Authentication Method Using Opening Gestures

Shogo Sekiguchi(✉), Shingo Kato, Yoshiki Nishikawa, and Buntarou Shizuki

University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan
{sekiguchi,skato,nishikawa,shizuki}@iplab.cs.tsukuba.ac.jp

Abstract. Smart locks can be used to improve door security. However, code- (e.g., PIN and passwords) and biometric-based (e.g., fingerprints and faces) authentication methods in smart locks can be spotted, limiting their usability in real life. In this study, we present an authentication method that uses a gesture to open a door (opening gesture). In this method, the user performs their own opening gesture to open a door, then authentication is performed based on the unique behavioral characteristics of their opening gesture. This design may have the following merits. First, the user can design their opening gesture in a way that reflects their preferences, making the gesture easily memorable. Second, it is difficult to imitate the movements since they inherently contain individuality. Finally, an opening gesture, unlike a biometric features such as a face or fingerprints, can be changed if it is duplicated by an attacker. To examine the idea of our authentication method, we asked participants to design their own opening gestures and perform them for data collection. Capacitive sensors, pressure sensors, and an IMU were used to measure the movements of the gestures. The results showed that a Random Forest with 11 gestures could reach an average precision rate of 0.816 and an average FAR of 0.015. Our shoulder hacking experiment with 8 participants showed that our system archived a FAR of 0.000 for the imitated gestures by *nonusers*. These showed resistance to imitation by attackers.

Keywords: motion-based authentication · door · behavioral biometric · inertial measurement unit · touch pressure · capacitive sensing · personal characteristic

1 Introduction

Smart locks can be used to improve door security. However, code- (e.g., PIN and passwords) and biometric-based (e.g., fingerprints and faces) authentication methods in smart locks can be spotted, limiting their usability in real life [30]. Knowledge-based methods are vulnerable to shoulder hacking [10]. While biometric-based methods are the potential to be duplicated for abuse. For these reasons, users might hesitate to use these authentication methods [10,13].

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 186–203, 2024.
https://doi.org/10.1007/978-3-031-61382-1_12

In this study, we present an authentication method that uses a gesture to open a door (opening gesture). In this method, the user performs their own opening gesture to open a door, then authentication is performed based on the unique behavioral characteristics of their opening gesture. This design may have the following merits. First, the user can design their opening gesture in a way that reflects their preferences, making the gesture easily memorable. Second, it is difficult to imitate the movements since they inherently contain individuality. Finally, an opening gesture, unlike a biometric features such as a face or fingerprints, can be changed if it is duplicated by an attacker.

To examine the idea of our authentication method, we asked participants to design their own opening gestures and perform them for data collection. With these data, we examined the performance of our authentication method. The results showed resistance to imitation by attackers. The contributions of our work can be summarized as follows:

- We analyzed user-defined opening gestures to elicit common features, finding Code-Length, Number-of-Fingers, and Finger-Identity to be the most preferred.
- The user and nonuser performance showed that there may be a trade-off between imitation resistance and overall authentication accuracy.
- Opening gestures were found to be feasible for interaction, and were an efficient, accurate, and private authentication technique for the doorknob.

2 Related Research

Currently, widely commercialized products adopt two major authentication methods: code- and biometric-based, which are simple to use and can achieve high authentication performance. To improve the performance of authentication, researchers have proposed leveraging a wider range of features [10,13,22]. For example, capacitance can identify users based on their hand shapes on touch screens [9], while bioimpedance differences across users' forearms have been explored [7]. Pressure sensors have been utilized to recognize users based on their touch force on an object [15,16]. Another approach recognizes users by extracting their motion characteristics with an inertial measurement unit (IMU) [5,12,17]. Since these sensors are inexpensive compared to sensors used for fingerprint, face, or iris recognition [3,4,6], we combine these sensors to achieve more robust and inexpensive authentication. In this section, we mainly reviewed authentication methods leveraging capacitive sensing, pressure sensing, and IMU sensing.

There are challenges with code- and biometric-based methods. Code-based authentication is prone to shoulder hacking when used in public. Memorable passwords are often easy to break, while it is difficult to remember secure passwords [20]. Biometric-based authentication relies on the user's unique physical characteristics, thereby ensuring high security. However, users may hesitate to use such technology due to privacy concerns, since immutable biometric features carry significant risks when duplicated [22]. To meet to these challenges,

researchers have proposed a motion-based authentication method (e.g., [2,28]). It leverages dynamic biometric features of gestures to improve code memorability. In this section, we compare our work with research on authentication that utilizes biometrics features.

2.1 Authentication Methods Leveraging Capacitive Sensing

The capacitive touch screen is the most common interaction interface on today's mobile devices. Due to its sensitivity to the human body, many researchers have tried to leverage it for authentication. CapAuth [9] authenticates user based on the contact area on which they place their fingers on the screen. Bodyprint [14] uses the capacitive touch screen of smartphones as an image scanner to authenticate the users based on the contact features of different body parts (e.g., ear, palm, and finger). These methods rely on static biometric features for authentication, which may be insecure if they were duplicated [22].

Dynamic biometric features have been tried to solve this concern. Rilvan et al. [26] used the frames of capacitance data while swiping on a capacitive touch screen for authentication. Feng et al. [8] extracted features from gestures on a capacitive touch screen to perform authentication by combining these data with additional IMU sensor glove information. Similar to Bodyprint, BioTouch [31] utilizes a capacitive touch screen on a smartphone for image scanning, authenticating users based on the touch motion feature of the finger. These methods using capacitive sensing illustrate the feasibility of motion-based authentication. Similarly, we employ opening gestures that were private and potentially efficient, given their execution feasibility.

2.2 Authentication Methods Leveraging Pressure Sensing

Pressure sensing is widely used for authentication because it can be unique to users, and thus difficult to imitate. Abbas et al. [1] proposed a user authentication method based on behavioral biometrics during the interaction of tapping on simple shapes (circle, square, rectangular, triangle, cross, and check-mark), utilizing 25 features, including coordinates, duration, distance, and velocity and employing supervised learning. Use the Force [15] explicitly combines touch pressure with pin code, significantly expanding the code space and achieving higher security. Pelto et al. [24] created more intricate and personalized touch dynamics for authentication by enabling users to simultaneously touch the screen of mobile devices with multiple fingers.

These methods improve the accuracy of traditional authentication technologies by utilizing touch pressure, while also limited hacking resistance. Notably, no methods reviewed shoulder hacking. In contrast, we assess the resistance of our method to shoulder hacking through experiments.

2.3 Authentication Methods Leveraging IMU Sensing

Other methods authenticate users by extracting their motion characteristics with IMU sensors. Liu et al. [18] leveraged built-in IMU sensors on smartphones

to gather biometric features from the vibrations of the user's lower jaw and attempt authentication. Feng et al. [8] performed authentication by extracting features from IMU sensor glove information when touching the screen. Similar to capacitive sensing, these methods using IMU sensing have demonstrated the feasibility of motion-based authentication.

2.4 Authentication Methods Leveraging Opening Gesture

Code- and biometric-based methods can be spotted, limiting their usability in real life [30]. Researchers have proposed dynamic authentication methods, which track features continuously to avoid static authentication behavior. SmartHandle [11] attempts authentication by attaching an IMU to a doorknob and collecting the trajectory and speed of hand movements when opening a door. SenseHandle [27] uses swept frequency capacitive sensing and an acoustic sensor in addition to a IMU to capture interactions when opening a door for authentication. In contrast to these systems, we attempt to use pressure, capacitive, and inertial sensing for opening gesture authentication.

3 Exploring the Design Space of Opening Gestures

In this section, we ask participants to design opening gestures for authentication in real-life scenarios, exploring the design space of practical opening gestures. Additionally, we evaluate the authentication performance of data collected from the participants.

3.1 Participants

We recruited 10 participants from the same laboratory as the authors (all male, M = 23.3 y.o., SD = 2.06 y.o.) as volunteers. Of the participants, nine were right-handed, and one was ambidextrous. Regarding the direction in which their door opens at home, six answered that it opens to the left, while four answered that it opens to the right.

3.2 Hardware

The door that was used had a doorknob with a width of 135 mm, a diameter of 15 mm, and a shaft diameter of 20 mm. The height from the floor to the center of the shaft was 1000 mm, and the door opened it opens to the left (Fig. 1a). We wapped the doorknob with copper tape as electrodes to measure its capacitance. A capacitor was charged through a digital output pin of a microcomputer with a 1 MΩ resistor in series. On the discharge (measurement) side, the copper tape was connected in parallel with the charging side, featuring a 1 kΩ resistor in series, and linked to a digital input pin of the microcomputer for capacitance measurement. The capacitance was determined by measuring the time required for charging. The door was conductive and magnetic. The doorknob part was

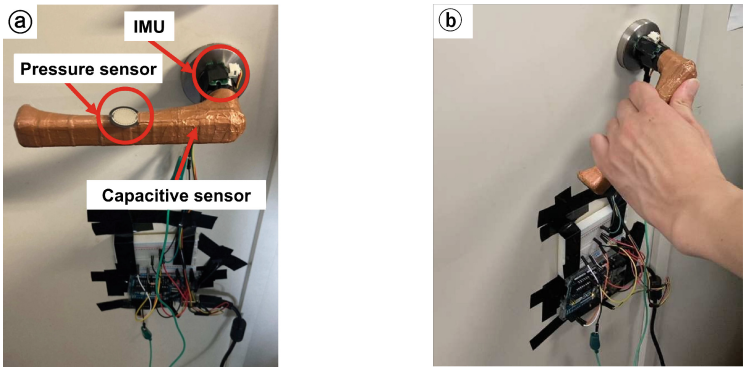

Fig. 1. Hardware installation on the door handle. (a) Front view and sensor placement. (b) Example of gesture demonstration.

nonconductive and nonmagnetic, but considering the influence of the door itself, we wrapped it with insulating tape before wrapping it with copper tape. A pressure sensor (Alpha's MF01A-N-221-A04) was installed at the center of the top of the doorknob handle. An IMU (Akizuki Tsusho's AE-LSM9DS1-I2C) was installed at the center of the top of the doorknob shaft. Arduino Uno R3 was used as a microcomputer to receive data from each sensor and to measure capacitance.

3.3 Procedure

Similar to code-based authentication, opening gestures are designed by individual users. Therefore, similar to existing research [29,30], we asked the participants to freely design their preferred opening gestures for authentication and analyzed the features they exploited in the design of their own opening gestures.

After explaining our idea to the participants, they were asked to design opening gestures. The instruction was, "Please design opening gestures for authentication in this scenario that you would like to use in real life." To inspire participants to design their own opening gestures, we introduced them to seven features frequently used in other gestures and pressure-based interaction methods [19,21,25], such as Code-Length (number of times to turn the doorknob), Touch-Pressure, Number-of-Fingers (for grasping the doorknob), Touch-Duration, Finger-Identity (order of the fingers used to touch the doorknob), Gripping-Hand (e.g., both hands or right hand) and Touch-Location. During the design, the participants were encouraged to include any other features they liked and were free to test their gestures until they were satisfied. After this, the participants were asked to reveal their gestures by demonstrating them to the experimenter and noting them in the questionnaire. They were also asked to describe the features they had used in their designs in the questionnaire. Then, each participant performed the gestures they designed 20 times (Fig. 1b), which involved performing them 10 times, taking a 60-seconds break, and then performing them another 10 times.

3.4 Results

In total, we collected 11 opening gestures (9 participants × 1 gesture +1 participant × 2 gestures). Table 1 and Fig. 2 show the gestures that were noted in the questionnaire. Although the participants were allowed to use any features they liked, almost half of the gestures (designed by P1, P3, P4, P6, and P10) were based on opening motions without many distinctive features.

Table 1. Opening gestures designed by the participants. Note that P2 designed two gestures.

Participant	Opening Gesture
P1	Placing the thumb on the shaft and turning normally
P2	Grasping the doorknob with the left hand and turning it once. Grasping the doorknob firmly with the left hand and turning it downward
P3	Turning the doorknob using the little finger, ring finger, and middle finger
P4	Turning the doorknob for roughly 0.5 s with enough grip strength for turning it, with the fingers other than the thumb of the right hand, placing each finger between its second and third joints on the handle
P5	Touching the inside of the lever, then touching the outside and turning it once
P6	Grasping the doorknob by the left hand, with the thumb under the doorknob, and then turning it quickly
P7	Grasping the doorknob from the little finger to the index finger and then turning it
P8	Without thinking, turning the doorknob with the right hand in the shape of a thumb-up
P9	Grasping the doorknob, turning it once, returning it to its original position, and turning the doorknob again
P10	Holding the knob with the base of the fingers other than the thumb and turning it with the thumb in a neutral position in the air

There was an average of 4.00 features (SD = 1.10) used in the design of eash gesture. Figure 3a shows the number of gestures that were leveraged each feature. In total, Code-Length was the most frequently used feature (used by all participants). Meanwhile, roughly half of the gestures leveraged Touch-Pressure, Number-of-Fingers, Finger-Identity, Gripping-Hand, and Touch-Location. In comparison, Touch-Duration was only used in a few gestures.

We analyzed the distribution of the features in the gestures, as shown in Fig. 3b. Because Finger-Identity and Touch-Location were dependent on other features, we did not analyze these two features. As shown in Fig. 3b, the Code-Length of 90% of gestures was only 1, implying that the participants favored short gestures. Of the Touch-Pressure 75% included a neutral grip, suggesting

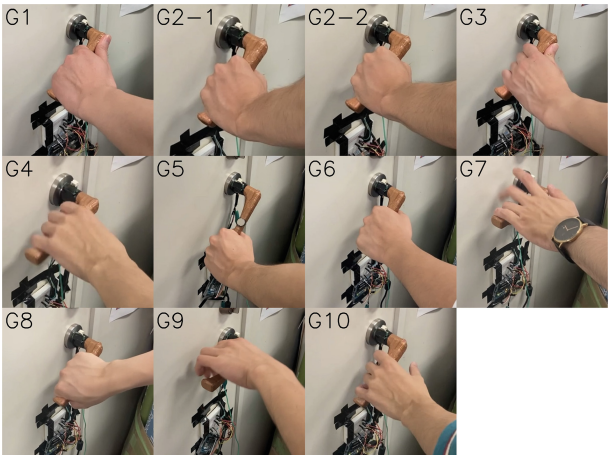

Fig. 2. Gestures designed by the participants.

that participants were not very concerned with pressure. Similarly, 100% of the Touch-Duration was 0.5 s, suggesting that participants were not very concerned about the duration. Regarding Number-of-Fingers, 86% of gestures leveraged four or more fingers, while 14% leveraged three fingers suggesting that the participants preferred opening gestures with a stable grip. Half of the Gripping-Hand gestures were performed with either hand, suggesting that both the left and right hands could be used to turn the doorknob. However, the participant who did not mention the hand for gestures opened the door with their left hand in this experiment, since the doorknob used was a left-opening type.

3.5 Feature Visualization

Eleven sensors (a capacitive sensor, a pressure sensor, three axis acceleration sensors, three axis gyro sensors, and three axis magnetic sensors) were used to measure the motion of the opening gestures (Fig. 1a). Similar to Ohmura et al. [23], we obtained a feature vector of 56 dimensions (11 sensors $\times$ 5 features + 1 duration feature), with fatures being the mean, variance, standard deviation, kurtosis, and skewness of 11 sensors, and the duration of the gestures. The principal component analysis (PCA) showed that the cumulative contribution rate exceeded 50% after the fourth principal component (Fig. 4). Among the 56 features, we extracted 31 by selecting those with an absolute value of main component scores of 0.2 or higher (Fig. 5). Another PCA was performed on the 31 extracted features. Figure 6 shows the results of dimension reduction down to the second principal component to examine how the participant data were distributed. As this figure shows, the data were spread out for each participant, suggesting the possibility that these 31 features could discriminate between participants.

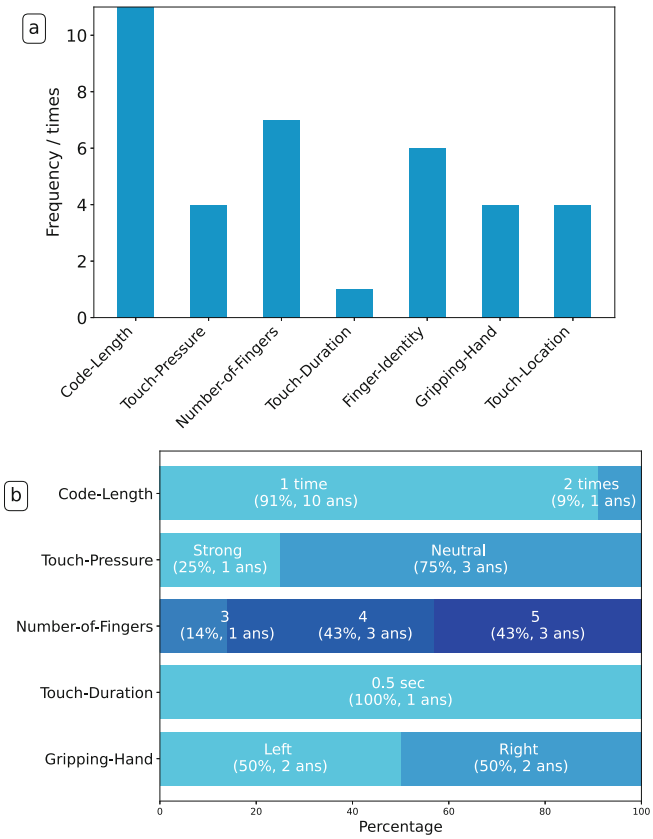

Fig. 3. Analysis of the features used in the gestures in Table 1. (a) The number of gestures with different features. (b) Distribution of the features.

3.6 Machine Learning

The results of 10-fold cross-validation using Random Forest with 31 features are summarized in Table 2. G1 denotes the gesture designed by P1. Since P2 designed two gestures, G2-1 and G2-2 are shown. This table shows that even similar gestures (G3, G4, G6, G10) can be classified with a precision rate of 0.94 or higher. This also shows that complex gestures (G1, G2-2, G5) can be classified with a precision rate of 0.87 or higher. However, some gestures (G2-1, G7, G8) were shown to be inaccurate, with a precision rate of 0.48 or lower. In the future, these inaccurate gestures should be analyzed.

4 Experiment: Shoulder Hacking

To explore whether it is possible to reject gestures made by *nonusers*, we conducted another experiment to examine the vulnerability of opening gestures to shoulder hacking.

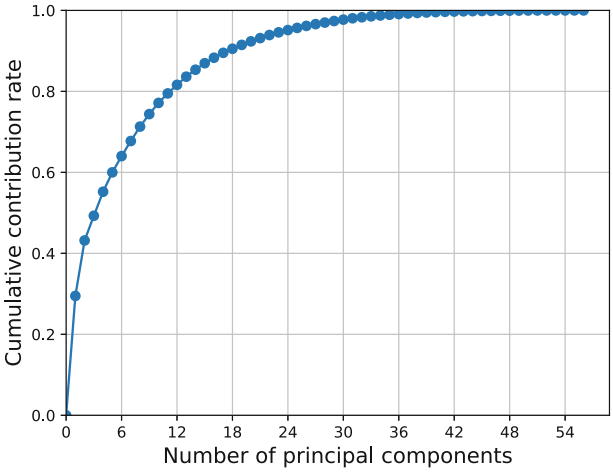

Fig. 4. Cumulative contribution rate changes.

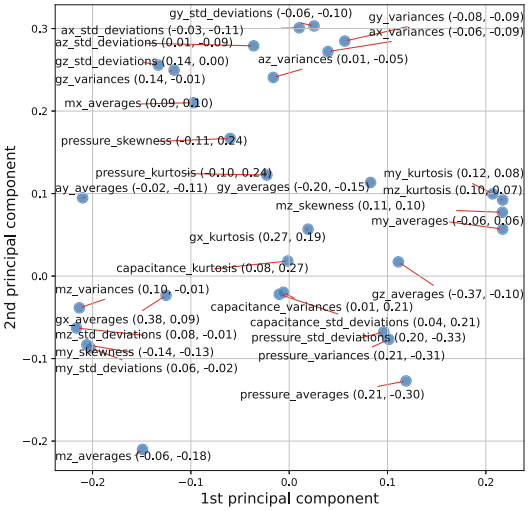

Fig. 5. PCA performed on 56 features. We plotted 31 features whose absolute value of principal component score was 0.2 or more. The numbers in parentheses are the scores of the third and fourth principal components.

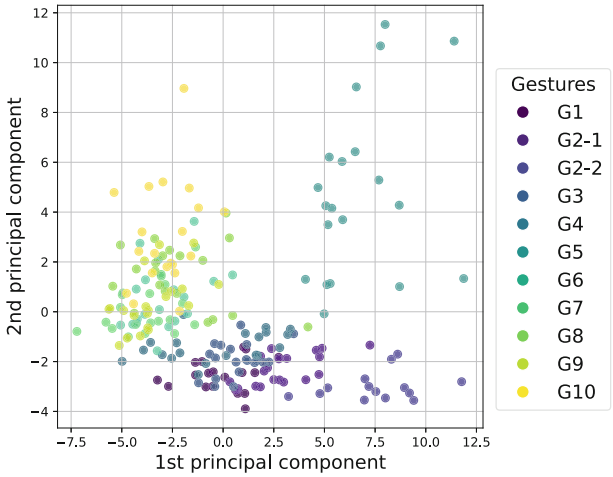

Fig. 6. PCA performed on 31 extracted features. G1 denotes the gesture designed by P1. Since P2 designed two gestures, G2-1 and G2-2 are shown.

Table 2. Authentication performance. Gesture G1 denotes the gesture designed by P1. Since P2 designed 2 gestures, G2-1 and G2-2 are shown.

Gesture	G1	G2-1	G2-2	G3	G4	G5	G6	G7	G8	G9	G10	Average
Precision rate	0.875	0.483	1.000	1.000	1.000	1.000	0.941	0.250	0.700	0.727	1.000	0.816
F-measure	0.778	0.571	0.963	0.974	0.919	1.000	0.865	0.187	0.467	0.516	0.750	0.726
FAR	0.010	0.077	0.000	0.000	0.000	0.000	0.005	0.046	0.015	0.015	0.000	0.015

4.1 Participants

We recruited eight participants from the same laboratory as the authors (all male, M = 22.8 y.o., SD = 0.66 y.o.) as volunteers. Six were right-handed, one was left-handed, and one was ambidextrous.

4.2 Procedure

The same door used in Sect. 3 was used to collect the data. The experiment consisted of the following two phases.

Data Collection. Three out of the eight participants (*users*) participated in the data collection. As in Sect. 3.3, we asked the participants to freely design their desired opening gestures for authentication.

After we had explained our idea to the participants, they were asked to design opening gestures. The instruction was, "Please design opening gestures for authentication in this scenario that you would like to use in real life." To inspire the participants to design their own opening gestures, we introduced

them to the seven features mentioned earlier. In their designs, the participants were encouraged to include any other features they liked and were free to test their gestures until they were satisfied. After this, they were asked to reveal the gestures by noting them in the questionnaire. They were also asked to enumerate the features they had used in their design among the seven features in the questionnaire. Then, each participant performed their designed gesture 20 times (Fig. 1b), by performing it 10 times, taking a 60-s break, and then performing it another 10 times. The participants' hand movements were video recorded (Fig. 7).

Hacking. After the data collection, we conducted a hacking experiment. Five participants (*nonusers*) who had not participated in the data collection took part in this experiment, which was divided into two sessions.

In the first session, the participants were asked to watch a video (Fig. 7) recorded during the data collection and imitate the three gestures designed by the *users*. While imitating the gestures, they were asked seven features used in the gestures by filling in the questionnaire used in Sect. 4.2. Then, each participant performed each of the three gestures 20 times.

In the second session, the participants were asked to imitate the gestures by watching the video and the seven features answered by the *users* in the data collection. Then, the participants performed each of the three gestures 20 times.

Fig. 7. Example of a gesture video.

4.3 Results

In total, we collected three opening gestures (3 *users* × 1 gesture). Table 3 shows the gestures designed by the *users*, that had been noted in the questionnaires.

We counted the features in these gestures (Fig. 8). Because Finger-Identity and Touch-Location were dependent on other features, we did not count them. As shown in Fig. 8b, *nonusers* could roughly estimate the *users*' gestures. There is no difference in the distribution of Code-Length, Number-of-Fingers, and

Table 3. Opening gestures designed by the *users* in the data collection.

User	Opening Gesture
U1	Quickly moving the doorknob down, standing for roughly 0.5 s, and then attempting to open it by turning
U2	Holding the tip of the doorknob, touching it with the thumb in the shape of a thumbs-up, turning it twice, and releasing
U3	Turning the doorknob with the thumb applying force to the thumb

Gripping-Hand, suggesting that these were easy to estimate by *nonusers*. The Touch-Pressure was 3 (neutral) or higher by *users*, whereas 20% of Touch-Pressure was 2 (slightly weak) by *nonusers*, suggesting that nonusers estimated the pressure to be weaker. The Touch-Duration ranged from 1.0 to 2.0 s by the *users*, while it ranged from 0.5 to 1.5 s by *nonusers*, suggesting that *nonusers* estimated gestures to be shorter. However, Touch-Pressure and Touch-Duration are subjective, with a possibility that the participant's subjective and actual pressure differed.

4.4 Feature Visualization

As in Sect. 3, we performed a PCA to examine how the participant data were distributed. Figure 9 shows the results of dimension reduction down to the second principal component. In this figure, U1 denotes the gestures designed by the *users* #1. NU1 denotes the gesture imitated by the *non-user*. 'only-video' denotes the first session, in which non-users watched only the gesture video. 'video&info' denotes the second session, in which *nonusers* watched the gesture video and the features mentioned by the *users*. As Fig. 9 shows, the data were spread out for each participant, suggesting the possibility that these features could classify participants. In particular, U3 is scattered with the 1st principal component = 5.0 or higher, while *nonusers* gestures that imitate *users* (NU1-NU5 in Fig. 9c) are classified with the first principal component = 5.0 or less. This indicates that it may be difficult to imitate even if videos and features are open.

4.5 Machine Learning

We performed authentication by classifying between *users* and *nonusers* using Random Forest. The results are summarized in Table 4. Due to an imbalance in *users* and *nonusers* data, we used a Balanced Random Forest. The ratio of test data to training data was 0.5, indicating that the results show the performance of our system when a user registered their own gesture 10 times on the doorknob of the user's private room.

In this analysis, we conducted two simulations. The first is to test if *nonusers* could open the door by imitating *users*' gestures. To this end, we trained a model with 10 *users* gestures and 200 *non-users*' gestures imitating the *users*' gestures and the model with the rest of the data (U1 vs. NU1, U2 vs. NU2, and U3

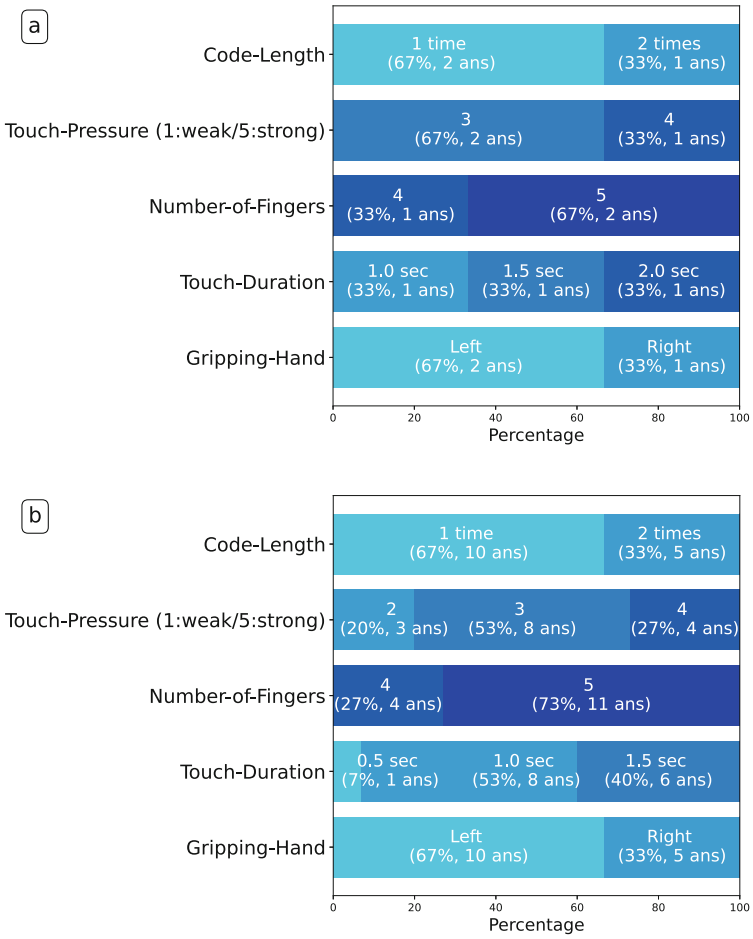

Fig. 8. Analysis of the features used in the designed gestures. (a) Distribution of the features by the *users* in the first session. (b) Distribution of the features estimated by the *nonusers* in the second session.

vs. NU3). The second simulation was to test if *nonusers* could open the door by performing random gestures, including the ones where *nonusers* imitated *users*' gestures. To this end, we trained a model with 10 *users*' gestures and 300 *nonusers*' gestures and tested it with the rest of the data (U1 vs. all-NU, U2 vs. all-NU, and U3 vs. all-NU).

The average accuracy and TAR by *users* and *nonusers* (U vs. NU) was 0.988. All FARs were 0.000, showing that *users* were not misclassified as *nonusers*. The average accuracy for *nonusers* authentication (U vs. all-NU) was 0.975. The average FAR was 0.025, meaning that other *users*' gestures imitated by *nonusers* were misclassified as *users*' gestures.

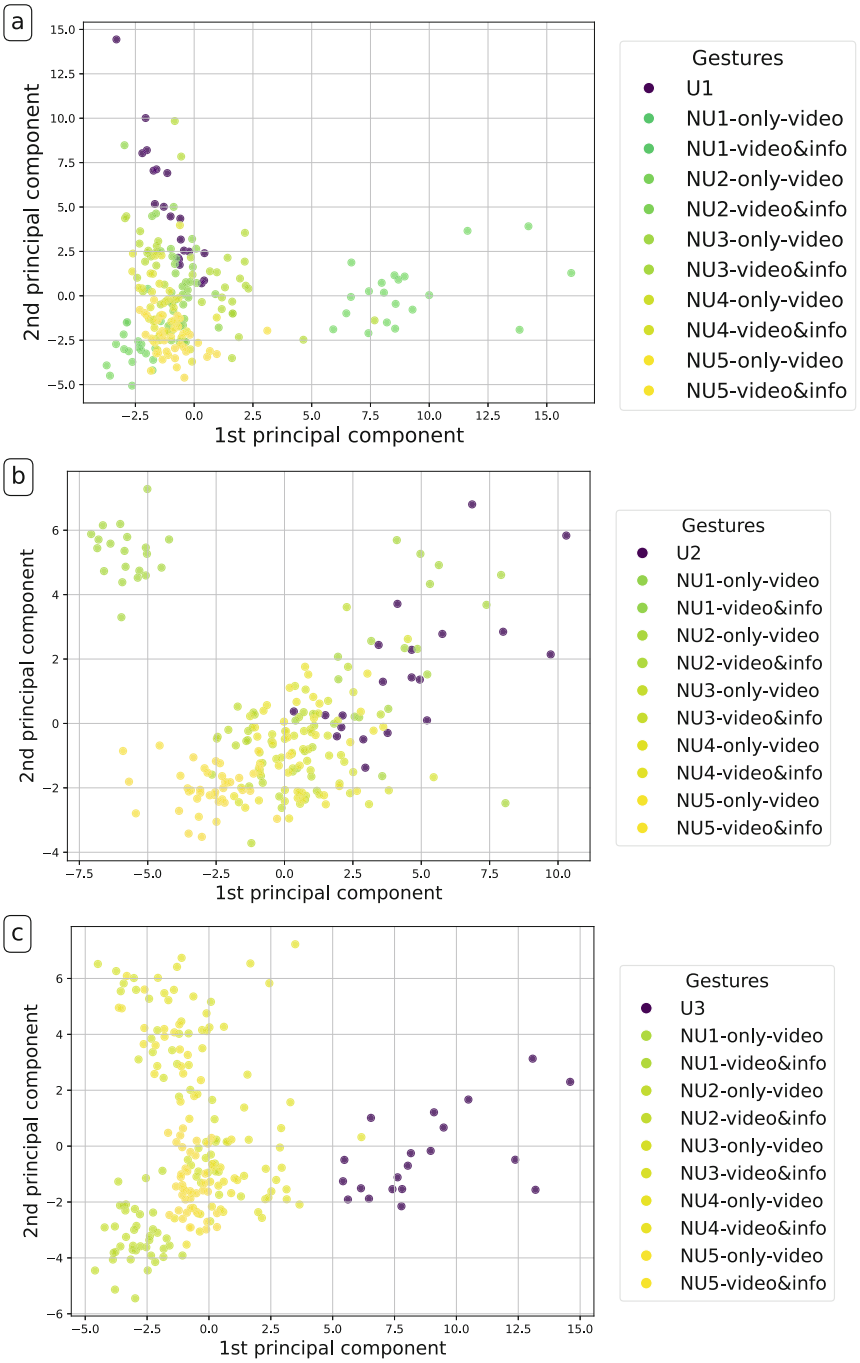

Fig. 9. PCA performed on the extracted features. Dimensions were compressed to the second principal component and displayed. (a) PCA on the data obtained when *nonusers* imitated U1. (b) PCA when *nonusers* imitated U2. (c) PCA when *nonusers* imitated U3.

U1 vs. all-NU had the highest accuracy among all *users*. However, the U1 vs NU1 accuracy was lower than that of U3 vs. NU3. U3 vs. NU3 had the highest accuracy among other *users*, while U3 vs. all-NU had the lowest accuracy among all *users*. This result shows a trade-off between imitation resistance and overall authentication accuracy.

Table 4. Classification between *users* and *nonusers*.

Performance	U1 vs. NU1	U2 vs. NU2	U3 vs. NU3	U1 vs. all-NU	U2 vs all-NU	U3 vs all-NU
Accuracy rate	0.982	0.982	1.000	1.000	0.980	0.946
Precision rate	1.000	1.000	1.000	–	–	–
Recall rate	0.800	0.800	1.000	–	–	–
F-measure	0.889	0.889	1.000	–	–	–
TAR	0.982	0.982	1.000	–	–	–
FAR	0.000	0.000	0.000	0.000	0.020	0.054

5 Discussion and Future Work

Opening Gestures in Authentication. In Sect. 3, we analyzed the opening gestures based on *users*' preferred features. In Sect. 4, we showed that our system has a FAR of 0.000 for *nonusers* imitated gestures and an average FAR of 0.025 for all *nonusers* gestures. Therefore, the opening gestures have the potential to be used for authentication.

User-Designed Gesture Implications. In Sect. 3, Code-Length, Number-of-Fingers, and Finger-Identity were the most preferred features when designing opening gestures. This result not only supports the design of our system but could also direct interaction techniques based on opening gestures (e.g., recognizing persons entering/leaving and operating IoT devices to control lights or to play music when a door is opened/closed).

Future Work. We showed Code-Length, Number-of-Fingers, and Finger-Identity to be the most preferred features. However, there is a possibility that other features (e.g., Touch-Pressure, Touch-Duration) might not align well with our system. We plan to improve the system to sense other features during opening and explore the feasibility of using these features. In addition, our participants were highly homogeneous in terms of age. Validating the performance with added participants is also needed. Furthermore, since opening gestures could change over time, even if users intentionally intend to maintain them, a long-term evaluation of our system is necessary.

6 Conclusion

We presented an authentication method using opening gestures.

Analyzing the participants' defined gestures showed that Code-Length, Number-of-Fingers, and Finger-Identity were the features they preferred the most. Our system was implemented on a door, testing its authentication performance on data from 10 participants. Capacitive sensors, pressure sensors, and an IMU were used to measure the movements of the gestures. The results showed that a Random Forest with 11 gestures could reach an average precision rate of 0.816 and an average FAR of 0.015.

Our shoulder hacking experiment with 8 participants showed that our system archived a FAR of 0.000 for the imitated gestures by *nonusers*. An average FAR of 0.025 for all gestures was shown. For these reasons, the *users* and *nonusers* performance also showed that there might be a trade-off between imitation resistance and overall authentication accuracy.

In the future, we will use a system that senses more features to verify the actual performance. Additionally, we will examine the system's performance by long-term evaluation, since opening gestures might change over time.

References

1. Abbas, G., Humayoun, S.R., AlTarawneh, R., Ebert, A.: Simple shape-based touch behavioral biometrics authentication for smart mobiles. In: Proceedings of the 2018 International Conference on Advanced Visual Interfaces, AVI 2018, pp. 50:1–50:3. Association for Computing Machinery (2018)
2. Ali, A.B.A., Ponnusamy, V., Sangodiah, A.: User behaviour-based mobile authentication system. In: AC3S 2019, Advances in Computer Communication and Computational Sciences, pp. 333–343 (2019)
3. Andriotis, P., Tryfonas, T., Oikonomou, G.: Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 115–126. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-319-07620-1_11
4. Azimpourkivi, M., Topkara, U., Carbunar, B.: Camera based two factor authentication through mobile and wearable devices. Proc. ACM Interact. Mob. Wearable Ubiq. Technol. **1**(3), 35:1–35:37 (2017)
5. Buriro, A., Crispo, B., Delfrari, F., Wrona, K.: Hold and sign: a novel behavioral biometrics for smartphone user authentication. In: 2016 IEEE Security and Privacy Workshops (SPW), pp. 276–285 (2016)
6. no Centeno, M.P., Guan, Y., van Moorsel, A.: Mobile based continuous authentication using deep features. In: Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning, EMDL 2018, pp. 19–24. Association for Computing Machinery (2018)
7. Cornelius, C., Peterson, R., Skinner, J., Halter, R., Kotz, D.: A wearable system that knows who wears it. In: Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys 2014, pp. 55–67. Association for Computing Machinery (2014)

8. Feng, T., et al.: Continuous mobile authentication using touchscreen gestures. In: 2012 IEEE Conference on Technologies for Homeland Security (HST), HST 2012, pp. 193–198. Institute of Electrical and Electronics Engineers (2012)
9. Guo, A., Xiao, R., Harrison, C.: CapAuth: identifying and differentiating user handprints on commodity capacitive touchscreens. In: Proceedings of the 2015 International Conference on Interactive Tabletops & Surfaces, ITS 2015, pp. 277–280. Association for Computing Machinery (2015)
10. Gupta, S., Buriro, A., Crispo, B.: Demystifying authentication concepts in smartphones: ways and types to secure access. Mob. Inf. Syst. **2018**, 2649598:1–2649598:16 (2018)
11. Gupta, S., Buriro, A., Crispo, B.: SmartHandle: a novel behavioral biometric-based authentication scheme for smart lock systems. In: Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications, ICBEA 2019, pp. 15–22. Association for Computing Machinery (2019)
12. Ehatisham-ul Haq, M., et al.: Authentication of smartphone users based on activity recognition and mobile sensing. Sensors (Basel, Switzerland) **17** (2017)
13. Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., Wagner, D.: Smart Locks: lessons for securing commodity internet of things devices. In: ASIA CCS 2016, pp. 461–472. Association for Computing Machinery (2016)
14. Holz, C., Buthpitiya, S., Knaust, M.: Bodyprint: biometric user identification on mobile devices using the capacitive touchscreen to scan body parts. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI 2015, pp. 1419–1428. Association for Computing Machinery (2015)
15. Krombholz, K., Hupperich, T., Holz, T.: Use the Force: evaluating force-sensitive authentication for mobile devices. In: Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security, SOUPS 2016, pp. 355–366. USENIX Association (2016)
16. Kudo, M., Yamana, H.: Active authentication on smartphone using touch pressure. In: Adjunct Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology, UIST 2018, pp. 55–57. Association for Computing Machinery (2018)
17. Lee, W.H., Lee, R.B.: Implicit smartphone user authentication with sensors and contextual machine learning. In: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 297–308. IEEE Computer Society (2017)
18. Liu, J., Song, W., Shen, L., Han, J., Ren, K.: Secure user verification and continuous authentication via earphone IMU. IEEE Trans. Mob. Comput. **21**(9), 2017–2030 (2022)
19. Luca, A.D., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and i know it's you! implicit authentication based on touch screen patterns. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2012, pp. 987–996. Association for Computing Machinery (2012)
20. Masuno, R.: Passwords and cognitive psychology. IPSJ SIG Techn. Rep. **2010-CSEC-49**(1), 1–6 (2010)
21. Murao, K., Tobise, H., Terada, T., Iso, T., Tsukamoto, M., Horikoshi, T.: Mobile phone user authentication with grip gestures using pressure sensors. In: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, MoMM 2014, pp. 143–146. Association for Computing Machinery (2014)
22. Nakanishi, I.: Biometric modality challenges and future prospects. IEICE ESS Fund. Rev. **16**, 185–195 (2023)

23. Ohmura, R., Naya, F., Noma, H., Kogure, K.: Architectural overview of a sensor network for supporting nursing activities. IPSJ SIG Tech. Rep. **2009**(8), 1–8 (2009)
24. Pelto, B., Vanamala, M., Dave, R.: Your identity is your behavior - continuous user authentication based on machine learning and touch dynamics. In: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), pp. 1–6 (2023)
25. Quinn, P., Lee, S.C., Barnhart, M., Zhai, S.: Active edge: designing squeeze gestures for the Google Pixel 2. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–13. Association for Computing Machinery (2019)
26. Rilvan, M.A., Chao, J., Hossain, M.S.: Capacitive swipe gesture based smartphone user authentication and identification. In: 2020 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), CogSIMA 2020, pp. 1–6. Institute of Electrical and Electronics Engineers (2020)
27. Rodriguez, S.D., Mecke, L., Alt, F.: SenseHandle: investigating human-door interaction behaviour for authentication in the physical world. In: SOUPS 2022, USENIX Symposium on Usable Privacy and Security (2022)
28. Saini, B.S., et al.: A three-step authentication model for mobile phone user using keystroke dynamics. IEEE Access **8**, 125909–125922 (2020)
29. Vatavu, R.D., Wobbrock, J.O.: Clarifying agreement calculations and analysis for end-user elicitation studies. ACM Trans. Comput.-Hum. Interact. **29**(1), 5:1–5:70 (2022)
30. Yi, X., et al.: Squeez'In: private authentication on smartphones based on squeezing gestures. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI 2023, pp. 532:1–532:15. Association for Computing Machinery (2023)
31. Zhang, C., Li, S., Song, Y., Meng, Q., Lu, L., Hou, M.: BioTouch: reliable re-authentication via finger bio-capacitance and touching behavior. Sensors **22**(3), 655:1–655:16 (2022)