A Study on System Architecture of Smart Lock Based on Authentication of Door Knocking Motion Using Machine Learning

Kakeru Nakabachi[†], Yoshitaka Nakamura[‡], and Hiroshi Inamura[‡]

[†]Graduate School of Systems Information Science, Future University Hakodate, Japan
[‡]School of Systems Information Science, Future University Hakodate, Japan
{g2119031, y-nakamr, inamura}@fun.ac.jp

Abstract - With the development of the Internet of Things (IoT) technologies, smart home systems that provide residents with a more comfortable lifestyle are attracting attention. One of the technologies that make up a smart home system is called Smart lock which allows users to use their smartphones to lock and unlock the doors of their homes instead of a physical key. Smart lock can improve the convenience of locking and unlocking doors. On the other hand, if a resident's smartphone is stolen, there is a risk that a malicious person could break into the user's home., because current Smart lock does not authenticate whether the user who is trying to unlock is the owner of the smartphone. As an approach to this problem, we have been studying personal authentication method using features of the door-knocking motions, which is a natural motion that the user can perform in front of the door. In this paper, we evaluated the performance of the proposed authentication method by calculating F-measure, precision rate, recall rate, and False Acceptance Rate (FAR) for various features that can be obtained from door-knocking motions by using various multi-class classification algorithms in machine learning.

Keywords: door knock, smart home, IoT, authentication, smart lock

1 INTRODUCTION

In recent years, with the development of Internet of Things (IoT) technologies, smart home systems that provide residents with a more comfortable lifestyle have been attracting a lot of attention. Smart home systems enable residents to operate home appliances such as air conditioners from outside using their own smartphones by installing IoT-compliant home appliances called smart home appliances at home. As one of such smart home services, there is a service called Smart lock that locks and unlocks the user's home door using a smartphone application instead of a physical key. Some Smart lock services have already been commercialized, and some of them can be installed externally on the thumbturn of an existing door to realize a Smart lock service without the need for large-scale construction [1] [2]. In addition to locking and unlocking using a smartphone, which is the main function of the Smart lock service, there are several other functions, such as a hands-free unlocking function that allows users to unlock the door by approaching it using their location information, and a function that allows users to share access privileges with family and friends. These functions improve the convenience of locking and unlocking the door. On the other hand, each function of the current Smart lock service is performed based on the prior pairing of the Smart lock product and the smartphone, and does not authenticate whether or not the user is the owner of the smartphone. Therefore, if the smartphone is stolen by someone who knows the user's address in advance, or if the smartphone is stolen along with the driver's license with the user's address, etc., there is a risk that a malicious person could break into the user's home. As a countermeasure against these problems, personal authentication near the door is necessary.

Conventional authentication technologies that can be used in front of door include possession-based authentication"what you have", knowledge-based authentication"what you know", and biometric authentication"what you are". Possession authentication is a technology that uses a physical device owned by the user, such as a physical key or an IC card, to authenticate the user. Knowledge authentication is an authentication technique that uses knowledge in user's memory, such as inputting a pre-registered password for authentication. There are two types of biometric authentication that use physical characteristics and behavioral characteristics. Biometric authentication using physical features uses other features of the human body such as fingerprints, face, irises, and so on. Biometric authentication using behavioral features uses features that appear in human behavior such as walking motion, typing motion on a keyboard, or opening motion and closing motion a door. There are advantages and disadvantages to each of these authentication technologies. In the case of possession authentication, users can be authenticated relatively easily using a physical key or IC card. However, if these devices are stolen or lost, personal authentication becomes impossible and there is a risk that someone other than the user will break the authentication. Knowledge authentication is a widely used authentication technology, such as unlocking a smartphone. However, there is a burden on the user's memory, such as the need to remember passwords. In addition, there is a high risk of password theft due to shoulder hacking, etc. Biometric authentication using physical features does not have memory burden such as remembering passwords, since it uses the unique features of the human body. However, because it is nearly impossible to change physical features, it is difficult to deal with the use of replicated physical feature information. In addition, it is necessary to register a part of the body information as a feature using a special device, which is a large psychological burden on the person. Biometric authentication using behavioral features extracts user-specific features from user actions. Therefore, the authentication cannot be broken unless another person makes the same motion as the user. However, it is difficult to select features to obtain sufficient authentication accuracy. On the other hand, there is a advantage that the features for authentication can be acquired implicitly, such as walking authentication.

In the current commercialized Smart locks, the user approaches the door and locks and unlocks the door at a short distance through Bluetooth, etc., using a smartphone that is paired with the Smart lock device in advance. In other words, the Smart lock device is the keyhole and the smartphone is the key corresponding to the keyhole. Since this is possession-based authentication, it also has the disadvantages of possession-based authentication.

We focus on the door-knocking motion, which is considered to be a behavioral feature that can be performed spontaneously in front of the door and is less burdensome for the motion. In this paper, we propose a door-knock type personal authentication system using biometrics based on personal features detected by door knocking motion. The proposed method is expected to increase the security strength by combining two-factor authentication with biometric authentication using behavioral features, and possession authentication which is performed by existing Smart locks.

The issues of this study can be broadly classified into the following four categories.

- Consideration of system configuration
- Investigation of features that are useful for authentication
- Assessment of resistance to peek-a-boo attacks
- Consideration of extension methods for registered action data

First, it is necessary to study how to handle the acquired motion data and how to configure the system to authenticate the user accurately and correctly. Second, it is necessary to investigate effective features for accurate authentication, which can be obtained from door knocking motions. Third, we need to investigate the resistance of the door knocking motions to being imitated by others when the door knocking is observed by a camera or directly by prying eyes. Fourth, in order to ensure sufficient authentication accuracy with a small amount of registration motion data, it is necessary to consider the extension method of registration motion data.

In addressing these issues, we have investigated the possibility of selecting individual-specific features from door knocking motions in a previous study. In this paper, we report the results of our research on the consideration of the system configuration and the investigation of effective features for authentication.

2 RELATED WORK

2.1 Authentication Using Behavioral Features

There are some existing authentication methods [3] [4] based on the spatial motion detection using an accelerometer of a mobile terminal or a wristwatch-type device. Patterned actions such as drawing characters and figures in space, and left hook punching are used as authentication motions using a special device. In addition, researches on rhythm authentication [5] [6] have been proposed. The user registers a patterned rhythm according to the music he or she has listened to beforehand, and the user is authenticated by recalling and reproducing the rhythm pattern at the time of authentication. Thus, there are some biometric authentication methods using behavioral features that require memory burden by asking the user to recall the registration pattern at the time of authentication. For the convenience of users, it is desirable to eliminate these memory burdens. On the other hand, there are methods to authenticate and identify individuals without placing a memory burden on the user by using natural behaviors in daily life, such as walking [7], typing on a keyboard [8], opening and closing doors [9], and rolling up toilet paper [10]. Based on these findings, the proposed method uses the individual features included in the natural knocking motions of daily life, rather than the unnatural knocking rhythm defined for authentication to identify the registration pattern, and removes the memory burden of recalling at the time of authentication.

2.2 Authentication of Smart Door Lock Systems

With regard to Smart locks, many studies have been conducted on smart door lock (SDL) systems [11] [12] [13] [14]. Each of these systems proposes its own hardware for door locking and a method for unlocking the door. An SDL system equipped with a touch panel on the door [11] proposes an authentication method in which the user enters a password on the touch panel as authentication when the door is unlocked. In addition, an SDL system [12] has been proposed to unlock door using the one-time password method from a logged-in smartphone application. This method uses knowledge authentication, which results in a large memory burden when unlocking the door. The SDL system [13] that unlock the door automatically when a device with access authorities enters the setting area achieves seamless door unlocking without making the user aware of the operation for authentication. However, when a device with registered access authorities is lost, it is necessary to log in to the web application and delete the registered devices. In addition, a function to authenticate the user and unlock the door using fingerprint authentication [13] has been proposed at the same time. However, since it uses physical features, there is a risk of spoofing if replicated. In addition, there is a significant psychological burden on the user due to the use of specialized devices to obtain fingerprints. An SDL system [14] uses a Passive Infrared Ray(PIR) motion sensor installed on the door to detect the presence of a person in front of the door, and notifies the door administrator to unlock the door. However, the cost of installing the sensor on an existing door and the user who receives the notification has to give permission to unlock the door each time. Sato et al. proposed an SDL system called the Intelligent Doorknob System, which is equipped with palmprint authentication using a Web camera installed on the doorknob [15]. This makes it possible to unlock the door lock seamlessly without making the user aware of the authentication operation. However, since 150 times SIFT (Scale Invariant Feature Transform) calculations are performed for a single authentication, the current authentication speed is not practical. And the cost of installing a Web camera on the doorknob is also incurred. As described above, many existing SDL systems have problems in terms of user's memory burden, psychological burden, and installation cost. Therefore, an authentication method that requires as little burden on the user as possible and does not require the installation of special equipment is needed.

3 PROPOSED SMART LOCK SYSTEM

3.1 Proposed system

In the proposed system, the user is authenticated by using a multi-class classification algorithms in machine learning through a series of processes shown in Fig. 1 after receiving 3-axis acceleration data and 3-axis angular velocity data obtained from the user's door-knocking motion. The Smart lock system installed at home and the smartphone are paired with Bluetooth in advance. The system first investigates whether or not the paired terminals can be authenticated using proximity detection of BLE (Bluetooth Low Energy). By using the distance measurement of the BLE, it is possible to detect the distance between the smartphone and the Smart lock by distinguishing the distance of more than 1 m (Far), about 1 m (Near), and less than 1 m (Immediate). The proposed system permits the authentication by door knock operation only when the BLE detects ”Immediate”. The door knock motion data acquired by the smartphone sensors at this time is pre-processed with noise removal and feature extraction. Only when the extracted features are determined to be the user's own class by the multi-class classification algorithm, authentication is performed. The Smart lock can only be unlocked when the user is authenticated. Thus, in the proposed system, in addition to the element of possession-based authentication using a smartphone connected to a Smart lock in advance, the authentication can be enhanced by adding an element of biometric authentication using behavioral features by knocking on the door. The proposed system aims to remove the memory burden of remembering the registered pattern by extracting the unique features of the user from the natural door-knocking motion that user performs in daily life.

3.2 Assumed environment

In the proposed system, the feature of door-knocking motion is extracted by the user's smartphone and used for the authentication for unlocking a Smart lock. The proposed system does not install any sensor or device on the door, but uses the sensor built into the smartphone. It is possible to reduce the time and cost to prepare a new dedicated device by using the device that users always carry in their daily lives. The smartphone acquires data from a 3-axis accelerometer and a 3-axis angular velocity sensor. Figure 2 shows the door-knocking motion and the direction of each axis of each sensor.

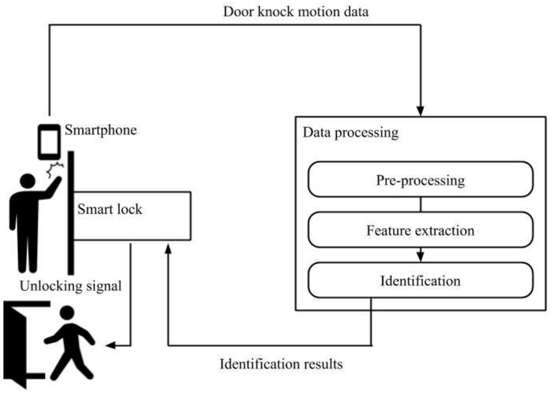

Figure 1: System overview

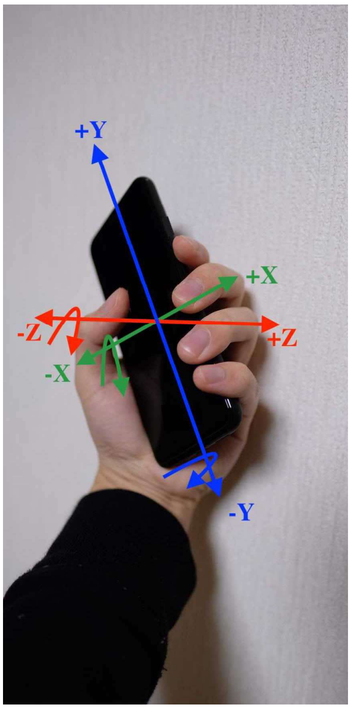

Figure 2: Door knock motion and the axial direction of each sensor

3.3 Pre-processing

In the pre-processing, the 3-axis acceleration data and 3-axis angular velocity data were trimmed to remove the noise except for the actual data. After that, a low-pass filter was applied to each to, to remove the small noise contained in the actual operating data. The result is shown in Fig. 3.

3.4 Feature extraction

From the door-knock motion data obtained in the above environment, the proposed system extracts features that are useful for personal authentication. We have shown that individual-specific features can be extracted from natural door-knocking motions that do not allow for special patterning [16]. The results show that the basic statistics of maximum, minimum, mean, variance, and standard deviation obtained from the 3-axis acceleration and 3-axis angular velocity data and the fea-

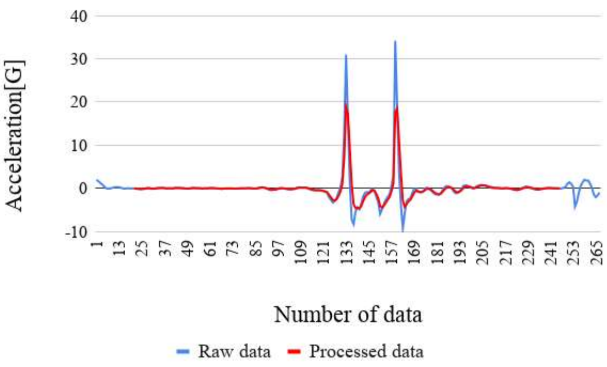

Figure 3: Pre-processing result

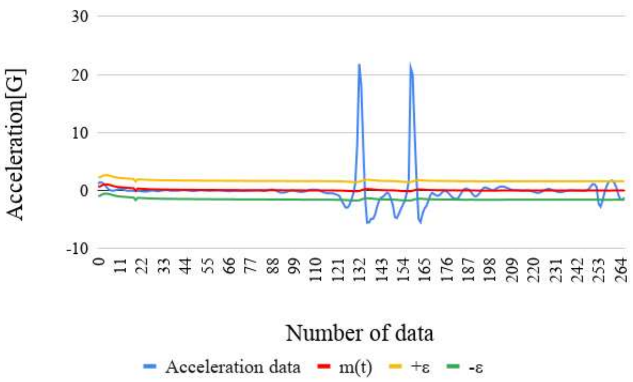

Figure 4: Applying the peak extraction algorithm

Table 1: The types of features

Name	Features	Number of items
3-axis acceleration	3-axis acceleration (max・min・mean・ variance・standard deviation）	15
3-axis angular velocity	3-axis angular velocity (max・min・mean・ variance・standard deviation)	15
Knock peak	Knock peak width・ height・interval (mean・standard deviation)	6
3-axis synthetic acceleration	3-axis synthetic acceleration (max・min・mean・ variance・standard deviation)	5
Frequency spectrum	Frequency spectrum of 3-axis synthetic acceleration	100

turesobtained from the knock peak which is the impact peak at the time of door knock motion appearing in the acceleration data, are effective. However, using the number of knocks and the height and width of each knock as features derived from the knock peaks changes the dimensionality of the feature vectors composed of those features. Therefore, depending on the analysis method of the feature vectors, the same user could be identified as a different user if the number of knocks changed between the registered knocking motion and authentication motions.

In the proposed method, the peak extraction algorithm proposed by Murao et al [17] is used for the knock peak extraction. The results of applying the peak extraction algorithm are shown in Fig. 4. The peak extraction algorithm calculates the average value $m(t)$ in the past Δt seconds (window) from the current time t of the acceleration time series data. In contrast, as shown in Fig. 4, a region called the Epsilon tube is established above and below $m(t)$ with a width of $m(t) \pm \epsilon$, and the waveform from once the acceleration value goes out of the Epsilon tube region until it returns to the Epsilon tube region again is extracted as a peak. In the door-knocking motion, we apply this peak extraction algorithm to the z-axis because the door-knocking peak appears directly on the z-axis of acceleration. In this system, the mean, standard deviation and interval of the width and height of each knock peak are extracted as features. In addition, the basic statistics obtained from the 3-axis synthetic acceleration data are also extracted as features, and the frequency spectrum obtained by Fast Fourier Transform(FFT) of the 3-axis synthetic acceleration data is also extracted as features. The types of features that may be used in the proposed system is shown in Table 1. By combining these features, the feature vector patterns shown in Table 2 are finally created and used for identification, respectively. Since each element of the generated feature vectors has a different scale and cannot be treated as equivalent the proposed system normalizes each feature vector so that the mean value of each feature vector is 0 and the variance is 1.

3.5 Identification

For identification, we use a multi-class classification algorithm for machine learning. In our previous work [18], we proposed a method of identification using a machine learning anomaly detection algorithm, but it was not sufficiently accurate. This method uses an unsupervised learning discriminator for the anomaly detection algorithm. Therefore, it is considered that there was insufficient information to identify the data obtained from the door-knocking motion, which is more difficult to distinguish from other people than the walking motion. By labeling the data to be trained, it is much easier to detect anomalies than unsupervised learning. The classifier learn feature vectors extracted from the motion data by the owner of the Smart lock with the person's label. The feature vectors extracted from the actions by other people are labeled as other people's data and generate a classifier by training it. When a feature vector of a person is given as input to the generated classifier, it is classified as either the person or a stranger the result of the classification is used as the authentication result. The proposed method uses Support Vector Machine (SVM), Logistic Regression, Decision Trees, Random Forest and K Neighbors Classifier as the most commonly used multiclass classification algorithms. In a real system, an appropriate multi-class classification algorithm among these is used. When generating a classifier, if there is little other data for training, the resistance to unknown other data is not enough, and there is a possibility that the user may be mistakenly identified. Therefore, it is assumed that a plurality of other person's motion data sets are collected and used as the other person data for attaching the other person's label at the time of learning.

Table 2: Feature vector patterns

Pattern Number	Features
1	3-axis acceleration・ 3-axis angular velocity・ Knock peak
2	3-axis acceleration・ 3-axis angular velocity
3	3-axis acceleration
4	3-axis angular velocity
5	3-axis synthetic acceleration
6	3-axis synthetic acceleration・ 3-axis angular velocity・ Knock peak
7	Frequency spectrum
8	3-axis synthetic acceleration・ 3-axis angular velocity・ Frequency spectrum
9	3-axis acceleration・ 3-axis angular velocity・ Frequency spectrum
10	3-axis synthetic acceleration・ 3-axis angular velocity・ Knock peak・ Frequency spectrum
11	3-axis acceleration・ 3-axis angular velocity・ Knock peak・ Frequency spectrum

4 EXPETIMENTAL EVALUATION

A malicious person with a malicious intent to break into the home may attempt to authenticate with the Smart lock system. Therefore, it is necessary to evaluate the accuracy of classification of the learned data of others. It is also necessary to evaluate the accuracy of the classification of unknown other's data that the classifier has not yet learned to classify. In order to evaluate the effectiveness of the proposed method, the following two evaluations are conducted.

Evaluation 1 Combination evaluation of best feature vector patterns and multi-class classification algorithms

Evaluation 2 Evaluation of the effectiveness of features for the feature vector patterns obtained in Evaluation 1

4.1 Experiments

In order to evaluate the two evaluations mentioned above, we conducted an experiment with subjects. 7 male university students in their twenties were asked to complete 60 trials each. Subjects were instructed to perform a door-knocking motion with their hands while holding a smartphone, and were instructed to perform natural door-knocking motions in their daily lives, rather than special door-knocking motions. In terms of the number of knocks, we fixed the number of knocks to 2 for all trials, because many subjects knocked twice when they were asked to perform the door-knocking action without instruction from our previous experiment [16].

When knocking on the door, the user was instructed to hold the smartphone in the knocking position before starting the knocking motion, and to hold it still for about 1 second from the start of the data measurement until the start of the door-knocking motion and from the end of the door-knocking motion until the end of the data measurement. The above experiment was conducted on the steel door shown in Fig. 5, which is located in the Future University Hakodate and the motion data were obtained. The main specification of the smartphone used in the proposed method are shown in Table 3. An Android application was developed using Kotlin to obtain the door-knocking motion. In order to generate classifiers from feature vectors obtained from motion data, we tuned the parameters of the multi-class classification algorithm to maximize the mean F-measure beforehand, and used 40 out of 60 trial data for training and 20 for testing.

Table 3: Main specification of the smartphone

Item	Specification
Device	VAIO Phone JCI VA-10J
OS	Android 5.0.2
Weight	130g
Device size	71.3mm x 141.5mm x 7.95mm
Sensors	3-axis acceleration sensor and 3-axis angular rate sensor
Display size	5-inch
Sampling rate	200Hz

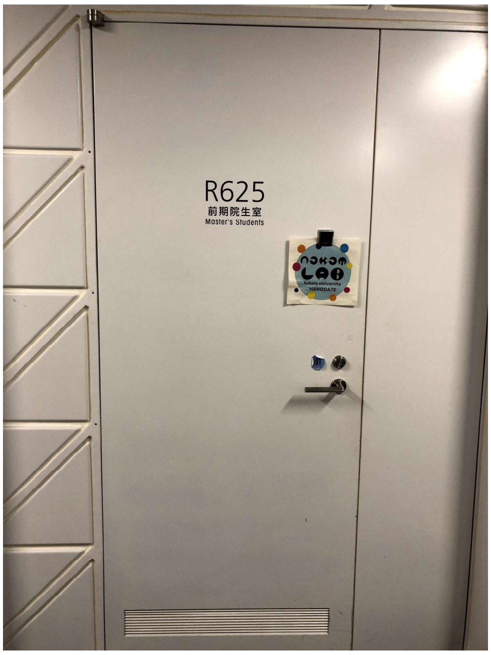

Figure 5: The door used in the experiment

4.2 Evaluation method

4.2.1 Evaluation 1

In Evaluation 1, we evaluate whether it is possible to correctly classify the learned person and others, and the accuracy of classification of unknown data that the classifier has not yet learned. We select one of the 7 subject's data as the authenticating user data, and split the data of the remaining 6 subjects into 3 other's data for training and the unknown data. The

Table 4: Results of mean F-measure, mean precision rate and mean recall rate for each feature vector pattern and multi-class classification algorithm

	SVM			Logistic Regression			Decision Trees			Random Forest			K Neighbors Classifier		
Pattern	F-measure	Precision rate	Recall rate	F-measure	Precision rate	Recall rate	F-measure	Precision rate	Recall rate	F-measure	Precision rate	Recall rate	F-measure	Precision rate	Recall rate
1	0.976	0.984	0.969	0.975	0.983	0.967	0.938	0.945	0.933	0.941	0.964	0.923	0.979	0.983	0.976
2	0.968	0.976	0.962	0.966	0.977	0.957	0.903	0.914	0.902	0.933	0.957	0.916	0.976	0.985	0.968
3	0.950	0.962	0.941	0.938	0.958	0.926	0.887	0.889	0.891	0.935	0.956	0.920	0.939	0.954	0.928
4	0.934	0.938	0.933	0.943	0.952	0.937	0.882	0.908	0.868	0.915	0.946	0.895	0.929	0.935	0.925
5	0.941	0.949	0.935	0.933	0.946	0.923	0.881	0.884	0.885	0.886	0.911	0.872	0.871	0.891	0.863
6	0.962	0.974	0.952	0.957	0.971	0.946	0.917	0.942	0.901	0.941	0.973	0.918	0.964	0.973	0.958
7	0.714	0.721	0.715	0.710	0.722	0.709	0.741	0.746	0.740	0.679	0.798	0.672	0.580	0.777	0.609
8	0.963	0.980	0.951	0.970	0.983	0.959	0.893	0.910	0.881	0.894	0.954	0.861	0.961	0.963	0.961
9	0.972	0.984	0.962	0.969	0.983	0.958	0.909	0.925	0.898	0.934	0.966	0.912	0.983	0.984	0.982
10	0.955	0.970	0.944	0.962	0.977	0.949	0.876	0.881	0.876	0.919	0.962	0.893	0.959	0.969	0.952
11	0.978	0.986	0.971	0.977	0.987	0.969	0.940	0.946	0.935	0.953	0.977	0.936	0.983	0.988	0.980

split between other's data and unknown data was done randomly. An evaluation is performed on the processed data by combining 11 feature vector patterns and 5 multi-class classification algorithms. A classifier is generated for each subject by supervised learning in which the data of the user to be authenticated is labeled with authenticating user and the data of another person is labeled with another person. Then, we evaluate whether it is possible to classify the known data correctly using the mean F-measure, the mean precision rate and the mean recall rate of the input data of the known person and others to all the identifiers generated. And to evaluate the classification accuracy of unknown data, we also evaluate the mean False Acceptance Rate (FAR) of untrained unknown data input to the classifier. Finally, to evaluate the best combination of the best feature vector pattern and the multi-class classification algorithm, we use the combination with the maximum value calculated using Eq. 1.

$$meanF\text{-}measure + (1 - meanFAR) \qquad (1)$$

Precision rate is the percentage of the data that the classifier predicts to be the person's identity, and recall rate is the percentage of the data that the classifier predicts to be the person's identity among the data that the classifier actually is. F-measure is the calculated harmonic mean of these values.

4.2.2 Evaluation 2

We already know that the feature vectors are effective for the proposed method among the 11 feature vector patterns, but it is unclear which features are specifically effective for authentication. Therefore, principal component analysis is used to evaluate the importance of each feature and optimize the feature vectors by compressing the number of dimensions of the feature vectors obtained in evaluation 1. In this case, the mean F-measure, the mean precision rate, the mean recall rate and the mean FAR are used to evaluate the feature vector after compression.

4.3 Evaluation results and discussion

4.3.1 Evaluation 1

The results for each feature vector pattern and the mean F-measure, mean precision rate, and mean recall rate for each multi-class classification algorithm are shown in Table 4 and the mean FAR results are shown in Table 5. These mean F-measure and mean FAR were evaluated using Eq.1, and it was found that the mean F-measure and the mean FAR were the maximum for the combination of feature vector pattern 4 and Random Forest, which included features extracted from the 3-axis angular velocity data. The mean F-measure was 0.915, the mean precision rate was 0.946, the mean recall rate was 0.895, and the mean FAR was 0.113. The next largest Eq. 1 was the combination of feature vector pattern 2 and Logistic Regression, which included features extracted from the 3-axis acceleration data and 3-axis angular velocity data. The mean F-measure was 0.966, the mean precision rate was 0.977, and the mean recall rate was 0.957, and the mean FAR was 0.196. In both cases, an mean F-measure of more than 0.9 and an mean FAR of less than 0.2 were obtained and the classifier was trained it was found that the classification of the data with high accuracy is possible. Therefore, we can say that it is possible to authenticate individuals using the results of this classification with high accuracy. However, in order for an unknown person to authenticate with the proposed method, the user needs to come close to the Smart lock at less than one meter away from the Smart lock with a smartphone that is paired with the Smart lock installed in the registrant's house. If a malicious person is trying to authenticate the target's home, it is necessary to steal the target's smartphone, know the address of the house, and move to the front door. This takes a lot of work and the possibility of an actual attack is much lower than that of an authentication to unlock the screen of a smartphone. We then need to break through the authentication with the mean FAR probability obtained from the combination of these feature vector patterns and the multiclass classification algorithm. Therefore, the possibility of accidentally authenticating an unlearned stranger is low and the proposed method can be used for authentication because it can classify the trained data with high accuracy. However, it is necessary to confirm whether the same level of accuracy can be obtained when the number of subjects is increased in the future, because these results are based on only 7 subjects.

From the above, the pattern selected as the most suitable among the 11 feature vector patterns were pattern 2, using basic statistics extracted from 3-axis acceleration and 3-axis angular velocity data, and pattern 4 using basic statistics extracted from 3-axis angular velocity data.

Table 5: FAR results for each feature vector pattern and multi-class classification algorithm

Pattern Number	SVM	Logistic Regression	Decision Trees	Random Forest	K Neighbors Classifier
1	0.325	0.278	0.298	0.350	0.479
2	0.284	0.196	0.244	0.263	0.248
3	0.227	0.198	0.295	0.221	0.236
4	0.302	0.209	0.191	0.113	0.302
5	0.487	0.471	0.490	0.386	0.331
6	0.423	0.398	0.163	0.208	0.445
7	0.328	0.298	0.438	0.131	0.096
8	0.374	0.375	0.274	0.160	0.434
9	0.306	0.209	0.303	0.267	0.468
10	0.389	0.406	0.294	0.217	0.448
11	0.337	0.255	0.256	0.360	0.505

4.3.2 Evaluation 2

For the optimization of the feature vector patterns 2 and 4 obtained in Evaluation 1, the results of mean F-measure, mean precision rate, mean recall rate and mean FAR for each dimensional compression of the vectors by principal component analysis are shown in Table 6. For the calculation of each value, the optimum multi-class classification algorithm for each of the feature vector patterns found by Evaluation 1 was used. The original number of dimensions of this vector is 30, but even if it is compressed to 10 dimensions, each value is almost the same as the value in the original number of dimensions. In addition, even if the number of dimensions after compression is about 6, the accuracy is as good as that of the original number of dimensions, and it is possible that the main features that are useful for authentication are included in the features. Next, we focus on the result of the feature vector pattern 4. The original number of dimensions of this vector is 15 dimensions, but even when compressed to 10 dimensions, we can confirm the same level of accuracy as in the case of the original number of dimensions. It shows that the main features that are valid for authentication are contained in this compressed 10 dimensions.

Table 7 shows the elements of the feature vectors when the number of dimensions of the feature vector patterns 2 and 4 are compressed to less than 10 dimensions, respectively. When we focus on the elements of the compressed feature vector pattern 2, we can see that the features extracted mainly from the acceleration remain. This feature vector pattern 2 was originally a feature vector with the basic statistics extracted from 3-axis acceleration and 3-axis angular velocity. Dimensional compression of feature vectors by principal component analysis shows that acceleration is an effective feature for authentication when features extracted from 3-axis acceleration and 3-axis angular velocity are used in combination.The features extracted from the x-axis and y-axis of the acceleration were found to be effective. In contrast, the feature vector pattern 4 contained the basic statistics extracted from the 3-axis angular velocity as features and it was found that the features were still selected from each axis after compression.

Table 6: The result of compressing feature vectors in each dimension

Pattern 2

Dimensions	F-measure	Precision rate	Recall rate	FAR
2	0.685	0.675	0.709	0.024
3	0.880	0.912	0.865	0.342
4	0.900	0.921	0.886	0.279
5	0.933	0.946	0.923	0.471
6	0.947	0.965	0.934	0.400
7	0.945	0.962	0.932	0.220
8	0.957	0.971	0.946	0.208
9	0.957	0.971	0.946	0.204
10	0.962	0.973	0.952	0.198

Pattern 4

Dimensions	F-measure	Precision rate	Recall rate	FAR
2	0.790	0.833	0.771	0.187
3	0.803	0.854	0.785	0.180
4	0.841	0.876	0.822	0.190
5	0.839	0.885	0.818	0.167
6	0.827	0.891	0.801	0.154
7	0.862	0.922	0.832	0.133
8	0.871	0.939	0.841	0.117
9	0.874	0.934	0.845	0.120
10	0.895	0.947	0.865	0.080

Table 7: Elements of feature vectors when the number of dimensions is compressed

Pattern 2	Pattern 4
Accel x-axis mean	Gyro x-axis max
Accel x-axis variance	Gyro x-axis variance
Accel x-axis standard deviation	Gyro x-axis standard deviation
Accel y-axis max	Gyro y-axis mean
Accel y-axis variance	Gyro y-axis variance
Accel y-axis standard deviation	Gyro y-axis standard deviation
	Gyro z-axis max
	Gyro z-axis min
	Gyro z-axis mean
	Gyro z-axis standard deviation

The results show that 3-axis acceleration is a more effective feature for authentication when 3-axis acceleration and 3-axis angular velocity are used together. When only 3-axis angular velocity was used, the accuracy of this method was slightly lower than that of the method using only 3-axis acceleration, but it was found that high accuracy was achieved by using it in combination with 3-axis acceleration. In this evaluation, the relationship between 3-axis acceleration and 3-axis angular velocity was not clear, and it is necessary to investigate it in the future.

5 CONCLUSION

In this paper, we proposed a door-knock authentication system using a 3-axis accelerometer and a 3-axis angular velocity sensor as a biometric authentication method using behavioral features that reduces the psychological burden of the user's actions at the time of authentication, without making the user's actions into a pattern. The proposed method is a two-factor authentication method that combines biometric authentication using behavioral characteristics with property authentication using a smartphone paired with a Smart lock.

The results of the experiment with the subjects show that Random Forest is used as a multiclassification algorithm in the prepared combination, and the feature vector pattern 4 using the basic statistics extracted from the 3-axis angular velocity as the feature was found to be the best combination. The mean F-value was 0.915, the mean fit rate was 0.946, the mean reproduction rate was 0.895, and the mean FAR was 0.113. The number of dimensions of the feature vectors in this case was 15, but it was confirmed that the accuracy of the feature vectors was comparable to the original number of dimensions even when compressed to 10.

In the future, we need to evaluate the proposed method through experiments with more subjects and effective feature combinations. In addition, we will use wearable devices such as smartwatches, which have become popular in recent years, to obtain authentication motions, and we consider the selection of appropriate features for acquisition by smartwatches. Also, in the experiments in this paper, the user may remember and reproduce the motions since the knocking motions are obtained continuously. Considering the actual use of the system, there may be a long period of time between the registration of the authentication motion and the authentication, so it is necessary to conduct evaluation experiments, including usability.

REFERENCES

[1] Qrio: Qrio Lock Qrio(online), available from ⟨https://qrio.me/smartlock/⟩ (accessed 2019-03-09).

[2] CANDYHOUSE: Sesami Smart Lock, CANDYHOUSE(online), available from ⟨https://jp.candyhouse.co/⟩ (accessed 2019-03-09).

[3] Ishihara, S., Ohta, M., Namikata, E. and Mizuno, T.: Individual Authentication for Portable Devices Using Motion of the Devices, *IPSJ Journal*, Vol. 46, No. 12, pp. 2997–3007 (2005). *(In Japanese)*

[4] Namikata, E., Ohta, M., Ishihara, S. and Mizuno, T.: An Individual Authentication Method With Arm Movements Using a Wrist Watch Loaded With an Accelerator Sensor, *IPSJ SIG Technical Report*, Vol. 2003, No. 94(2003-HI-105), pp. 21–26 (2003). *(In Japanese)*

[5] Ichimura, R., Notomi, K. and Saito, K.:A Rhythm Identification Method for Smart Phones with Peek-a-boo Attack Resistance -Evaluation of authentication accuracy using the main melody of the music-, *DICOMO2013*, Vol. 2013, pp. 230–233 (2013). *(In Japanese)*

[6] Kita, Y., Kamizato, K, Park, M. and Okazaki, N.: A study of rhythm authentication using multi-touch operation, *IPSJ SIG Technical Report*, Vol. 2014-UBI-41, No. 19, pp. 1–7 (2014). *(In Japanese)*

[7] Konno, S., Nakamura, Y., Shiraishi, Y. and Takahashi, O.: Improvement of accuracy based on multi-sample and multi-sensor in the gait-based authentication using trouser front-pocket sensors, *International Journal of Informatics Society (IJIS)*, Vol.8, No.1, pp.3-13, (2016).

[8] Ito, S., Shiraishi, Y. and Konno, S.: A Method for Personal Authentication by Using Wrist-mounted Sensors Based on Characteristics of Keystroke Action, *DICOMO2016*, Vol. 2016, pp. 1165–1171 (2016). *(In Japanese)*

[9] Mitsukude, Y., Hayashi, K., Ishida, S., Tagashira, S. and Fukuda, A.: Proposal and Initial Evaluation of Human Identification Based on Door Opening/Closing Operations, *IPSJ SIG Technical Report*, Vol. 2019-UBI-61, No. 32, pp. 1–6 (2019). *(In Japanese)*

[10] Kurahashi, M., Murao, K., Terada, T. and Tsukamoto, M.: A System for Identifying Toilet User by Characteristics of Paper Roll Rotation, *Proc. of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (Mobiquitous 2016)*, pp. 282-283 (2016).

[11] Park, Y. T., Sthapit, P. and Pyun, J.: Smart digital door lock for the home automation, *Proc. 2009 IEEE Region 10 Conference(TENCON2009)*, pp. 1–6 (2009).

[12] Dhondge, K., Ayinala, K., Choi, B. and Song, S.: Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones, *Proc. 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, pp. 251–257 (2016).

[13] Hadis, M. S., Palantei, E., Ilham, A. A. and Hendra, A.: Design of smart lock system for doors with special features using bluetooth technology, *Proc. 2018 International Conference on Information and Communications Technology (ICOIACT2018)*, pp. 396–400 (2018).

[14] Aman, F. and Anitha, C.: Motion sensing and image capturing based smart door system on android platform, *Proc. 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 2346–2350 (2017).

[15] Sato, K., Noma, Y., Kashima, M. and Watanabe, M: A Study on the Development of an Intelligent Door Knob System with Palmprint Authentication, *MIRU2011*, Vol. 2011, pp. 580–585 (2011). *(In Japanese)*

[16] Nakabachi, K., Nakamura, Y. and Inamura, H.: Door

knock type person authentication method for smart lock system, *DICOMO2019*, Vol. 2019, pp. 1433–1440 (2019). *(In Japanese)*

[17] Murao, K., VanLaerhoven, K., Terada, T. and Nishio S.: A Method for Context Awareness using Peak Values of Sensors, *IPSJ SIG Technical Report*, Vol. 2009-UBI-22, No. 11, pp. 1–8 (2009). *(In Japanese)*

[18] Nakabachi, K., Nakamura, Y. and Inamura, H.: Improvement of door knock type authentication method for smart door lock system, *IPSJ SIG Technical Report*, Vol. 2020-CSEC-88, No.45, pp.1-7 (2020). *(In Japanese)*