication method based on machine learning; to ease the learning process, it incorporated data augmentation and incremental learning.

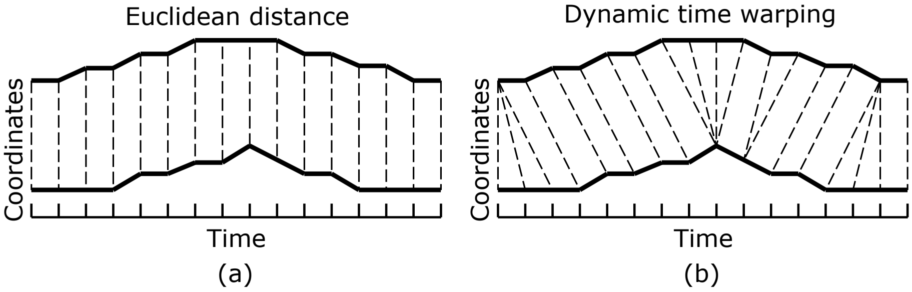


Fig. 1. Matching two data sequences by dynamic time warping.

3 Preliminaries

In this section, we briefly describe the Japanese fingerspelling alphabets, the Leap Motion Controller, and dynamic time warping, which we use for our hand gesture-based authentication method.

3.1 Japanese Fingerspelling Alphabets

Fingerspelling is a visual language that maps static hand gestures into alphabets. A hand gesture is made by extending or bending fingers and occasionally turning over the hand. Fingerspelling differs according to countries. The Japanese fingerspelling alphabets [19] are used in Japan.

3.2 Leap Motion Controller

The Leap Motion Controller [26] is a motion sensor specialized in hand gestures. It is equipped with a stereo infrared camera and an infrared light-emitting diode (LED). It computes the positional information of hands in the 3D space by lightening and capturing the hands with the LED and the stereo camera. It achieves the tracking speed of 120 fps and the tracking accuracy of 1/100 mm, and captures a stereo image each frame.

3.3 Dynamic Time Warping

Dynamic time warping [21] computes the matching of two data sequences in such a way that the distances between the matched points in the sequences are the shortest. As shown in Figure 1(a), comparing two data sequences by simply using the same time points may yield large errors for parts of large movements. By contrast, dynamic time warping minimizes the errors by matching the time points as shown in Figure 1(b).

4 Proposed Method

Our method allows a user to register a single sequence of gestures by combining gesture elements that were borrowed from the Japanese fingerspelling alphabets [19]. However, simply increasing the number of such gesture elements imposes a burden on the user. Therefore, to make the gesture sequence difficult for third persons to memorize and forge, our method allows the user to insert multiple dummy gestures into real gestures during authentication. Since human short-term memory has the capacity of 7 ± 2 [16], the additional dummy gestures make the entire gesture sequence more difficult for third persons to memorize and forge.

Dummy gestures should not be recognizable to third persons although the user needs to distinguish dummy gestures from real gestures for authentication. For this purpose, we introduce conditions that real gestures should satisfy, and allow the user to select a condition at the time of registering a gesture sequence. Specifically, we introduce the following 12 conditions for real gestures that we decided from the observation of the Japanese fingerspelling alphabets: (1) the palm directs downward and (2) upward; (3) the thumb extends and (4) bends; (5) the index finger extends and (6) bends; (7) the middle finger extends and (8) bends; (9) the ring finger extends and (10) bends; (11) the little finger extends and (12) bends.

Dummy gestures can be constructed by performing gestures that do not satisfy the condition selected by the user. It is not necessary to select gestures from the Japanese fingerspelling alphabets. For example, if the user selects the condition for real gestures that the thumb bends, then any gestures with the thumb extending will be recognized as dummy gestures and will be excluded from the authentication. The user can insert various dummy gestures such as the other finger bending and extending, which will make the condition difficult for third persons to recognize.

In authentication, the order of real gestures must be preserved, but dummy gestures can be inserted anytime. For example, let g_1, g_2, g_3, and g_4 be a sequence of real gestures and d_1, d_2, and d_3 be a sequence of dummy gestures. Then the following sequences P_1 and P_2 of seven gestures are legal:

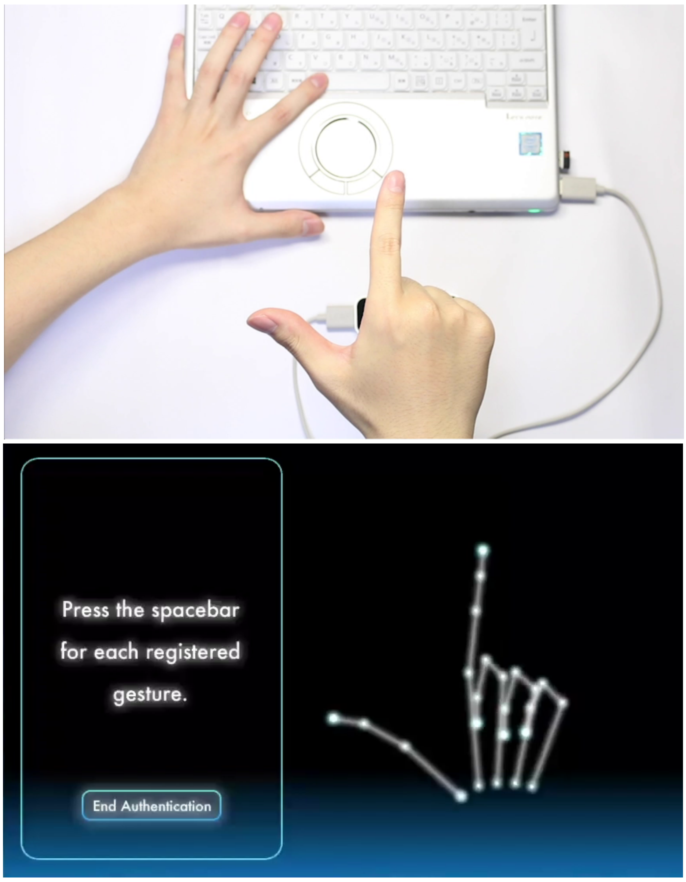
$$P_1 = (g_1, d_1, g_2, g_3, d_2, d_3, g_4)$$
$$P_2 = (d_1, g_1, g_2, d_2, g_3, g_4, d_3).$$

By contrast, the following sequence P_3 of gestures is illegal because the order of the real gestures is not the same:

$$P_3 = (g_1, d_1, g_3, g_2, d_2, d_3, g_4).$$

5 Implementation

We implemented the proposed method as a prototype system in Java by using the Leap Motion Controller [26]. For dynamic time warping, we used Salvador



Press the spacebar for each registered gesture.

Fig. 2. Prototype system based on our hand gesture-based authentication method.

and Chan's implementation [21]. The system consists of approximately 1100 lines of code. Figure 2 shows the system that is performing the authentication of a user's gesture sequence.

5.1 Template Registration

The system first asks the user to register gesture templates. The user selects one from the 12 conditions for real gestures described in Section 4. The user selects four real gestures from the Japanese fingerspelling alphabets in such a way that they satisfy the selected gesture condition. We determined this number four of the real gestures, based on the preliminary experiment that we previously conducted.

This is the author's version. The final authenticated version is available online at
https://doi.org/10.1007/978-3-031-05563-8_18.

In the same way as our previous method [10], we obtain the following data for each frame of the Leap Motion Controller:

$$\begin{aligned}&(\text{x, y, and z coordinates}) \times (\text{fingertip and 4 joints}) \times (\text{5 fingers})\\&\quad = \text{75-dimensional vector.}\end{aligned}$$

The system additionally obtains the data of whether the fingers extend or bend, and their pitch, roll, and yaw values. It uses the additional data to identify dummy gestures.

To register a gesture template, the user repeats the real gestures five times. Then the system generates the template by computing the average of the data of the five gestures for each frame. To compute the threshold for authentication, we used the same way as our previous method.

5.2 Authentication

In authentication, the user performs dummy gestures in addition to four real gestures. To identify dummy gestures, the system records for each frame whether the hand is turned over or not and whether each finger extends or bends. It uses the roll value to judge whether the hand is turned over. It decides that a finger bends if the finger bends for 30 % or more of the period of a gesture.

When the system does not regard an input gesture as a dummy, it compares the input gesture with the stored gesture templates. To handle difference in speed between the input gesture and the templates, we use our previous interpolation method [10] as well as dynamic time warping [21]. Also, we handle difference in positions between the input gesture and the templates by translating the input gesture to the initial positions of the templates. The system compares the input gesture with a template by computing the Euclidean distances between the matched frames by dynamic time warping. If the sum of the Euclidean distances is smaller than the predetermined threshold, the system accepts the input gesture.

6 Experiment

To evaluate the proposed method, we conducted an experiment. We particularly examined whether new users could perform hand gestures for authentication and whether dummy gestures could work as a countermeasure against gesture forgery.

6.1 Procedure

We recruited 12 participants who were all male and 22.0 years old on average (more specifically, one 24-year-old, one 23-year-old, seven 22-year-old, and three 21-year-old persons). We restricted them only to male to exclude the influence of the difference of hand geometry as much as possible. They all were new to hand gestures.

Table 1. Result of the questionnaire.

Question	Mean	Variance
1: Easiness of hand gesture-based authentication	2.7	1.7
2: Easiness of authentication with dummy gestures	2.9	1.7
3: Easiness of inserting dummy gestures	3.3	1.4
4: Appropriate number of dummy gestures	2.9	0.24
5: Number of dummy gestures that disabled memorizing	1.8	0.69

We asked each of them to select one from the 12 conditions. They started and finished each gesture element by extending all the fingers. They first selected four gesture elements (g_1, g_2, g_3, and g_4) from the Japanese fingerspelling alphabets, and registered a gesture template by repeating the gesture sequence five times. Then they authenticated the gesture sequence without dummy gestures five times. Next, they performed gestures by inserting two to six dummy gestures that occurred to them at that time. In addition, they watched the videos where another person was performing gestures, by which we investigated how many dummy gestures were needed to make them difficult to memorize.

After the experiment, we conducted a questionnaire. We asked them to answer the following three questions in Likert scale from 1 (very difficult) to 5 (very easy).

Question 1: Was the hand gesture-based authentication easy?
Question 2: Was the authentication with dummy gestures easy?
Question 3: Was it easy to insert dummy gestures by yourself?

We also asked them to answer the numbers of gestures for the following two questions.

Question 4: How many dummy gestures do you think are appropriate?
Question 5: How many dummy gestures disabled you from memorizing another person's gesture sequences?

6.2 Results

Table 1 shows the results of the questionnaire. The results of questions 1 and 2 indicate that the participants who were new to hand gestures were able to use our hand gesture-based authentication method. The result of question 3 indicates that it was not difficult for the participants to insert dummy gestures by themselves. According to the results of questions 4 and 5, they wanted to insert about three dummy gestures, but they were disabled by nearly two dummy gestures from memorizing gesture sequences.

Table 2 shows the result of the acceptance rates of the gestures of the participants. The rates varied according to the participants; while the rates for participant 2 were significantly low, the rates for participant 5 were comparatively high. The error rate for dummy gestures was 0.038 % since 9 out of the 240 dummy gestures performed by the 12 participants were accepted.

Table 2. Acceptance rates of the gestures of the participants.

Participant	g_1 (%)	g_2 (%)	g_3 (%)	g_4 (%)	Mean (%)
1	40	60	70	70	60
2	0	0	10	20	7.5
3	0	90	70	20	45
4	30	30	10	60	33
5	90	80	70	30	68
6	40	40	60	0	35
7	30	30	100	0	40
8	100	80	60	20	65
9	30	10	40	0	20
10	20	10	30	90	38
11	0	0	70	90	40
12	20	80	30	20	38

7 Discussion

The result of question 1 indicates that the participants found it slightly difficult to perform the hand gesture-based authentication for the first time. However, as far as we observed the participants' behaviors during the experiment, they were able to perform hand gestures after practice. We think that, since the Japanese fingerspelling alphabets include hand gestures that appear in daily life, the participants were able to perform the gestures without much difficulty.

According to the result of question 2, the authentication with dummy gestures was easier than the hand gesture-based authentication. More specifically, some participants answered to question 2 that the authentication with dummy gestures was easy even if they answered to question 1 that the hand gesture-based authentication was difficult. We think that the authentication with dummy gestures is not difficult even for users who think of the hand gesture-based authentication as being difficult.

The result of question 3 indicates that the participants did not think that it was difficult to insert dummy gestures by themselves. We think that this is because of the simplicity of our method that specifies only one condition for real gestures and lets the users perform dummy gestures that do not satisfy the condition. A participant commented that it was easy to produce variations of gestures because only turning over the hand made a different gesture.

The result of question 5 indicates that inserting only 1.8 dummy gestures made it difficult for the participants to memorize entire gesture sequences. In other words, it was difficult to memorize a sequence of 5.8 gestures consisting of four real and 1.8 dummy gestures. Our experiment showed that the general capacity of 7 ± 2 of human short-term memory [16] was also true for gesture sequences. According to the result of question 4, the participants thought that adding 2.9 dummy gestures was appropriate. Therefore, we claim that performing seven gestures including three dummy gestures works as a countermeasure against gesture forgery.

As shown in Table 2, our system did not achieve high acceptance rates, compared to other related methods. There were few gestures that achieved the acceptance rates of 90 % or more although it is difficult to simply compare the results because of the different gestures performed by the participants. We think that a cause for those low acceptance rates was that it was difficult for the participants to accurately perform each gesture while performing multiple gestures, compared to the case of performing only one gesture. In fact, we confirmed that the variance of the time for performing gestures in authentication was larger than that in registration, which means that the time for performing gestures in authentication largely varied.

8 Conclusions and Future Work

We proposed a hand gesture-based authentication method that incorporated dummy gestures to make forgery difficult. Although the acceptance rate of real gestures was not high, we showed that the method worked as a countermeasure against gesture forgery by incorporating 1.8 dummy gestures. Also, it effectively identified dummy gestures with the low error rate of 0.038 %.

Our future work is to support an undo function; some participants commented that it was troublesome to perform gestures from the beginning when they made a single mistake while performing multiple gestures. Another future direction is to improve the acceptance rate of real gestures by using Wang and Tanaka's method [27].

Acknowledgment

This work was partly supported by JSPS KAKENHI Grant Number JP21K11836.

References

1. M. Ataş. Hand tremor based biometric recognition using Leap Motion device. *IEEE Access*, 5:23320–23326, 2017.
2. M. T. I. Aumi and S. G. Kratz. AirAuth: Evaluating in-air hand gestures for authentication. In *Proc. ACM MobileHCI*, pages 309–318, 2014.
3. 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.
4. A. Chahar, S. Yadav, I. Nigam, R. Singh, and M. Vatsa. A Leap password based verification system. In *Proc. IEEE BTAS*, pages 1–6, 2015.
5. 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.
6. G. D. Clark and J. Lindqvist. Engineering gesture-based authentication systems. *IEEE Pervasive Comput.*, 14(1):18–25, 2015.
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. S. Imura and H. Hosobe. A hand gesture-based method for biometric authentication. In *Proc. HCI Int.*, volume 10901 of *LNCS*, pages 554–566, 2018.
11. 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.
12. A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.*, 14(1):4–20, 2004.
13. A. Kholmatov and B. Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recogn. Lett.*, 26(15):2400–2408, 2005.
14. 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.
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. G. A. Miller. The magical number seven, plus or minus two: Some limits on our capacity for processing. *Psychol. Rev.*, 63(2):81–97, 1956.
17. I. Nigam, M. Vatsa, and R. Singh. Leap signature recognition using HOOF and HOT features. In *Proc. IEEE ICIP*, pages 5012–5016, 2014.
18. Y. Niu and H. Chen. Gesture authentication with touch input for mobile devices. In *Proc. MobiSec*, volume 94 of *LNICST*, pages 13–24, 2011.
19. K. Ochiai and K. Kamata. Description method of Japanese manual alphabet using image features. In *Proc. IEEE SMC*, pages 1091–1093, 1989.
20. 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.
21. S. Salvador and P. Chan. Toward accurate dynamic time warping in linear time and space. *Intell. Data Anal.*, 11(5):561–580, 2007.
22. 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.
23. A. Shabtai, Y. Fledel, and U. Kanonov. Google Android: A comprehensive security assessment. *IEEE Security & Privacy*, 8(2):35–44, 2010.
24. 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.
25. 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.
26. Ultraleap. Leap Motion Controller. https://www.ultraleap.com/product/leap-motion-controller/.
27. X. Wang and J. Tanaka. GesID: 3D gesture authentication based on depth camera and one-class classification. *Sensors*, 18(3265):1–23, 2018.
28. J. Wayman, A. Jain, D. Maltoni, and D. Maio. An introduction to biometric authentication systems. In *Biometric Systems*, pages 1–20. Springer, 2005.
29. J. L. Wayman. Fundamentals of biometric authentication technologies. *Int. J. Image Gr.*, 1(1):93–113, 2001.

30. 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.
31. G. Xiao, M. Milanova, and M. Xie. Secure behavioral biometric authentication with Leap Motion. In *Proc. ISDFS*, pages 112–118. IEEE, 2016.
32. R. V. Yampolskiy and V. Govindaraju. Taxonomy of behavioural biometrics. In *Behavioral Biometrics for Human Identification: Intelligent Applications*, pages 1–43. IGI Global, 2009.
33. 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.
34. J. Zhao and J. Tanaka. Hand gesture authentication using depth camera. In *Proc. FICC*, volume 887 of *AISC*, pages 641–654, 2018.