Two-Factor Authentication Using Leap Motion and Numeric Keypad

Tomoki Manabe[1(✉)] and Hayato Yamana[2,3(✉)]

[1] Graduate School of Fundamental Science and Engineering, Waseda University, Shinjuku-ku, Tokyo, Japan
tomoki_manabe@yama.info.waseda.ac.jp
[2] Faculty of Science and Engineering, Waseda University, Shinjuku-ku, Tokyo, Japan
yamana@yama.info.waseda.ac.jp
[3] National Institute of Informatics, Chiyoda-ku, Tokyo, Japan

Abstract. Biometric authentication has become popular in modern society. It takes less time and effort for users when compared to conventional password authentication. Furthermore, biometric authentication was considered more secure than password authentication because it was more difficult to steal biometric information when compared to passwords. However, given the development of high-spec cameras and image recognition technology, the risk of the theft of biometric information, such as fingerprints, is increasing. Additionally, biometric authentication exhibits lower and less stable accuracy than that of password authentication. To solve the aforementioned issues, we propose two-factor authentication combining password-input and biometric authentication of the hand. We adopt Leap Motion to measure physical and behavioral features related to hands. Subsequently, a random forest classifier determines whether the hand features belongs to a genuine user. Our authentication system architecture completes the biometric authentication by using a limited amount of data obtained within a few seconds when a user enters a password. The advantage of the proposed method is that it prevents intrusion by biometric authentication even if a password is stolen. Our experimental results for 21 testers exhibit 94.98% authentication accuracy in a limited duration, 2.52 s on an average while inputting a password.

Keywords: Hand-based authentication · Multi-factor authentication · Behavioral biometrics

1 Introduction

Recently, extant studies note the vulnerability of password authentication [1]. Although there is an increase in incidents caused by password leakage (such as SNS account hacking), biometric authentication systems are common as a new authentication method. A few biometric authentication methods are practically used, such as fingerprint authentication, iris authentication, and face authentication, which are implemented on smartphones. Biometric authentication involves less time and effort for users when compared with conventional password authentication. Furthermore, biometric

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 38–51, 2019.
https://doi.org/10.1007/978-3-030-22351-9_3

authentication was considered more secure than password authentication because it was more difficult to steal biometric information when compared to passwords [2]. However, the risk of theft of biometric information is increasing with the development of high-spec cameras and image recognition technology. For example, smartphones that use fingerprint authentication are unlocked by a fake fingerprint created from fingerprints that remain on the touch screens [3]. In contrast to passwords, biometric information cannot be changed, and thus it is difficult to reuse biometric information as an authentication key once it is stolen. Another problem is that the authentication accuracy is lower and less stable than the password authentication because biometric authentication uses a device such as a camera or an infrared sensor. More specifically, even with the same authentication device, the authentication accuracy can be affected by sunlight or dirt on the device [4].

To solve the aforementioned problems, behavioral features are used for biometric authentication. Chan et al. [5] proposed a biometric authentication system that uses Leap Motion [6], and the method of [5] adopted the geometric structure and movement of a user's hand as physical and behavioral features. Experimental results for 16 testers indicated 99.97% classification accuracy. Although they achieved a low error rate, it took more than 25 s for the authentication. Other biometric authentication methods [7–10] using behavioral features of hand were also examined. They used motion for handwriting and signatures written in air. However, the studies exhibit less accuracy when compared to that of [5] and is approximately in the range of 86.57% to 98.82%.

The remaining problem is that extant studies [5, 7, 9] require a long time for authentication. To shorten the authentication time without decreasing accuracy, we propose a new method that enables authentication in a limited duration by simultaneously extracting both features, i.e., physical and behavioral features of hand. Our authentication system architecture completes biometric authentication by using a limited amount of data obtained within a few seconds when a user enters a password, i.e., two-factor authentication combining password-input and biometric authentication of hand. We adopt Leap Motion to measure physical and behavioral data of hands. Subsequently, random forest classifiers determine whether hand data belongs to a genuine user. The advantage of the proposed method is that it prevents intrusion via biometric authentication even if a password is stolen.

The structure of the study is as follows. In Sect. 2, we provide an overview of Leap Motion. In Sect. 3, we describe biometrics research that uses Leap Motion. In Sect. 4, we explain the outline of the proposed method. In Sect. 5, we discuss details of experiments, results of the system evaluation, and results. Finally, the study is summarized in Sect. 6.

2 Overview of Leap Motion

Leap Motion is an optical 3D sensor that tracks the geometric structure of hand and finger movements. In hand tracking, Leap Motion first irradiates infrared rays to an object as tracked. Subsequently, Leap Motion acquires the data related to the hand and fingers by measuring the reflection time of irradiated infrared rays. Leap Motion is

normally placed vertically upwards in a horizontal place. Leap Motion can recognize both hands and ten fingers independently in units of 0.01 mm.

In this paper, we used Leap Motion to measure the length of hand bones, width of fingers, and velocity vectors of each finger based on the tip of a finger. In the study environment, Leap Motion is performed 60 times per second. Thus, Leap Motion can measure a user's hand data 60 times per second and save the measurement result. In the study, the time taken by Leap Motion to measure hand data once is expressed in units corresponding to "frame". Hence, a frame is 1/60 s in the study (Fig. 1).

Fig. 1. Leap motion

3 Related Work

In the section, we describe related studies on biometric authentication using Leap Motion.

3.1 Biometric Authentication Using Gesture

Chan et al. [5] proposed a biometric authentication system using gestures for authentication at login of personal computer and on-line authentication in 2015. Their study consisted of two parts. The first part involved temporary authentication assuming scenes where users use Leap Motion for login authentication. The second part discussed online authentication. The on-line authentication assumes that the user browses web pages as a situation of practical use.

With respect to temporary authentication at login, a user initially holds his hands over the Leap Motion for 25 s. Subsequently, the system determines who the user is by analyzing physical features of his/her hands. When the user is determined as a genuine user, the user is requested to draw a circle with one finger to obtain behavioral features. The physical features consist of the width and length of the hands, arms, metacarpals, and phalanges of each finger. The behavioral features include the radius of the drawn circle, time taken for the gesture, and acceleration of finger movements. The results for the experiments with 16 testers indicate that the authentication accuracy (1 – Equal Error Rate) of static authentication using the random forest algorithm corresponds to 99.97%.

In online authentication, a user engages in an application run on a PC to control both cursors and seek bars via gestures. Both physical and behavioral features related to the hand are recorded to authenticate. The results of the experiments for 10 testers indicate that the value of authentication accuracy (1 - EER) corresponds to 98.39% in online authentication.

3.2 Biometric Authentication Using Handwriting in Air

Tian et al. [7] proposed a challenge-response authentication method using in-air handwriting in 2017. Their proposed method (hereafter, MoCRA) aims to deal with insider attacks by combining challenge-response authentication and biometric authentication. In its authentication phase, MoCRA asks a user to write a randomly chosen string in air to capture the movements of his/her hand via Leap Motion. Specifically, the random string corresponds to "challenge" in challenge-response authentication. After completing the writing part, MoCRA extracts the user's features as "response" in challenge-response authentication. By using the behavioral feature of users as a part of the "response," MoCRA can prevent imposter's attacks, while normal challenge-response authentication is unable to deal with attacks from an individual who knows the password. Experimental results for 24 testers indicate 98.82% authentication accuracy although a persistent issue is that it takes an average of 17.5 s to write the requested string.

In the same year (2017), Kamaishi et al. [8] proposed a biometric authentication system by adopting handwritten signatures. The biometric authentication combined a handwritten signature itself and features obtained from the hand when a user signs in air. The aim involved realizing changeable biometric authentication via adopting a handwritten password (i.e., signature) and biometric information. In the proposed method, the trait and speed of fingers measured by Leap Motion was used for authentication purposes. In [8], they performed experiments to track simple movements of a finger drawing (i.e., a straight line) as the initial stage of the proposed method. The results indicate that their system achieved 86.57% authentication accuracy.

Another example of handwritten signature biometrics system corresponded to the study by Xiao et al. (2016) [9]. They conducted experiments to examine the effect of user authentication using physical and behavioral features captured via Leap Motion. They initially constructed a system that authenticates based on biometric data of the user's hand structure and behavioral features when a user provided their signature in front of the sensor. The experimental data was collected from 10 testers, and the experimental results were evaluated via false rejection rate (FRR), false acceptance rate (FAR), and equal error rate (EER). Specifically, EER corresponds to the error rate when FRR and FAR are equal. The result of experiments indicated that they achieved an average EER of 34.80% by using physical features of the hand and an average EER of 3.75% by using behavioral data for handwriting. However, in the method, users can begin to provide their signature only when Leap Motion recognizes a maximum of two fingers because the method assumes that a user only extends their index finger or thumb. Hence, [9] may involve a long time period for authentication.

Additionally, Nigam et al. [10] proposed a system that is combined with handwritten signature and face authentication in 2014. By combining handwritten signature

and face authentication, they intended to increase the accuracy of authentication compared to handwritten signature or face authentication only. In their experiments, they collected data from 60 testers and achieved a genuine acceptance rate (GAR) of 91.43%.

3.3 Summary of Related Work

Figure 2 shows the graph of the classification accuracy (1 - EER) values in previous studies [5, 7–10]. The result of EER was not described in the study by [10], and thus value of GAR of [10] was graphed as a reference.

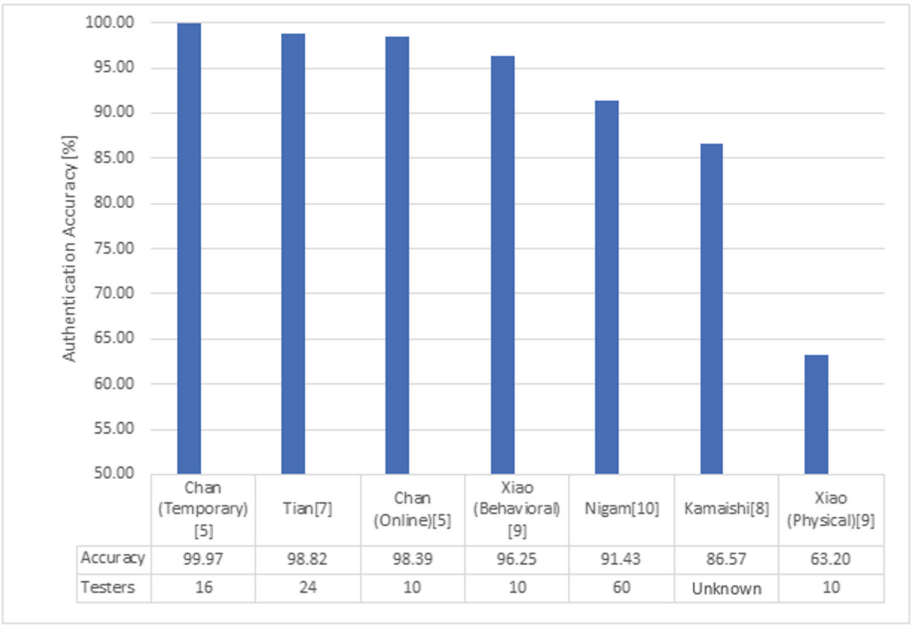

Fig. 2. Comparison of the authentication accuracy of each study

As shown in Fig. 2, Chan et al. [5] achieved the highest accuracy by adopting both the hand structure recognized by Leap Motion and the random forest classifier. The results indicated that the hand structure is indispensable for authentication and that the random forest classifier works well. However, the main three studies exhibit the disadvantage wherein the authentication is a time-consuming process.

4 Proposed Method

4.1 Overview of the Proposed Method

We propose two-factor authentication with Leap Motion and numeric keypad termed as *Hand and Password Combination Authentication* (hereafter, HPCA). Specifically, we assume the environments where a user inputs a numeric password into a system such as an ATM and door locker keypad. Figure 3 shows the flowchart of HPCA. In HPCA, Leap Motion simultaneously acquires hand geometry data and hand movement data. When the password is completely input, the system initially determines whether the password is correct or not. Subsequently, random forest classifier determines whether or not a user is an imposter based on the data obtained from Leap Motion.

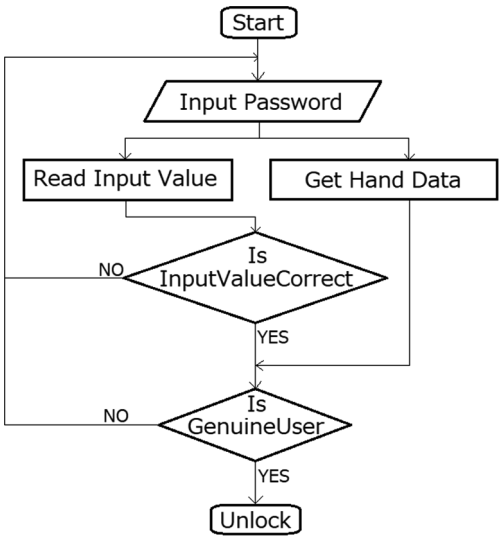

Fig. 3. Flowchart of HPCA

4.2 Purpose of HPCA

As a scene for the practical use of HPCA, we assume a situation such as unlocking doors or using an ATM. Although extant studies [5] realize high recognition accuracy of 99.97%, a potential issue is that authentication takes at least 25 s. Therefore, the aim involves shortening the time required for authentication and subsequently improving its practicality. Specifically, we aim to construct a system that can perform biometric authentication with a limited amount of data that is collected within a short time period while a user enters a password into a numeric keypad.

To enable authentication in a short time, we only adopt the features that are obtained during password input (such as within a few seconds) to authenticate. Table 1 shows the features used for our biometric authentication. While the password is input into a numeric keypad, it is essential to prevent the invasion of a third party. Therefore, we

focus on reducing a false acceptance rate (FAR) among authentication errors. The errors in authentication include false rejection (FR) that falsely recognizes a genuine user as a third party and false acceptance (FA) that falsely recognizes a third party as a genuine user. Specifically, the objective involves decreasing the false acceptance rate (FAR) by allowing classifiers to learn the maximum possible number of other individuals' data.

Table 1. Features used for authentication (40 features)

Feature	Explanation
Length of phalanges and metacarpals (19 features)	Length (mm) of the distal phalanx, median phalanx, and basal bone of each finger Length of metacarpal bone other than thumb (mm)
Width of each finger (5 features)	Unit: mm
Maximum, minimum, and average value of each finger speed (15 features)	Maximum, minimum, and average value (mm/s) of the speed of the tip of each finger
Duration of password input (1 feature)	Unit: second

4.3 Authentication Method

In this section, we describe how HPCA is performed by using information obtained from Leap Motion. In HPCA, Leap Motion acquires hand geometry data and hand movement data when a user enters the password. Next, a random forest classifier determines whether the user has the right to open a key.

The classification method is as follows: First, a classifier is constructed for each genuine user. Each classifier outputs 1 iff the given features belong to the genuine user and 0 iff not. We assume that the user takes n frames to enter the password, Leap motion measures the same features n times while the user enters password. For each of the n data sets, the classifier determines whether or not the data set belongs to a genuine user. Subsequently, only when the number of data sets wherein the user is determined as a genuine user is equal to or more than the threshold value th, then the classifier concludes that the user is a genuine user and finally outputs 1. Specifically, the parameter th is determined based on the data set for parameter adjustment. While concluding that the user is not a genuine user, the classifier outputs 0.

4.4 Summary of the Proposed Method

In the section, we explain the outline and objective of HPCA. Our proposed method corresponds to two-factor authentication with Leap Motion and numeric keypad. We assume that unlocking a door or using an ATM corresponds to a scene where HPCA is practically used. The purpose of HPCA involves improving safety when compared to password authentication by itself by combining biometric authentication with password authentication. To achieve the purpose of the study, we consider a method to realize *short-term authentication* and *low FAR*. To shorten the authentication time, we adopt the data that is sufficiently obtained in a short time while entering password to authenticate. Additionally, to achieve low FAR, various individuals' data are used in learning as third party data to train the classifier.

5 Experimental Evaluation

5.1 Data Collection

Figure 4 shows the experimental environment to collect biometric data. In the experiment, 21 testers were asked to perform three trials of authentication procedure to input random four digit numbers displayed on the screen 25 times via a numeric keypad. Specifically, the random numbers are assumed as the password and they simulate a random key pad to eliminate any side-effects of input key positions. The three sets of procedures (i.e., three sets of inputs were considered 25 times wherein each asks a tester to input random four digit numbers) were prepared to examine the difference when testers possessed more experience related to inputting the password.

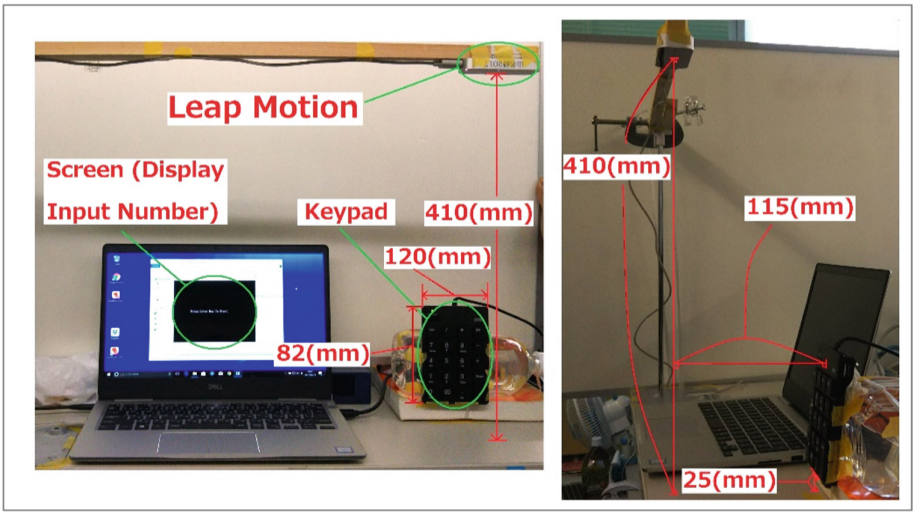

Fig. 4. Experimental environment

When the testers input passwords, the physical and behavioral data related to their hands were measured. The physical and behavioral data consist of 40 features as shown in Table 1. We constructed 21 random forest classifiers wherein each is trained to determine whether or not the given data belongs to a genuine user.

5.2 Verification of Measurement Error Range of Leap Motion

As a preliminary experiment, we examine the measurement error range of Leap Motion by using data collected from testers to confirm whether we can adopt the lengths of the phalanges and metacarpals as features. In the verification, we used input data obtained from 21 testers 525 times (i.e., 25 inputs per person). Specifically, each input data consists of 19 features because the total number of phalanges and metacarpals is 19 per hand. Furthermore, each input data consists of several frames because Leap Motion output data is observed 60 times per second. Thus, we term each observed data as a frame data.

With respect to each set of frame data when inputting a password, we calculate the difference between the maximum and minimum values of the lengths of the phalanges and metacarpals. Subsequently, we assume the difference as measurement error. Leap Motion recognizes hand in units of 0.01 mm based on its specification, and thus we separate the measurement error less than 0.01 mm and above. Figure 5 shows the result of the distribution of measurement errors. The verification results indicate that the ratio above an error of 0.01 mm is 15.09%.

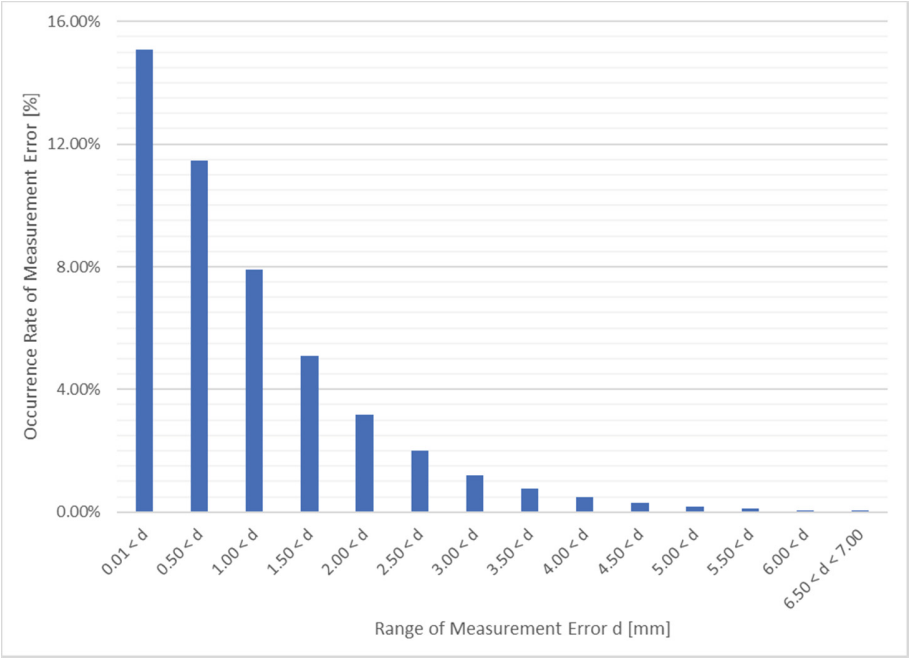

Fig. 5. Relationship between range and measurement error rate

Specifically, we reconsider whether the lengths of the phalanges and metacarpals as measured by Leap Motion during password input are useful as biometric authentication features. The results indicate that (1) the length of the phalanges and metacarpals of adults approximately corresponds to several tens of millimeters, (2) the rate at which the measurement error in the password input corresponds to 0.01 mm or less is 84.91%, (3) the maximum measurement error is less than 7 mm, and (4) the ratio of the measurement error of 1 mm or less is 92.09%. Hence, it is determined that the measurement results of Leap Motion with respect to the user's hand during password input can be adopted as the features of biometric authentication.

5.3 Evaluation of HPCA

With respect to the evaluation of HPCA, the classification accuracy of the classifiers is verified.

Evaluation Criteria. We calculate FRR, FAR, and error rate (ER) as evaluation indexes of the system. Specifically, nTrue, nFalse, nFR, and nFA are defined as follows:

nTrue: number of test data of genuine users
nFalse: number of test data of third parties
nFR: number of FRs that occur
nFA: number of FAs that occur

Subsequently, FRR, FAR, and ER are expressed as follows.

$$\mathrm{FRR} = \frac{\mathrm{nFR}}{\mathrm{nTrue}} \tag{1}$$

$$\mathrm{FAR} = \frac{\mathrm{nFA}}{\mathrm{nFalse}} \tag{2}$$

$$\mathrm{ER} = \frac{\mathrm{nFR} + \mathrm{nFA}}{\mathrm{nTrue} + \mathrm{nFalse}} \tag{3}$$

In the study, classification accuracy is expressed as a percentage (%) of 1 - ER.

Features. We adopt 40 features as shown in Table 1. In the experiment, the cue to finish the password input is defined as pressing the enter key after inputting a random four-digit password. It also corresponds to the cue to display the next password on the display to ask a tester to input the next password. If it takes n frames (where 1 frame is 1/60 s) from the beginning to the end while inputting the password, then the number of frame data generated for a password input corresponds to n. Each frame data consists of both the length of the bones of the fingers and the width of each finger. Besides, the maximum, minimum, and average values of the speed of the finger movement and duration of password input are calculated after the password input is completed.

Training. We construct 21 random forest classifiers with m decision trees (m = 1, 2, …, 200). Each classifier is trained by the training data set which consists of a genuine data and the other 19 users' data, each of which includes 20 password input data. Here, in each password input, we use the first five frames as training data to shorten the training phase. Here, we have confirmed the accuracy stays same even if we increase the number of flames. During the training, we exclude the remaining one user's data because it is used as other user's test data which is not included in the training data.

Test. We examine the accuracy of 21 random forest classifiers with m decision trees (m = 1, 2, …, 200). Each classifier is evaluated by the test data set which consists of a genuine data and other user's data that were not used for training. Here, each user's data includes 5 password input data that exclude 20 password input data already used for training. In each password input, we use the first 70 flames, because the minimum value of time for testers to enter a 4-digit password was 1.22 s (>73 frames) in the experiment. Then, the accuracy was averaged by whole test.

Effectiveness of Each Feature. We examine the effectiveness of each feature used on classification. First, we exclude the i ($1 \leq i \leq 40$) th feature from the data set used in evaluation experiment. Subsequently, both training and test are performed in the same procedure as the evaluation experiment in the case of 40 features. Let A be the maximum value of the classification accuracy with 40 features and let A_i [%] be the classification accuracy in the case where the i-th feature is excluded. Specifically, the effectiveness of the i-th feature is defined as follows:

$$A - A_i[\%] \tag{4}$$

As shown in Eq. (4), it is considered that the feature with larger effectiveness more contributes to improving classification accuracy.

5.4 Experimental Result

In the section, we first discuss the evaluation results of the classification accuracy of HPCA with 40 features and without features having negative effectiveness value. Subsequently, we detail the evaluation results of effectiveness of each feature.

Classification Accuracy. Table 2 summarizes the classification accuracy with all features and without features with a negative effectiveness value. As shown in Table 2, FAR worsens although FRR and total accuracy improve if negative features are excluded.

Table 2. Classification accuracy

Experiments	All features (P)			w/o negative features (Q)			Diff. of Acc. Q-P [%]
	Accuracy [%]	FAR [%]	FRR [%]	Accuracy [%]	FAR [%]	FRR [%]	
First trial	90.19	1.78	17.84	90.37	5.4	13.87	0.18
Second trial	89.65	2.32	18.38	91.02	5.61	12.34	1.38
Third trial	93.98	1.49	10.54	94.98	1.93	8.11	1.00

Analysis of the Effectiveness of Each Feature. Figures 6 and 7 show the effectiveness of each feature. Generally, physical features are more effective than behavioral features. Specifically, behavioral features are effective when users get used to the password input, i.e., at the third trial, three out of 11 behavioral features contribute to increase the total accuracy.

5.5 Discussion

As mentioned in Sect. 4.2, the study focuses on preventing invasion of third parties. In the section, we consider practicality and safety of HPCA based on the experimental results.

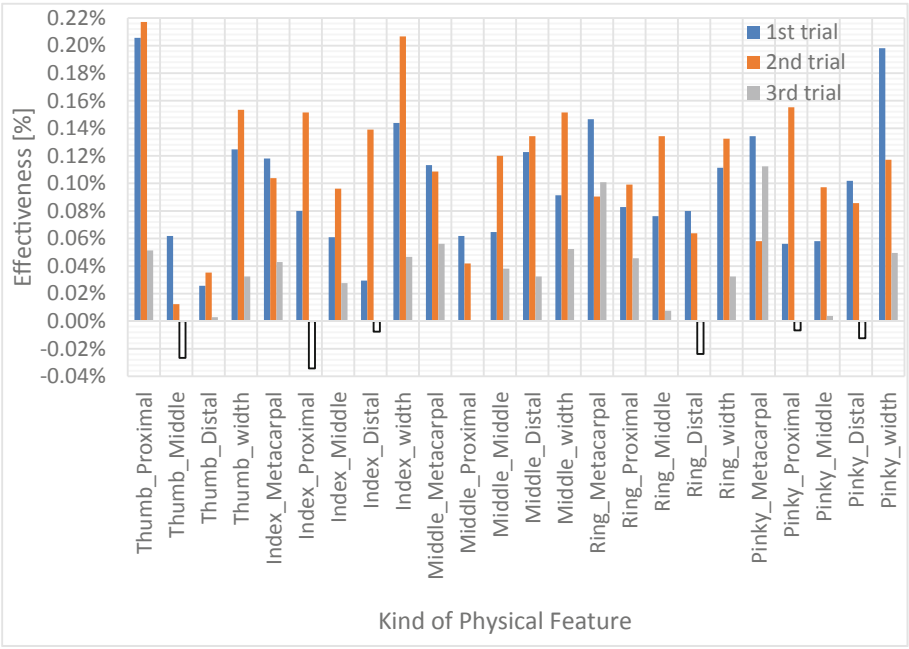

Fig. 6. Effectiveness of physical features

As shown in Table 2, FRR worsens (18.38%) when we use the dataset in the second trial with all features. However, the probability that false rejection occurs n consecutive times is represented as follows:

$$(0.1838)^n \tag{5}$$

Thus, the probability of being rejected twice consecutively corresponds to 3.38%, and the probability of being rejected three consecutive times corresponds to 0.62%. Thus, even when FRR is 18.38%, it is sufficiently possible to unlock by reentering the password several times.

Conversely, the optimal value of FAR corresponds to 1.49% and the worst value of FAR corresponds to 5.61%. If the probability that a third party is accepted by a one-time input is p%, then the probability that a third party is rejected n consecutive times when the third party inputs the correct password n times is as follows:

$$(1-p)^n \tag{6}$$

Figure 8 shows the relationship between the number of inputs and the rejection rate of others.

As shown in Fig. 8, when a third party enters the correct password 50 times, the probability of breaking through the key is 52.79% in the case of the optimal FAR and 94.42% in the case of the worst FAR. However, in the case of the optimal FAR, the

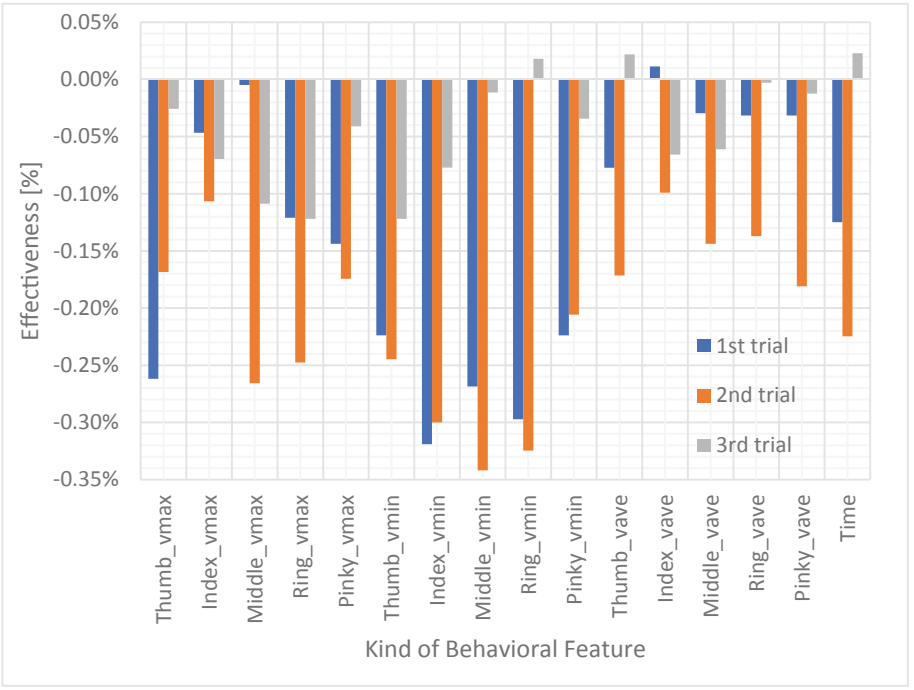

Fig. 7. Effectiveness of behavioral features

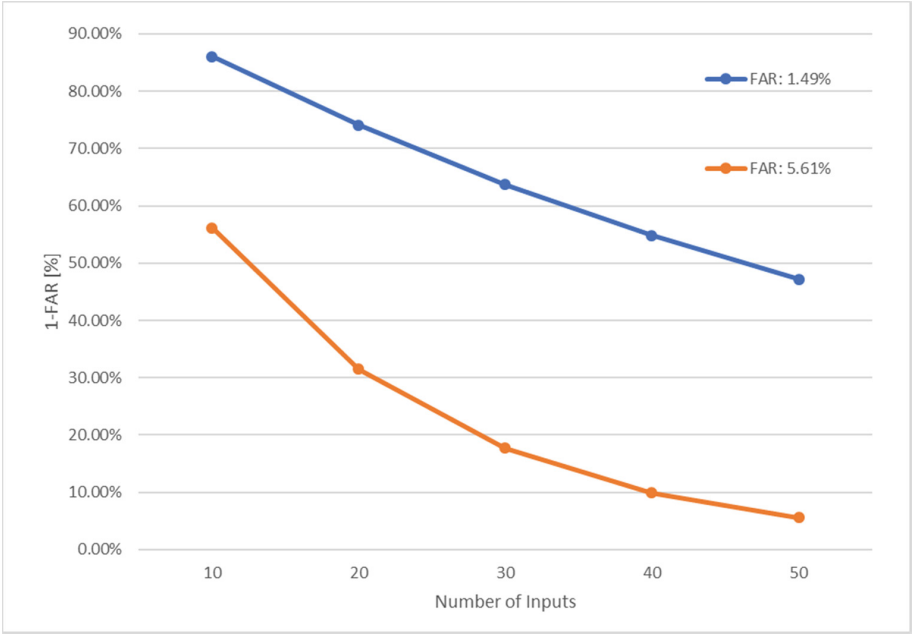

Fig. 8. Relationship between the number of inputs and the rejection rate of others

probability of preventing a third party from breaking through the key from 10 to 50 times is superior to that in the case of the worst FAR by 41.01% on an average.

6 Conclusion

In the study, we first described a previous study on biometric authentication using Leap Motion. In the case of biometric authentication using Leap Motion, previous studies realized recognition accuracy exceeding 99%, and this shows that Leap Motion can be used for biometric authentication. However, increases in the accuracy required increase in the time necessary to perform authentication.

The aim of the study is to perform biometric authentication using limited data obtained from Leap Motion while entering the password. In the experiment, we confirmed whether authentication can be performed with data obtained in a short time. Thus, the results indicated that our proposed method can perform biometric authentication with an accuracy of 94.98% by using the data obtained within the limited time while entering the password.

A future study will further investigate biometric authentication using Leap Motion and improve the authentication method so that it is more useful.

References

1. Masuno, R.: Passwords and cognitive psychology. IPSJ CSCE **49**(5), 1–6 (2010)
2. Biometric market to grow 21% by 2014 – SecureIDNews. https://www.secureidnews.com/news-item/biometric-market-to-grow-21-by-2014/. Accessed 30 Dec 2018
3. Chaos Computer Club breaks Apple TouchID – Chaos Computer Club. http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid. Accessed 2 Jan 2018
4. Kawahara, H., Kouno, A., Nakamoto, A., Endo, J., Yasuhiro, M.: High speed/high accuracy face recognition sensor corresponding to ambient light. In: Technical Report of Panasonic Electric Works, vol. 57 (2), pp. 10–15. (2009)
5. Chan, A., Halevi, T., Memon, N.: Leap motion controller for authentication via hand geometry and gestures. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2015. LNCS, vol. 9190, pp. 13–22. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-20376-8_2
6. Leap Motion – LEAP MOTION, Inc. https://www.leapmotion.com/. Accessed 2 Jan 2018
7. Tian, J., Cao, U., Xu, W., Wang, S.: Challenge-response authentication using in-air-handwriting style verification. IEEE Trans. Dependable Secure Comput. (2017) https://doi.org/10.1109/tdsc.2017.2752164
8. Kamaishi, S., Uda, R.: Biometric authentication by handwriting with single direction using self-organizing maps. In: Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication, Article No. 106 (2017)
9. Xiao, G., Milanova, M., Xie, M.: Secure behavioral biometric authentication with Leap Motion. In: Proceedings of IEEE 4th ISDFS 2016, Article No. 7473528 (2016)
10. Nigam, I., Vatsa, M., Singh, R.: Leap signature recognition using HOOF and HOT features. In: Proceedings of 2014 IEEE International Conference on Image Processing, pp. 5012–5016 (2014)