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

Various types of helmets exist, including industrial protective helmets, motorcycle helmets, sports helmets, and military/police helmets. By identifying individuals wearing a helmet, their name, affiliation, and qualification can be presented on a display mounted on the helmet, and sensor data collected through the helmet, such as acceleration, video, and eye-tracking data, can be labeled with the user's ID. In this paper, we propose a user identification method based on head shape using a helmet equipped with 32 pressure sensors. Our method has two functions: user identification and authentication. Identification aims to classify a user as a registered user, while authentication aims to accept users who are registered in the system and reject unknown users. We implemented a prototype helmet device and collected data from nine subjects, resulting in 100% accuracy for user identification and an average equal error rate of 0.076 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

There are various types of helmets, such as industrial protective helmets, motorcycle and bicycle helmets, sports helmets (for American football, baseball, ice hockey, etc.), and military/police helmets. These are all worn to protect the head in the event of an accident [3]. From a safety point of view, it is important that there is no gap between the head and the helmet.

Workers in factories and disaster sites must also often wear helmets. Wearing a helmet can allow individuals who do not know each other, such as classroom use is granted without fee provided that copies are not made or distributed short-term workers and vendors, to be identified by displaying their names and work division on their helmets. Helmets can also allow wearers to be identified from a distance or overhead even if their faces cannot be clearly seen. Identifying individuals also serves as a deterrent to trespassers. In addition, displaying qualifications, such as a hazardous materials engineer's license and a heavy machinery license, can help create a safe work environment. In many cases, this information is written directly on the helmet, or an identifiable sticker is attached to the helmet. However, such an analog system makes it possible for trespassers to easily disguise themselves by forging or stealing a sticker. In addition, a worker can put on another worker's helmet without being aware of it, and incorrect information will be displayed. If helmets are shared among workers, they are not marked with 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 wearer's data and registered users' data and outputs the user with the most similar data.

The prototype helmet has a display to indicate the user's name and credentials based on the identification results; therefore, incorrect information is not displayed on the helmet if a helmet belonging to someone else is used. One advantage of this system is that identification information is automatically displayed on a shared helmet, allowing workers to identify each other. Another advantage of user identification is data annotation. Data collected by sensors attached to the helmet or wearer's body, such as a camera, eye tracker, and accelerometer, can be automatically annotated with the wearer's ID. By attaching a Global Positioning System (GPS) module or antenna to localize the user [12], the name and location of a worker can be determined in real time, allowing the foreperson to have a better understanding of the overall situation in the field. Furthermore, from the pressure data between the helmet and the head, it is possible to verify whether the shape of the head matches the helmet, as a zero pressure value signifies that there is a gap between the helmet and head. Another potential use of the proposed helmet is to serve as a key to a room whose access is restricted based on one's position or qualifications.

The proposed method has two functions: user identification and authentication. User identification is based on the assumption that a single helmet is shared by multiple individuals. The pressure sensor data of an individual who may wear a helmet are registered in advance, and an individual wearing a helmet is identified as one of the registered persons. Personal identification does not take into

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

account that a non-registered individual may wear the helmet; if a non-registered individual wears the helmet, the identification result will be a registered user who has the most similar data to the wearer. User authentication determines whether the individual wearing the helmet is in fact the individual with the ID when the ID is provided to the system. We assume an environment in which all individuals have their own helmets (as in smartphone authentication). In addition, we assume an environment in which the user ID is entered when using a shared helmet (as in automated teller machine [ATM] authentication). Even if an intruder wears a helmet and enters a stolen ID, he or she can be identified as an intruder (authentication denied) because the head shape differs from that of the individual with the ID.

The remainder of this paper is organized as follows. Section 2 introduces related work, Section 3 describes the proposed method, Section 4 evaluates the proposed method, and Section 5 concludes the 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 for identifying individuals: password, personal identification number (PIN), and stroke pattern; physical characteristics, such as face, fingerprint, voice print, and iris; and behavioral characteristics, such as handwriting and gait. However, passwords, PINs, and stroke patterns that can be freely set by individuals have a risk of spoofing by shoulder hacking, brute force attacks, and password duplication.

For physical characteristics, Chen et al. [5] proposed an authentication method using video images of the user's face and fingertips captured from the front and rear cameras of a mobile device. Siddharth et al. [1] proposed an authentication system based on the palm print and palm vein. The system uses visible and infrared light to acquire images of the palm print and palm vein, and authentication is performed by verifying the data against registration data in the database. Sayo et al. [15] proposed an authentication method based on a camera image that captures the shape of a user's lips (physical characteristic) and the movement of the lips during speech (behavioral characteristic). Another authentication method involving the mouth proposed Kim et al. [10] 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 the distance of the infrared reflection of the eye. Using a camera-based approach such as the ones described above, a camera can be mounted on the outside of the helmet, and individuals can be identified by facing the camera before putting on the helmet. However, taking a picture of one's own face with the camera is complication. Using the palm print and palm vein method, users would have to hold the camera each time before putting on the helmet. It is also complication. A camera can be attached to the mouth of the helmet so that the shape and movement of the wearer's lips and teeth can be acquired. However, the space around the mouth inside a full-face helmet is limited, and it is difficult to distinguish the shape and movement around the mouth with a single camera. In addition, this approach is not practical because helmets are sometimes used in dark places.

Nogueira et al. [13] used convolutional neural networks for fingerprint authentication and achieved high classification accuracy. However, the limitation of fingerprint authentication is that fingerprints can be easily duplicated from photographs. In contrast, head shape, which is used in this paper, is a physical characteristic that is difficult to replicate due to its three-dimensional shape.

With respect to behavioral characteristics, the authors proposed a method that authenticates smartphone users using acceleration sensor data from taking a smartphone out of their pockets [8]. Guerra-Casanova et al. [7] proposed a method for authenticating users by the gestures of their hands using a mobile device with an embedded accelerometer. For motion-based authentication using accelerometers, it is possible to use the acceleration characteristics of motions before the helmet is put on for authentication by mounting an accelerometer on the helmet. However, there are various ways of putting on a helmet, such as putting it on in a hurry and taking care not to let the interior of the helmet become wet in the rain. Therefore, it is not practical to collect data from all individuals for various situations.

2.2 Head State Recognition

Toth et al. [18] focused on facial muscle signals, and six different facial expressions were classified using muscle signals and gyroscope values that were obtained from a low-cost off-the-shelf electroencephalogram (EEG) headset. EEG headsets are generally used to measure brain waves; however, muscle signals are detected locally because the measurement is performed by placing electrodes on the scalp. This method only uses existing EEG devices for the classification of facial expressions, and no additional electromyography sensors are used. Kwon et al. [11] designed a glasses-type wearable device to detect a user's emotions based on facial expressions and physiological reactions. The device can capture facial expressions with a built-in camera and detect physiological responses, such as photoplethysmogram signals and electrodermal activity. Fukumoto et al. [9] designed a smile-based life-logging system that focuses on smile and laughter to index interesting or enjoyable events on recorded video. They used photointerrupters, and smile/laughter was detected separately by threshold-based clustering. The evaluation results demonstrated a 73–94% accuracy in detecting smile/laughter during actual use of the system.

These studies all use dynamic information, such as facial expressions and physical movements in the facial area. In contrast, our study uses static features of head shape.

I think it is necessary to separate them in subsections here? In other research, Kouno et al. [6] proposed an image-based person identification system using depth images from an overhead camera. By using depth information, this system captures the precise location of the individual, and four features are extracted from the images: body height, body dimensions, body size, and a depth histogram. The identification accuracy was 94.4% and 91.4% while standing in front of a door and touching a doorknob, respectively.

In this paper, we propose a method for identifying individuals by acquiring their head shape with pressure sensors while they wear a helmet. Our method does not require individuals to perform special

behaviors or remain stationary for identification. With a wearable approach, our method can be used at any place and time. To breach the system, the exact three-dimensional shape of a person's head is required, which is difficult to replicate.

3 PROPOSED METHOD

In this section, we present the details of the proposed method.

3.1 Overview

The proposed method assumes that a user wears a helmet equipped with pressure sensors. It then acquires the shape of the wearer's head and determines whether the wearer is a registered user. The proposed method has two functions: user identification and authentication.

- **User identification** assumes that a single helmet is shared by multiple people and that no other information, such as the ID, is provided to the system; the user simply puts on the helmet. Users' pressure sensor data are registered in advance, and a user who puts on a helmet is identified as one of the registered users, as illustrated in **Figure 1**. User identification does not consider that a non-registered person may put on the helmet. If a non-registered person puts on the device, the identification result will be an individual with the closest data among the registered users.
- **User authentication** determines whether the individual wearing the helmet is the correct individual when his/her ID or username is provided. We assume two cases in which authentication is used: (i) each individual has his/her own helmet and only the individual's pressure sensor data have been registered (single user; username is preset on device, as in smartphone authentication); and (ii) a helmet is shared among multiple users, and a username is entered when putting on the helmet (multiple users; usernames are input manually, as in ATM authentication). The pressure sensor data are registered in advance, and a user who puts on the helmet is accepted or rejected by calculating the similarity between the input data and the data corresponding to the ID, as illustrated in **Figure 2**. Even if the ID is leaked, an intruder can be rejected if his/her head shape differs from the data corresponding to the ID.

In the proposed system, a total of 32 pressure sensors are attached to the inner side of the helmet to acquire data, producing one-dimensional 32-channel pressure data. Pressure data of individuals who are expected to wear helmets are registered in the system in advance and are called training data in this paper. In user identification, the proposed system uses a 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 user authentication, the system calculates the Mahalanobis distance between the training and input data of the user, including non-registrants, and authenticates the user if the distance is less than the threshold; otherwise, the user is rejected.

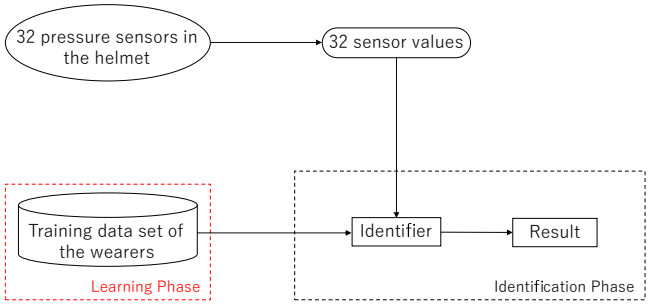

Figure 1: Process of user identification.

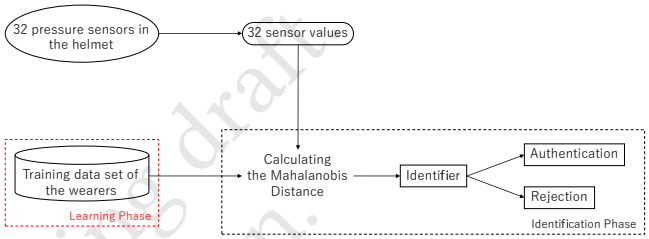

Figure 2: Process of user authentication.

3.2 Hardware

We developed a helmet equipped with 32 pressure sensors. **Figure 3** presents the configuration of the device, and **Figure 4** provides an image of the device. The head of the user 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 Short Tail manufactured by Interlink Electronics, Inc. The Arduino MEGA2560 R3 was used as a microcomputer. Because the helmets was difficult to attach and remove the interior, we removed the interior of the top of the helmet and installed a thick urethane sponge, as illustrated in **Figure 5**. The urethane sponge was cut and a pressure sensor was inserted into the cut line, as illustrated in **Figure 6**.

Four pressure sensors were placed at the top of the head, 16 sensors were placed around the top of the head, six sensors were placed at the back of the head, and six sensors were placed at the cheek pads on both sides. A total of 32 sensors were installed at the points, as displayed in **Figure 7**. The wiring for the pressure sensors passed through a hole drilled at the top of the helmet and was then connected to a 5V power supply port, GND, and analog input port, which was on the Arduino MEGA2560 R3 via a printed circuit board (PCB) with a 10KΩ resistor that was mounted outside the helmet. The PCB and a display to show ID attached to the exterior of the helmet are illustrated in **Figure 8** and **Figure 9**. The PCB and a display were bolted to both of the cheek area using a threaded hole drilled to secure the helmet shield, and was fixed and removable.

3.3 User Identification Method

3.3.1 Preprocessing. Data acquisition begins when a user puts on the helmet. Data from 32 pressure sensors $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$

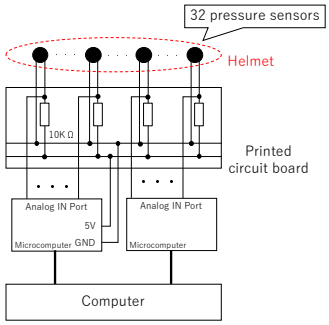

Figure 3: Structure of device.

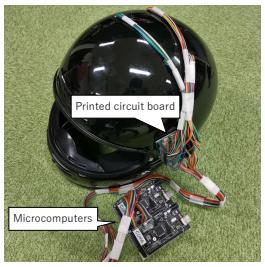

Figure 4: Appearance of device.

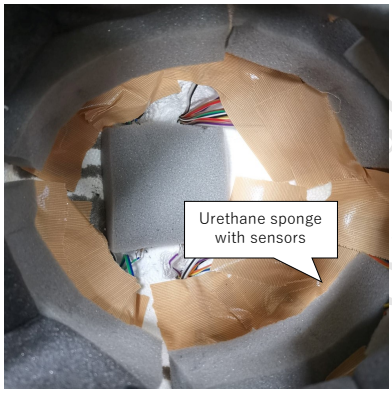

Figure 5: Interior of device.

are acquired at time t. The voltage values of all pressure sensors are almost 5V when the helmet is not worn, then sum of the data show $\sum_{i=1}^{32} p_i(t) \approx 160[V]$. When the helmet is worn, $p_i(t)$ decreases, and the system segments the data over a 2-s window starting from $t = T_s$ after the values are stabilized. Time $t = T_s$ is the time at which the change of the sum of 32 dimensions per sample is less than 2V for 11 consecutive samples (≈11/30 second as the sampling rate is approximately 30 Hz) after the sum of 32 dimensions is less than 155V, i.e. $\sum_{i=1}^{32} |p_i(t) - p_i(t-1)| < 2[V]$ $(i = T_s, \cdots, T_s - 10)$. 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

Figure 6: Mounting method for pressure sensors.

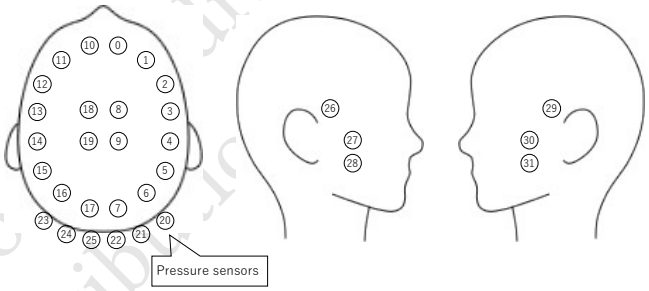

Figure 7: Position of pressure sensors.

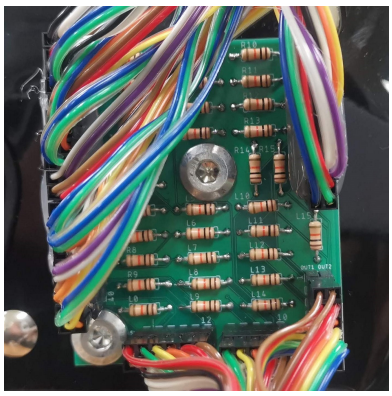

Figure 8: Printed circuit board connected to 32 pressure sensors.

$\boldsymbol{x}(t) = [x_1(t), \ldots, p_{32}(t)]$ as a feature. Once the data is segmented, the preprocessing is suspended until $\sum_{i=1}^{32} p_i(t) > 159[V]$ is met.

3.3.2 Identification. Given training data $[\boldsymbol{x}_m, y_m]$ $(m = 1, \ldots, M)$ from users who are expected to use the helmet by wearing the helmet a total of M times 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

Figure 9: Showing name on a display.

the user to be identified are 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, data from 32 pressure sensor data $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$ and the average $\boldsymbol{x}(t) = [x_1(t), \ldots, p_{32}(t)]$ are obtained as a feature in the same manner as for user identification.

3.4.2 Similarity calculation. In user authentication, there are two cases for using training data: data of a single user are used and data of multiple users are used. For single-user data, data of only a single user (e.g., owner of the helmet) are registered or data of multiple users are registered; however, the data of only one of the users whose ID is provided are used. For multiple-user data, data of multiple users who are expected to use the helmet are used. With training data $[\boldsymbol{x}_m, y_m]$ $(m = 1, \ldots, M)$ obtained from user(s) 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 a method for calculating the distance between multiple variables, and 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 (1) and (2).

$$\boldsymbol{\mu} = \frac{1}{M}\sum_{m=1}^{M}\boldsymbol{x}_m \tag{1}$$

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

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

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

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

3.4.3 Authentication decision. Letting θ be the threshold value, a user is authenticated if (4) is satisfied and is rejected if (4) is not satisfied.

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

3.5 Software

The Arduino MEGA program was implemented by Arduino IDE, and a computer program that received data from Arduino MEGA and saved it in comma-separated values format was implemented in Python. A computer program to analyze the data was also implemented in Python.

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

In user authentication, the system loaded the collected sensor data and computed the variance-covariance matrix using `sklearn.covariance.MinCovDet`. For calculation of the Mahalanobis distance, `scipy.spatial.distance` was used. The 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 implement Fast-MCD [14], a faster version of MCD. `scipy.spatial.distance` is a SciPy [17] library that implements functions for calculating various distances.

4 EVALUATION

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

4.1 Data Collection

We instructed nine subjects (A~I, all male, mean age 23 years) to wear the helmet implemented in Section 3 and collected sensor data. The sampling rate was approximately 30 Hz. The subjects put the helmet on for 2 s to collect data, then took it off and put it on again for 2 s to collect data, through which a set of two samples was obtained. By collecting data of 10 sets (20 samples) from each subject, a total of 180 samples (2 s × 20 samples × 9 subjects) were collected. Up to four sets of data were collected per person per day. To collect data for various positions of the sensors and head, 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 using 5-fold cross-validation in which 80% of the data (16 samples) collected from each subject were trained and 20% (four samples) were tested. To investigate the effect of the number of sensors used, the identification accuracy for all combinations of sensors from 1–32 sensors was measured.

To simulate a half helmet, which is commonly used at construction sites, the identification accuracy for all combinations of sensors from 1 to 20 sensors limited in the top half out of 32 sensors were measured. These 20 sensors are sensors #0–#19 in **Figure 7**. In

Table 1: Identification accuracy with a full-face helmet, where the number of sensors was reduced from 32 to 1.

Sensors used	Accuracy
32 sensors	1.000
31 sensors	1.000
⋮	⋮
5 sensors	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, where the number of sensors was reduced from 20 to 1.

Sensors used	Accuracy
20 sensors	1.000
19 sensors	1.000
⋮	⋮
5 sensors	1.000
#0, #3, #5, #16	0.994
#0, #3, #13	0.983
#3, #16	0.928
#10	0.617

this evaluation, two types of sensor configurations were tested: a full-face helmet with 32 sensors and a half helmet with 20 sensors.

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

We determined that the accuracy was 1.000 when 32 and 31 sensors were used for the full-face helmet and 20 and 19 sensors were used for the half helmet. Therefore, we measured the accuracy from one sensor until the accuracy reached 1.000 and skipped the measurement of the accuracy for additional sensors.

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

For the half helmet, nine subjects were identified with 100% accuracy when five sensors were used. The accuracy was 99.4% using four sensors, 98.3% using three sensors, and 92.8% using two sensors. However, the accuracy decreased significantly to 61.7% when only one sensor was used.

Both the full-face helmet and half helmet achieved 100% accuracy with at least five sensors for the dataset used in this experiment. However, the number of sensors required to achieve high accuracy may increase as the number of registrants increases. For the sensors used for the full-face helmet, most were numbered under #20, signifying that sensors in the top half were significant.

Table 3: Equal error rate (EER) for 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 User Authentication Method

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

In user authentication, the false rejection rate (FRR), false acceptance rate (FAR), and equal error rate (EER) were used as indicators of authentication accuracy. The FRR is the rate at which a registered user is mistakenly considered a stranger and rejected, whereas the FAR is the rate at which a stranger is mistakenly considered a registered user and authenticated. The smaller the threshold value θ in 4 is set, the stricter the authentication decision becomes, resulting in an increased FRR. In contrast, the larger the threshold value θ is set, the looser the authentication decision becomes, resulting in an increased FAR. There is thus a trade-off between the FRR and FAR, and the value at which the FRR and FAR are equal is called the EER. The EER value is commonly used as an indicator to evaluate the performance of authentication methods, and a small EER indicates better performance.

4.3.2 Results and discussion. The EER of each subject is presented in **Table 3**. In this table, "Average" represents the average EER of all subjects. The FRR and FAR values for each subject by varying the thresholds from 0 to 60 by 1 are presented in **Figure 10**. In this figure, "Average" represents the average FRR and FAR of all subjects. The EER of subjects A, E, G, and I was approximately 0.01 or lower, which signifies that the owner failed authentication less than once in 100 times and that strangers broke the authentication less than once in 100 times. An 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 were C, D, and H, with an EER of approximately 0.05. To determine the cause of the decline in accuracy compared with subjects A, E, G, I, all collected data were compressed to the first principal component and second principal

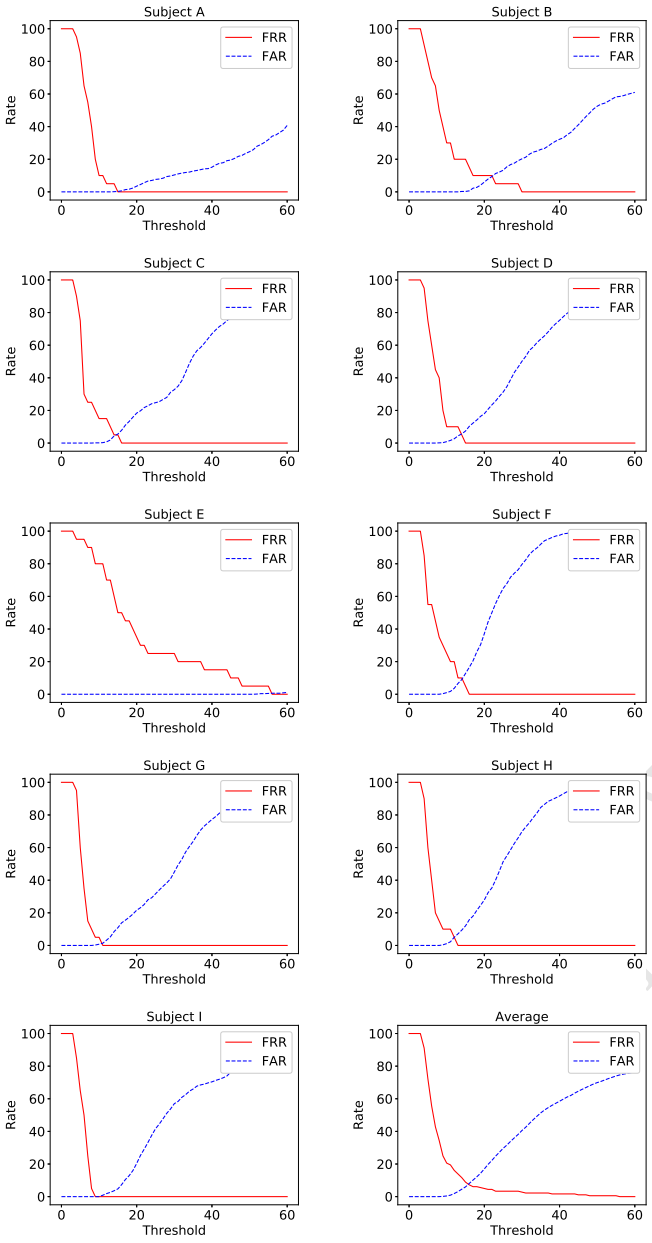

Figure 10: False rejection rate (FRR) and false acceptance rate (FAR) for subjects in user authentication.

component by principal component analysis (PCA). The results of the data plotted on a two-dimensional plane are presented in **Figure 11**. The plots for subject C indicate that one sample of the data of subject C was close to the data of subject I and the variance in the first principal component was large, which would reduce the accuracy. Furthermore, the data for subjects D and H significantly overlapped with each other, which affected the accuracy of both subjects.

The least accurate subjects were B and F, with an EER of approximately 0.095. Data for subject B was some overlap with the data

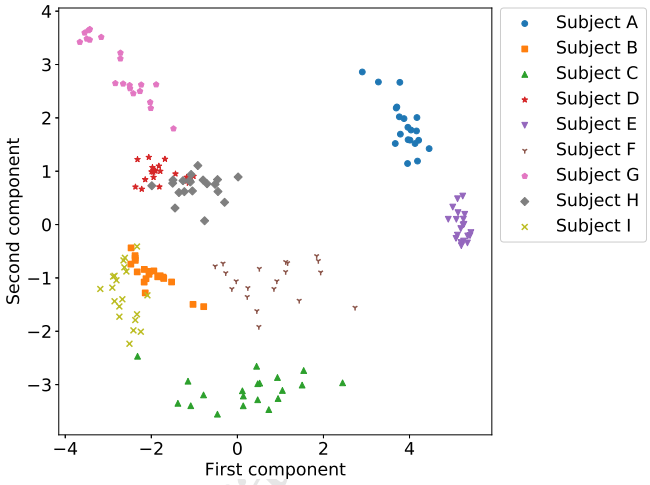

Figure 11: Principal component distribution of 32-dimensional features compressed into two dimensions by principal component analysis.

of subject I. However, the EER of subject I was 0, which indicates perfect authentication. Therefore, the overlap of these data groups was likely due to the loss of data when they were compressed into two dimensions by PCA. On the other hand, subject F's data did not exhibit any overlap with other subjects' data; however, there was a large variance in 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 for subjects B and C, who had 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 was likely to be lower than that of subject C because the two samples of subject B were located in close proximity to subject F's data group.

The data of subject E were located at the rightmost points. In addition, the variance was small, and the data were thus considered distinct. For subject E in **Figure 10**, the FRR and FAR crossed at a threshold of approximately 60, which was greater than for the other subjects. This is because the data were quite different from the others, and the FAR did not increase by increasing the threshold.

In summary, the mean EER of all subjects in user authentication was approximately 0.076. It is necessary to validate with data from a larger number of subjects, as there was a difference in the EER between subjects. In addition, it is necessary to investigate a method for authentication using time series pressure data from the start of wearing the helmet to the complete of wearing.

5 CONCLUSION

In this study, we proposed a method to identify individuals based on differences in head shape, which was measured by wearing a helmet with pressure sensors. We implemented the prototype device and evaluated our proposed method. The prototype device was a commercially available full-face helmet, and we attached 32 pressure sensors inside the helmet. In the evaluation, we obtained sensor values for 2 s 20 times from nine subjects as head shape data. Using

the acquired data, we evaluated the user identification accuracy to determine which user was wearing the helmet among the registrants. In addition, we evaluated the user authentication accuracy to determine whether the helmet wearer was the registrant.

As the accuracy was 100% with 32 sensors in user identification, we tested how the accuracy changed by decreasing the number of sensors. The results indicated that the smallest number of sensors producing 100% accuracy was five. The EER of four out of nine subjects was less than 0.012, and the average EER in authentication was 0.076. These results suggest that our method is effective as a user identification method. In the future, we will collect additional 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.