User Identification Method based on Head Shape using a Helmet with Pressure Sensors

Atsuhiro Fujii
Ritsumeikan University
Shiga, Japan
atsuhiro.fujii@iis.ise.ritsumei.ac.jp

Kazuya Murao
Ritsumeikan University
Shiga, Japan
murao@cs.ritsumei.ac.jp

ABSTRACT

Helmets are used for various purposes such as industrial protective hat (work helmet), motorcycle Helmet, sports helmet, and military/police helmet. If the wearer is known through wearing a shared helmet, name, affiliation, qualification can be shown on a display mounted on the helmet, and sensor data collected through helmet such as acceleration data, video, eye track data can be labeled with wearer's ID. In this paper, we propose a user identification method based on User's head shape using a helmet equipped with 32 pressure sensors. Our method has two functions: identification and authentication. Identification is to classify users into one of the registered users. Authentication is to accept users who have been registered to the system and reject unknown users. We have implemented a prototype helmet device and collected data from nine subjects, resulting in 100% accuracy for user identification and 0.076 average EER for user authentication.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

User identification, pressure sensor, helmet, head shape

ACM Reference Format:
Atsuhiro Fujii and Kazuya Murao. 2020. User Identification Method based on Head Shape using a Helmet with Pressure Sensors. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Helmets are used for various purposes such as industrial protective hat (work helmet), motorcycle Helmet (bike, car, bicycle, etc.), sports helmet (American football, baseball, ice hokey, etc.), and military/police helmet. These are all worn to protect the head in the event of an accident[3]. It is considered important from a safety point of view that there is no gap between the head and the helmet.

Workers in factories and disaster sites have to wear helmets. There are also various people who do not know each other, such as short-term workers and vendors. If these people have own helmet, the wearer's name and work division are shown on the helmet, allowing the helmet wearer to be identified from a distance or overhead even if the wearer's face cannot clearly be seen. Identifying individuals is a deterrent to trespassers. In addition, showing the qualifications such as a hazardous materials engineer's license and heavy machinery licence helps create a safe work environment. In many cases, such information is directly written on the helmet or an identifiable sticker is attached to the helmet. However, in such an analog operation, it is easy for a trespasser to disguise himself by writing or stealing a sticker. Moreover, even if the worker puts on other people's helmet, they are not aware of it and wrong information is displayed. If the helmets are shared among the workers, the helmet is not marked with the identifiable information.

In this paper, we propose a method that identifies users based on the shape of their heads by installing pressure sensors inside a helmet. We implemented a prototype helmet with 32 pressure sensors. Our method calculates the similarity between the wear's data and registered users' data and outputs the user of the most similar data as an identification result.

The prototype helmet has a display to show user's name and credentials upon the identification result, therefore, wrong information is not displayed on the helmet if a helmet of someone else is used. It is useful that the identification information is automatically displayed on a shared helmet and workers can recognize each other. In addition, another advantage of user identification is data annotation. Data collected through sensors attached to the helmet or wears' body such as a camera, an eye tracker, and an accelerometer can automatically be annotated with the wear's ID. By attaching a GPS module or an antenna to localize the user[12], the name and location of the worker can be determined in real time and it will be easier for the foreman to understand the overall situation in the field. Furthermore, from the pressure data between the helmet and the head, it is possible to check whether the shape of the head matches the helmet as zero pressure value means that there is a gap between the helmet and the head. Another possible use of the proposed helmet is a key for the door where access to the room is restricted according to the position or qualifications.

The proposed method has two functions: user identification and user authentication. User identification is based on the assumption that a single helmet is shared by several people. The pressure sensor data of a person who may wear a helmet is registered in advance, and the person who wears the helmet is identified as one of the registered persons. Personal identification does not assume that a non-registered person will wear the device. If a non-registered person wears the device, the identification result will be the one with the closest data among the registered users. The user authentication

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/1122445.1122456

determines whether the person wearing the helmet is actually the person with the ID or not when the ID of a user wearing a helmet is given to the system. We assume an environment in which each individual has own helmet (the same as for smartphone authentication) and an environment in which the user ID is entered when using a shared helmet (the same as for ATM authentication). Even if an outsider wears a helmet and enters the stolen ID, they can be identified as an outsider (authentication denied) because their head shape is different from the person of the ID.

In the following sections, Section 2 introduces the related works, Section 3 explains the proposed method, Section 4 evaluates the proposed method, and Section 5 concludes this paper.

2 RELATED WORK

In this section, we introduce research on user identification and head state recognition.

2.1 User Authentication Method

There are several methods to identify individuals: password, PIN, and stroke pattern; physical characteristics such as face, fingerprint, voice print, and iris; and behavioral characteristics such as handwriting and gait. Password, PIN, and stroke pattern that can be freely set by individuals has a risk of spoofing by shoulder hacking, brute force attack, and password duplication.

For physical characteristics, Chen et al.[5] proposed an authentication method using the user's face and fingertips video images captured from the front and rear cameras of a mobile device. It is possible to identify the wearer by using a camera mounted on the helmet, however, it is messy to take a picture of the face all the time wearing the helmet. Siddharth et al.[1] proposed an authentication system based on palm print and palm vein. The system uses visible and infrared light to acquire images of the palm print and palm vein, and the authentication is performed by checking the data against the registration data in the database. Sayo et al.[15] proposed an authentication method based on the camera image capturing the shape of the lips which is a physical characteristics and the movement of the lips during speech which is behavioral characteristics. As another method using the mouth, Kim et al.[10] proposed an authentication method that combines dental images and voice. Bednarik et al.[4] proposed an identification system that uses eye movements such as pupil size and variation, gaze velocity, and distance of the infrared reflection of the eye.

For such camera-based approaches, mounting a camera on the outside of the helmet, individuals can be identified by turning toward the camera before putting on the helmet. However, there is a complication of taking a picture of one's own face with a camera. For the method using palm print and palm vein, this method also requires the user to hold the camera each time the wearing the helmet. A camera can be attached to the mouth of the helmet so that the shape and movement of the lips and teeth can be acquired. However, the space around the mouth inside the full-face helmet is limited, and it is difficult to distinguish the shape and movement of around the mouth with a single camera. In addition, it is not practical as helmets have to be considered being used in the dark places.

Nogueira et al.[13] used convolutional neural networks (CNN) for fingerprint authentication, and achieved a high classification accuracy. However, fingerprint authentication has a risk that fingerprints can be easily duplicated from photographs. The head shape we use in this paper is a physical characteristic, and is difficult to be replicated because of its three-dimensional shape.

For behavioral characteristics, it may be possible to authenticate the users by focusing on the action of wearing a helmet. The authors have proposed a method that authenticates a smartphone user from acceleration sensor data when taking it out of the pocket[8]. Guerra-Casanova et al.[7] proposed a method to authenticate users by gestures of their hands using a mobile device with an embedded accelerometer. For motion-based authentication using accelerometers, there is a possibility that the acceleration characteristics of the motion until the helmet is worn can be used for authentication by mounting an accelerometer on the helmet. However, there are various wearing actions, such as wearing the helmet in a hurry and taking care not to let the interior of the helmet get wet in the rain. Therefore, it is not practical to collect data from all the people in various situations.

2.2 Head State Recognition

Toth et al.[18] focused on the facial muscle signal, and six different facial expressions were classified using the muscle signals and the gyroscope values which were got from a cheap off-the-shelf electroencephalogram (EEG) headset. EEG headsets are actually used to measure brain waves, however, the muscle signals are detected locally since the measurement is performed by placing electrodes on the scalp. It uses only existing EEG devices for classification of facial expressions and no additional electromyography (EMG) sensor is used. Kwon et al.[11] designed a glass-type wearable device to detect the user's emotions based on facial expressions and physiological reactions. The device can capture facial expressions with a built-in camera and obtain physiological responses such as photoplethysmogram (PPG) and electrodermal activity (EDA). Fukumoto et al.[9] designed a smile-based life-logging system that focuses on smile/laughter for indexing the interesting/enjoyable events on a recorded video. They use photo-interrupters and smile/laughter is detected separately by threshold-based clustering. Evaluation results showed 73%–94% accuracy in detecting smile/laughter while actual use of the system. These researches obtain dynamic information such as facial expressions and physical responses in the face area. On the other hand, our study differs from them in that it obtains static features of the head shape.

Kouno et al.[6] proposed an image-based person identification system using an depth image from an overhead camera. By using depth information, this system captures the precise person's area and four features extracted from images based on depth information to the identification method; body height, body dimensions, body size and depth histogram. The identification accuracy is 94.4% and 91.4% while standing in front of a door and touching a doorknob, respectively.

In this paper, we propose a method to identify individuals by acquiring their head shape while wearing a helmet with pressure sensors. Our method does not force the users to do special behavior or to remain stationary for identification. Taking a wearable

approach, our method can be used in any place and any time. To breach the system, the exact three-dimensional shape of the head is needed, but it is difficult to replicate the head shape.

3 PROPOSED METHOD

This section describes the details of the proposed method.

3.1 Overview

The proposed method assumes that the user wears a helmet equipped with pressure sensors, acquires the shape of wearer's head, and identifies whether the wearer is registered person or not. The proposed method has two functions: user identification and user authentication.

- **User identification** assumes that a single helmet is shared by multiple people and any other information such as ID is not given to the system; users just wear the helmet. Their pressure sensor data are registered in advance and the person who put on the helmet is identified as one of the registered persons as shown in **Figure 1**. User identification does not assume that a non-registered person will wear the helmet. If a non-registered person wears the device, the identification result will be the one with the closest data among the registered users.
- **User authentication** determines whether the person wearing the helmet is actually the person or not when his/her ID or username is given. We assume two cases where the authentication is used: each individual has own helmet and only the person's pressure sensor data has been registered (single user; username preset in the device; the same as for smartphone authentication); and a helmet is shared with multiple people and username is entered when using the helmet (multiple users; username input accordingly; the same as for ATM authentication). Their pressure sensor data are registered in advance and the person who put on the helmet is judged to be accepted or rejected by calculating the similarity between the input data and the data of the ID as shown in **Figure 2**. Even if an ID is leaked, an outsider can be rejected because his/her head shape is different from the data of the ID.

32 pressure sensors are attached to the inner side of the helmet to acquire data, producing 1-dimensional 32-channel pressure data. Pressure data of the people who are expected to wear helmets have been registered to the system in advance and the data is called training data in this paper. In user identification, the system uses the Support Vector Machine (SVM) to build a recognition model from the feature values extracted from the training data and outputs the identification results from the features of the input data of an unknown registrant in the identification phase. On the other hand, in user authentication, the system calculates Mahalanobis' distance between the training data and the input data of the person including non-registrant is calculated and authenticates the user if the distance is less than the threshold, otherwise the user is rejected.

3.2 Hardware

We implemented a helmet equipped with 32 pressure sensors. **Figure 3** shows the configuration of the device and **Figure 4** shows

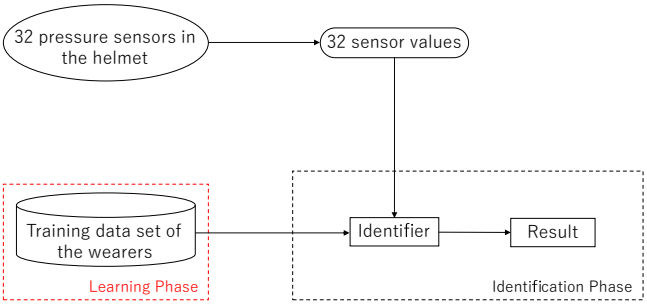

Figure 1: Structure of the user identification.

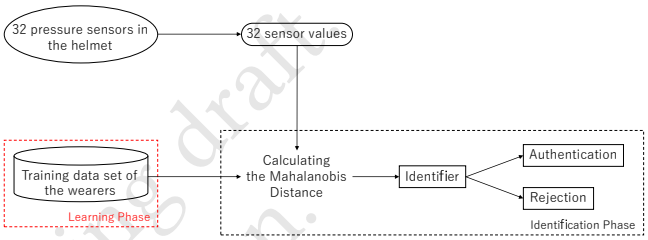

Figure 2: Structure of the user authentication.

the appearance of the device. The head of the helmet wearer must be in close contact with the sensors to obtain the correct pressure values, therefore, we used a commercially available full-face helmet with high adhesion. The pressure sensors were FSR402 and FSR402 ShortTail manufactured by Interlink Electronics, Inc. The Arduino MEGA2560 R3 was used as a microcomputer. Since the helmets used were free size and it was difficult to attach and remove the interior, we removed the interior of the top of the head and installed a thick urethane sponge as shown in **Figure 5**. The urethane sponge is cut and a pressure sensor was inserted into the cut line as shown in **Figure 6**.

Four pressure sensors were set at the top of the head, 16 sensors were set around the top of the head, six sensors were set at the back of the head, and six sensors were set at the cheek pads on both sides. A total of 32 sensors were installed at the points as shown in **Figure 7**. The wiring for the pressure sensors went through a hole drilled in the top of the helmet, then it is connected to 5V power supply port, GND, and analog input port which is on the Arduino MEGA2560 R3 via a printed circuit board (PCB) with a 10 KΩ resistor which is mounted outside the helmet. The PCB attached to the outside of the helmet is shown in **Figure 8**. The PCB is bolted to the left cheek area using a threaded hole drilled for securing the helmet shield. It is fixed and removable.

3.3 User Identification Method

3.3.1 Preprocessing. The data acquisition starts when the user puts on the helmet. The voltage values of all the pressure sensors are almost 5V when the helmet is not worn and the voltage decreases when the helmet is worn. 32 pressure sensors data $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$ are acquired at time t and the system segment the data over 2-second window starting from the $t = T_s$.

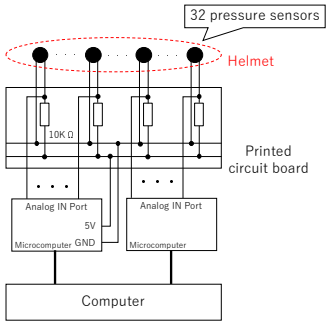

Figure 3: Structure of the device

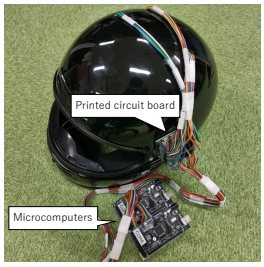

Figure 4: Appearance of the device

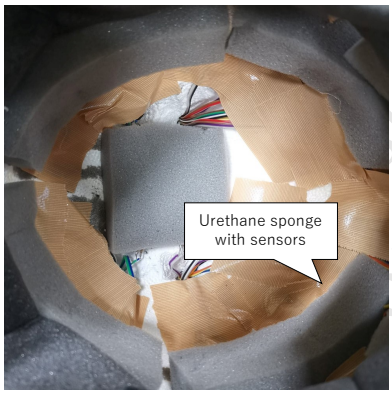

Figure 5: Inside of the device

Figure 6: Mounting Method for Pressure Sensors

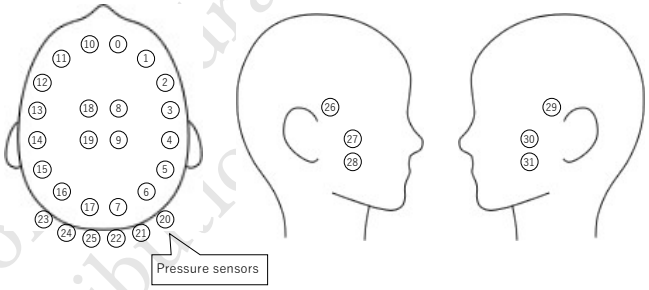

Figure 7: The position of the pressure sensors

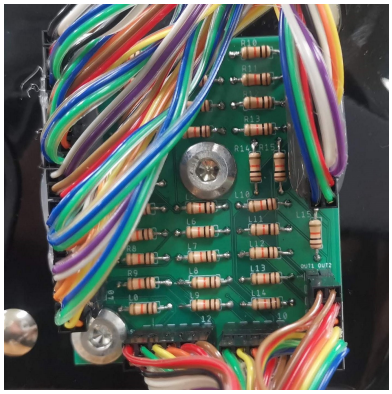

Figure 8: A printed circuit board connected to 32 pressure sensors

Time $t = T_s$ is the time when the change of the sum of 32 dimensions per sample $\sum_{i=1}^{32}(p_i(t) - p_i(t-1))$ is first less than 1V for 11 consecutive samples (11/30 second), i.e. $\sum_{i=1}^{32}(p_i(t) - p_i(t-1)) < 1[V]$ $(i = T_s, \cdots, T_s - 10)$ The average value over the window $x_i(t) = \frac{1}{N}\sum_{t=T_S}^{T_S+N-1} p_i(t)$ for sensor channel i $(i = 1, \cdots, 32)$ is calculated, where N is the number of samples in the window. We then obtain a 32-dimensional vector $\boldsymbol{x}(t) = [x_1(t), \ldots, p_{32}(t)]$ as a feature.

3.3.2 Identification. Given training data $[\boldsymbol{x}_m, y_m]$ $(m = 1, \ldots, M)$ from the users who are expected to use the helmet by wearing the helmet M times in total in advance, the SVM is trained with the training data, where y_m is the registrant label, such as the registrant's name and number. The input data $\boldsymbol{x}_{test}$ collected by the user to be identified is fed into the SVM and the classification result $\hat{y}_{test}$ is obtained.

3.4 User Authentication Method

3.4.1 Preprocessing. In user authentication, 32-dimension pressure sensors data $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$ and its average $\boldsymbol{x}(t) = [x_1(t), \ldots, p_{32}(t)]$ as a feature are obtained in the same manner as in user identification.

3.4.2 Similarity calculation. In user authentication, there are two cases of training data usage: data of a single user is used and data of multiple users is used. For single user data, data of only a single user, e.g., owner of the helmet, is registered or data of multiple users are registered but data of one of them whose ID is given is used. For multiple user data, data of multiple users who are expected to use the helmet is used. Given training data $[\boldsymbol{x}_m, y_m]$ $(m = 1, \ldots, M)$ from the user(s) by wearing the helmet M times in advance, the proposed method calculates the Mahalanobis distance, where y_m is the registrant label, such as the registrant's name and number.

The Mahalanobis distance is one of the methods for calculating the distance between multiple variables, which can be normalized considering the distribution of the data. The mean vector $\boldsymbol{\mu}$ and the variance-covariance matrix Σ of the training data are calculated by Eqn. 1 and 2.

$$\boldsymbol{\mu} = \frac{1}{M}\sum_{m=1}^{M}\boldsymbol{x}_m \quad (1)$$

$$\Sigma_{i,j} = \frac{1}{M}\sum_{m=1}^{M}(\boldsymbol{x}_i - \boldsymbol{\mu})(\boldsymbol{x}_j - \boldsymbol{\mu})^T \quad (2)$$

The Mahalanobis distance between training data $\boldsymbol{x}_m$ $(m = 1, \ldots, M)$ and input data $\boldsymbol{x}_{test}$ can be calculated with Equation 3.

$$d(\boldsymbol{x}, \boldsymbol{x}_m) = \sqrt{(\boldsymbol{x} - \boldsymbol{x}_m)^T \Sigma^{-1} (\boldsymbol{x} - \boldsymbol{x}_m)} \quad (3)$$

If the input data are collected from the pre-registered user, the input data $\boldsymbol{x}_{input}$ follows the probability distribution of the variance-covariance matrix Σ.

3.4.3 Authentication decision. Let θ be the threshold value, the user is authenticated if Eqn. 4 is satisfied, while the the user is reejcted if Eqn. 4 is not satisfied.

$$\theta \geq \min_m(d(\boldsymbol{x}_{input}, \boldsymbol{x}_m)) \ (m = 1, \cdots, M) \quad (4)$$

3.5 Software

The program of Arduino MEGA was implemented by Arduino IDE. A computer program that receives data from Arduino MEGA and saves it in csv format was implemented by Python. A computer program to analyze the data was implemented by Python.

In the user identification, the system loads the pre-collected sensor data in csv format. For SVM, `sklearn.svm.SVC` of a scikit-learn[16] library which is an implementation of the standard soft margin SVM is used. We also used `sklearn.model_selection.cross_val_score` for cross-validation and `sklearn.model_selection.GridSearchCV` for grid search were used for evaluation.

In the user authentication, the system loads pre-collected sensor data in csv format and computes the variance-covariance matrix using `scipy.spatial.distance`. For the calculation of the Mahalanobis distance, `sklearn.covariance.MinCovDet` is used for variance-covariance matrix. Minimum Covariance Determinant (MCD) is an algorithm that is robust to outlier values for estimating a variance-covariance matrix. `sklearn.covariance.MinCovDet` is a scikit-learn library that is implemented Fast-MCD[14] which is a faster version of MCD. `scipy.spatial.distance` is a SciPy[17] library that is implemented functions for calculating various distance.

4 EVALUATION

This section describes the experiments we conducted to evaluate the effectiveness of the proposed method.

4.1 Data Collection

We asked nine subjects (A~I, all males, mean age 23 years) to wear the helmet implemented in Section 3 and collected sensor data. The sampling rate is approximately 30 Hz. The subjects put it on for two seconds to collect data, then put it off, and put it on again for two seconds to collect data, tough which a set of two samples is obtained. By collecting data of ten sets (20 samples) from each subject, a total of 180 samples (2 seconds×20 samples×9 subjects) were collected. Up to four sets of data were collected per person per day. In order to collect data on the various positions of the sensors and head as the helmet was worn, a rest period of at least 30 minutes was provided between sets.

4.2 User Identification Method

4.2.1 Evaluation environment. We evaluated the proposed method in five-fold cross-validation manner that 80% (16 samples) of data collected from each subject were trained and 20% (four samples) were tested. In order to investigate the effect of the number of sensors used, identification accuracies for all combinations of sensors from one sensor to 32 sensors were measured.

To simulate a half helmet which is commonly used at a construction site, all combinations of sensors from 1 to 20 sensors aligned in the top half out of 32 sensors; four sensors at the top of the head and 16 sensors around the top half of the head. These 20 sensors are the sensors #0–#19 in **Figure 7**. In this evaluation, two types of sensor configurations are tested: a full-face helmet with 32 sensors and a half helmet when 20 sensors.

4.2.2 Results and discussion. The accuracy of user identification with a full-face helmets and a half helmet is shown in **Table 1** and **Table 2**. The numbers shown in "Sensors used" are the sensor number in **Figure 7**. For a full-face helmet, when the number of sensors is 32, the number of sensor combination is one ($_{32}C_{32} = 1$), and when the number of sensors is 31, the highest accuracy of $_{32}C_{31} = 32$ combinations is shown in the table. For a half helmet, when the number of sensors is 20, the number of sensor combination is one and when the number of sensor is 19, the highest accuracy of 19 combination is shown in the table. For one through four sensors, the regularization parameter of SVM is set to $C = 1.0$, and the sensor combination with the highest accuracy was recorded. Then, the best C was searched by grid search for the sensor combination, and the highest accuracy is shown in the tables.

We found that all the accuracies when 32 and 31 sensors for full-face helmet are used and 20 and 19 sensors for half helmet are used were all 1.000. Therefore, we measured the accuracy from one sensor until the accuracy reaches to 1.000 and skipped the measurement of accuracies for more sensors.

For full-face helmet, nine subjects were identified with 100% accuracy when the number of sensors was five. The accuracy was 99.4% with four sensors, 97.2% with three sensors, and 92.2% with two sensors. However, the accuracy dropped significantly to 61.7% when the number of sensors was one.

Table 1: Identification accuracy with a full-face helmet; sensors are reduced from 32 to 1.

Sensors used	Accuracy
All	1.000
Exclude 1	1.000
⋮	⋮
0, 3, 5, 16, 17	1.000
0, 3, 5, 16	0.994
3, 11, 24	0.972
3, 25	0.922
10	0.617

Table 2: Identification accuracy with a half helmet; sensors are reduced from 20 to 1.

Sensors used	Accuracy
All	1.000
Exclude 1	1.000
⋮	⋮
0, 3, 5, 16, 17	1.000
0, 3, 5, 16	0.994
0, 3, 13	0.983
3, 16	0.928
10	0.617

For half helmet, nine subjects were identified with 100% accuracy when the number of sensors was fine. The accuracy was 99.4% with four sensors, 98.3% with three sensors, and 92.8% with two sensors. However, the accuracy dropped significantly to 61.7% when the number of sensors was one.

Both of the full-face helmet and the half-helmet achieved 100% accuracy with at least five sensors for the data set used in this experiment. However, the number of sensors required to achieve high accuracy may increases as the number of registrants increases. Focusing on the sensors used for full-face helmet, most of the sensors are less than #20, which means that sensors in the top half were significant. Sensors not used in half helmet were aligned around neck and ear and the position of the sensors related to the user's head are supposed to be inconsistent.

4.3 User Authentication Method

4.3.1 Evaluation environment. One subject was considered to be the individual to be authenticated, i.e. owner, and the remaining eight subjects were considered to be strangers. The authentication accuracy of the owner was measured in 5-fold cross-validation manner; 80%(16 samples) of the owner's data were registered as training data, and the remaining 20%(4 samples) data were used as test data. In addition, the authentication accuracy for the strangers were measured using data from all eight strangers (160 samples). All 160 samples were tested in each fold of the cross-validation. All nine subjects were evaluated on a rotation basis.

In user authentication, FRR, FAR, and EER are used as indicators of authentication accuracy. FRR is false reject rate at which a registered person is mistakenly considered to be a stranger and rejected. FAR is false accept rate at which a stranger is mistakenly considered to be a registered person and authenticated. The smaller the threshold value θ in Eqn. 4 is set, the stricter the authentication decision becomes, resulting in increasing FRR. On the other hand, the larger the threshold value θ is set, the looser the authentication decision becomes, resulting in increasing FAR. There is a trade-off between FRR and FAR, and the value at which FRR and FAR become equal is called EER (equal error rate). Normally, the value of EER is used as an indicator to evaluate the performance of authentication methods, and the smaller EER, the better the performance.

Table 3: EER for the subjects in user authentication.

Subject	EER
A	0.002
B	0.095
C	0.050
D	0.055
E	0.006
F	0.094
G	0.012
H	0.050
I	0.000
Average	0.076

4.3.2 Results and discussion. EER of each subject is shown in **Table 3**. "Average" means the average EER of all subjects. FRR and FAR for each subject with varying thresholds from 0 to 60 by 1 are shown in **Figure 9**. EER of subjects A, E, G, and I was roughly less than 0.01, which means that the owner fails in authentication less than once a 100 times, and that the strangers break the authentication less than once a 100 times. EER of 0.0097 for user authentication using ear acoustics was reported in Ref. [2], therefore, our method achieved comparable performance for four of nine subjects.

The next most accurate subjects are C, D, and H, with EER of approximately 0.05. In order to determine the cause of the decline in accuracy compared with subject A, E, G, I, all collected data were compressed to the first principal component and the second principal component by principal component analysis (PCA). The results of this data plotted on a two-dimensional plane are shown in **Figure 10**. Looking at the plots of subject C, one sample of data of subject C is close to data of subject I and the variance in the first principal component is large, which would deteriorate the accuracy. On the other hand, the data for subjects D and H overlapped each other significantly, which affected the accuracy of the both subjects.

The least accurate subjects are B and F, with EER of approximately 0.095. Data of subject B has a small variance and there is some overlap with data of subject I. However, EER of subject I was 0, which is perfect authentication. Therefore, the overlap of these data groups is likely due to the loss of data when they are compressed into two dimensions by principal component analysis.

On the other hand, subject F's data does not show any overlap with the other subjects' data, but there is a large variance to both directions for the first and second principal components. Considering the effect of data compression by PCA, duplication with other subjects' data groups can be inferred in the 32-dimensional data. The accuracy of subjects B and C, who has data groups located close to subject F's data groups, may have been affected by the scattered data of subject F. In particular, the accuracy of subject B is likely to be lower than that of subject C because the two samples of subject B are located in close proximity to subject F's data group.

Data of subject E are located at the rightmost points. In addition, the variance is small so the data are considered to be very distinctive. For subject E in **Figure 9**, FRR and FAR crossed at a threshold of approximately 60, which is greater than the other subjects. This is because the data are quite different from the others and the FAR did not increase by increasing the threshold.

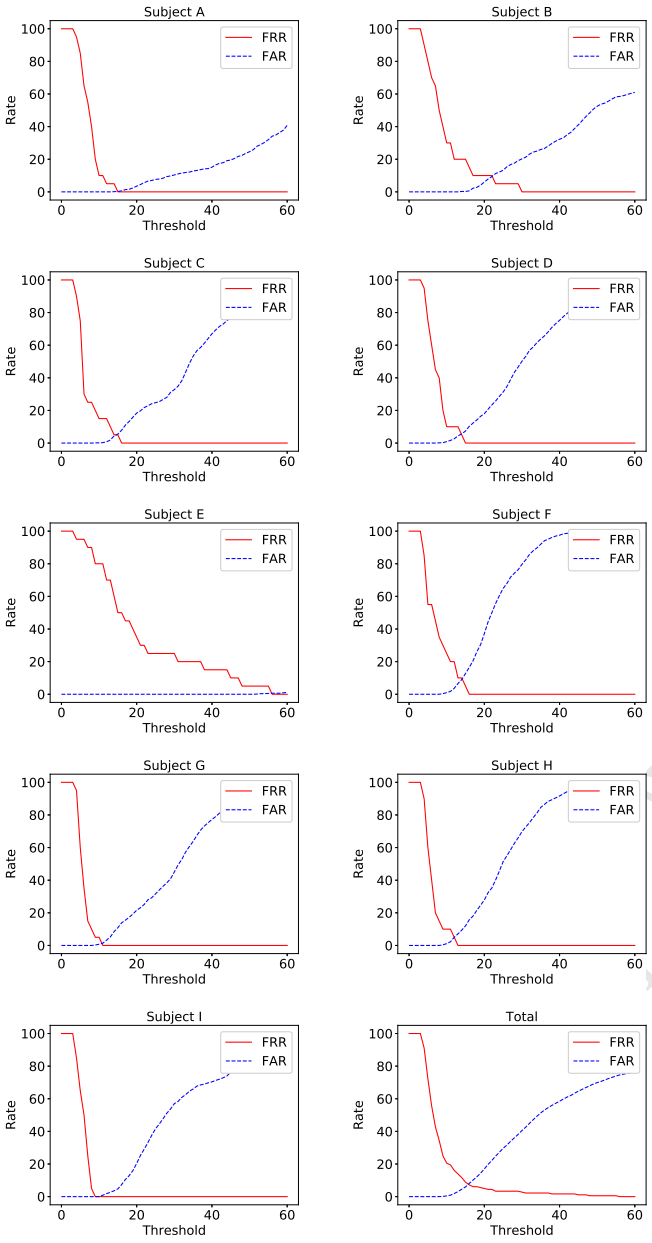

Figure 9: FRR and FAR for the subjects in user authentication.

Summarizing the results of user authentication, the mean EER of all subjects was approximately 0.076. It is necessary to validate with data from a larger number of subjects because there was a difference in EER between subjects. In addition, we will also examine a method for authentication using time series pressure data of helmet from start wearing to finish wearing.

5 CONCLUSION

In this study, we proposed a method to identify individuals based on individual differences in head shapes which is measured by wearing a helmet with pressure sensors. We implemented the prototype device and evaluated the proposed method. The prototype device is a commercially available full-face helmet and we attached 32 pressure sensors inside the helmet. In the evaluation, we obtained the sensor values for 2 seconds 20 times from nine subjects as head shape data. Using the acquired data, we evaluated the accuracy of user identification to determine who is wearing the helmet among the registrants and the accuracy of user authentication to determine whether the helmet wearer is the registrant or not.

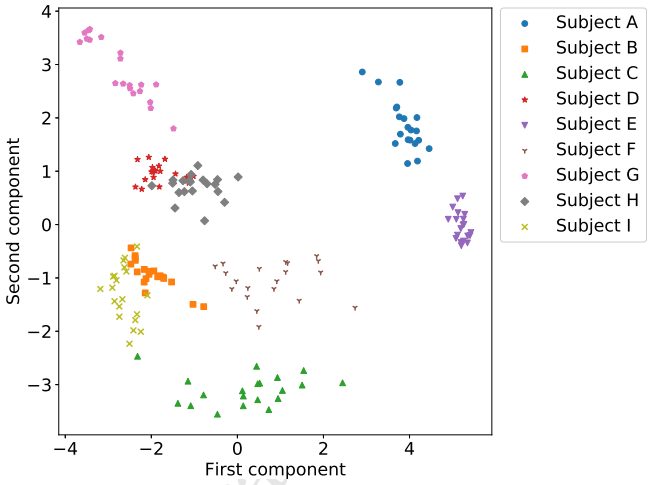

Figure 10: Principal component distribution of 32-dimensional features compressed into two dimensions by PCA

Since the accuracy was 100% with 32 sensors in the user identification, we tested how the accuracy changed by decreasing the number of sensors. The results showed that the smallest number of sensors showing 100% accuracy was five. EER of four out of nine subjects showed less than 0.012, and the average EER was 0.076 in the authentication. These results suggest that our method is effective as a user identification method. In the future, we will collect more data and evaluate the proposed method in a real environment.

REFERENCES

[1] J. Ajay Siddharth, A. P. Hari Prabha, T. J. Srinivasan, and N. Lalithamani. 2017. Palm Print and Palm Vein Biometric Authentication System. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Subhransu Sekhar Dash, K. Vijayakumar, Bijaya Ketan Panigrahi, and Swagatam Das (Eds.). Springer Singapore, Singapore, 539–545.

[2] T. Arakawa, T. Koshinaka, S. Yano, H. Irisawa, R. Miyahara, and H. Imaoka. 2016. Fast and accurate personal authentication using ear acoustics. In *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*. 1–4.

[3] R.G. Attewell, K. Glase, and M. McFadden. 2001. Bicycle helmet efficacy: a meta-analysis. *Accident Analysis & Prevention* 33, 3 (2001), 345–352. https://doi.org/10.1016/S0001-4575(00)00048-8

[4] Roman Bednarik, Tomi Kinnunen, Andrei Mihaila, and Pasi Fränti. 2005. Eye-Movements as a Biometric. In *Image Analysis*, Heikki Kalviainen, Jussi Parkkinen, and Arto Kaarna (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 780–789.

[5] Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang. 2017. Your face your heart: Secure mobile face authentication with photoplethysmograms. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. 1–9.

[6] T. Endo D. Kouno, K. Shimada. 2013. Person Identification Using Top-View Image with Depth Information. 1, 2 (2013), 67–79.

[7] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra. 2012. Authentication in mobile devices through hand gesture recognition. *International*

Journal of Information Security 11, 2 (2012), 65–83. https://doi.org/10.1007/s10207-012-0154-9

[8] R. Izuta, K. Murao, T. Terada, T. Iso, H. Inamura, and M. Tsukamoto. 2016. Screen Unlocking Method using Behavioral Characteristics when Taking Mobile Phone from Pocket. In *The 14th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2016)*. 110–114.

[9] M. Tsukamoto K. Fukumoto, T. Terada. 2013. A smile/laughter recognition mechanism for smile-based life logging. In *Proceeding of of the 4th Augmented Human International Conference (AH '13)*. 213–220.

[10] D. Kim and K. Hong. 2008. Multimodal biometric authentication using teeth image and voice in mobile environment. *IEEE Transactions on Consumer Electronics* 54, 4 (2008), 1790–1797.

[11] J. Kwon, D. Kim, W. Park, and L. Kim. 2016. A wearable device for emotional recognition using facial expression and physiological response. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 5765–5768.

[12] T. Nakao, N. T. Hung, M. Nagatoshi, and H. Morishita. 2012. Fundamental study on curved folded dipole antenna. In *Proceedings of the 2012 IEEE International Symposium on Antennas and Propagation*. 1–2.

[13] R. F. Nogueira, R. de Alencar Lotufo, and R. Campos Machado. 2016. Fingerprint Liveness Detection Using Convolutional Neural Networks. *IEEE Transactions on Information Forensics and Security* 11, 6 (2016), 1206–1213.

[14] Peter J. Rousseeuw and Katrien Van Driessen. 1999. A Fast Algorithm for the Minimum Covariance Determinant Estimator. *Technometrics* 41, 3 (1999), 212–223. https://doi.org/10.1080/00401706.1999.10485670 arXiv:https://amstat.tandfonline.com/doi/pdf/10.1080/00401706.1999.10485670

[15] A. Sayo, Y. Kajikawa, and M. Muneyasu. 2011. Biometrics authentication method using lip motion in utterance. In *2011 8th International Conference on Information, Communications Signal Processing*. 1–5.

[16] scikit-learn. [n.d.]. https://scikit-learn.org/.

[17] SciPy.org. [n.d.]. https://www.scipy.org/.

[18] J. Toth and M. Arvaneh. 2017. Facial expression classification using EEG and gyroscope signals. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 1018–1021.