Journal of Information Processing Vol.26 1–9 (Jan. 2018)

[DOI: 10.2197/ipsjjip.26.1]

Regular Paper

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

Atsuhiro Fujii[1,a)] Kazuya Murao[1,2,b)]

Received: March 4, 2016, Accepted: August 1, 2016

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. User identification is based on the assumption that a single helmet is shared by multiple individuals. The goal of this method is to identify which of the registered people is the person wearing the helmet. User authentication determines whether the individual wearing the helmet is the individual with the ID when the ID is provided to the system. In the evaluation, we obtained sensor values for 2 seconds 20 times from nine subjects as head shape data. The accuracy was evaluated using 5-fold cross-validation, and we achieved 100% accuracy with five sensors and 92% with two sensors for user identification and an average equal error rate of 0.076 with 32 sensors for user authentication.

Keywords: User identification, pressure sensor, helmet, head shape

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[1]. 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 an antenna to localize the user[2], 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 assump-

[1] Ritsumeikan University, Kusatsu, Shiga 525–8577, Japan
[2] PRESTO, Japan Science and Technology Agency, Kawaguchi, Saitama 332–0012, Japan
[a)] atsuhiro.fujii@iis.ise.ritsumei.ac.jp
[b)] murao@cs.ritsumei.ac.jp

tion 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 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. This helps avoid the risk of motorcycle theft. For example, the helmet and the motorcycle are paired in advance using RFID[3], then theft of the motorcycle can be prevented by authenticating the user when riding.

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, Section 5 describes limitation of the proposed method, and Section 6 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.[4] 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.[5] 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.[6] 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 by Kim et al.[7] combines dental images and voice. Bednarik et al.[8] 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. Barros Barbosa et al.[9] showed that images of the fingernail plate can be used as a transient biometric with a useful life-span of less than 6 months. 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. In addition, this approach is not practical because helmets are sometimes used in the rain. In the case of authentication methods that use images from a camera, the accuracy may be degraded if the camera lens is covered with water droplets or dust.

Nogueira et al.[10] used convolutional neural networks for fingerprint authentication and achieved high classification accuracy. However, fingerprint authentication requires the user to touch the sensor for each authentication. In contrast, our method does not require any specific behavior. Schneegass et al.[11] proposed a biometric user identification method using that the way sound is transmitted through the head differs from person to person. They played white noise from a bone conduction speaker attached to the side of the head, received signals using a microphone, and identified the subjects based on their characteristics. As a result, they achieved 97.0% accuracy. Dai et al.[12] proposed SpeakPrint, a human speech authentication scheme for smartphones which is resistant for attacks such as spoofing, based on the user's mouth movements and the voice changes. Jian et al.[13] proposed the process of voiceprint recognition with Gaussian mixture model (GMM) which is a kind of probability and statistics model. Zhang et al.[14] constructed a voiceprint recognition model using DNN to achieve higher recognition performance. However, the experiment showed that the DNN-based voiceprint recognition system still had a low accuracy rate of rejection of counterfeiters. For this reason, the trust degree and label distance were introduced, and the two-order judgment structure based on DNN-RLIANCE algorithm was proposed. These are studies on authentication methods that use sound. The helmet may be used in noisy environments such as construction sites, so these authentication methods are not suitable.

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[15]. Guerra-Casanova et al.[16] 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. We think that the helmet-wearing motion is not highly reproducible. As for the motion of taking the smartphone out of the pocket, the reproducibility is high because the movement is restricted to some extent. However, the helmet is worn with one hand, two hands, or in a different direction, and there are a variety of actions from picking up the helmet to putting it on. Therefore, it is not practical to collect data from all individuals for various situations.

2.2 User Authentication Method with Pressure Sensors

Chen et al.[17], [18] proposed a user authentication method based on the driver's grasping pattern using a pressure sensor sheet attached to the handlebars of a bicycle. In Reference [17], the authentication decision was made using the features of the grasp data obtained from the pressure sensor sheet. The experimental results obtained in this study show that the mean acceptance rates of 78.15% and 78.22% for the trained subjects and the mean rejection rates of 93.92% and 90.93% to the un-trained ones are achieved in two trials, respectively. In Reference [18], authentication was performed using time series data of pressure values. The experimental results obtained in this study show that mean acceptance rates of 85.4% for the trained subjects and mean rejection rates of 82.65% for the un-trained ones are achieved by the classifier in the two batches of testing. Iso et al.[19] proposed a user authentication method by using a pressure sensor array mounted on the side of a mobile phone to identify the grasping state of the phone during use. The authors proposed a user authentication method using pressure sensors mounted on the side and back of a mobile phone, based on a pre-registered gripping method[20].

These are all researches on authentication methods based on behavioral characteristics such as grasping using a pressure sensor. On the other hand, we use a pressure sensor to obtain physical characteristics for user authentication.

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. 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. Even if the ID is leaked, an intruder can be rejected if his/her head shape differs from the data corresponding to the ID.

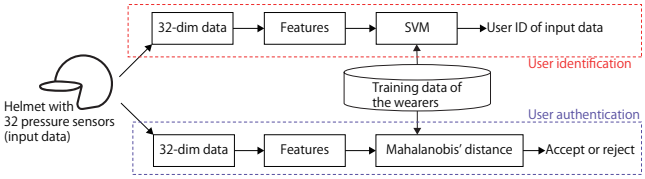

Fig. 1 Process of user identification and authentication.

The flow of our system is illustrated in **Fig. 1**. 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.

3.2 Hardware

We developed a helmet equipped with 32 pressure sensors. **Fig. 2** presents the configuration of the device, and **Fig. 3** 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 free size (57~60 cm) full-face helmet (BB100 manufactured by B&B ≈ 4,000 JPY). The pressure sensors were FSR402 (≈ 500 JPY) and FSR402 Short Tail (≈ 550 JPY) manufactured by Interlink Electronics, Inc. The Arduino MEGA2560 R3 (≈ 6,000 JPY) was used as a microcomputer. This is equipped the 10-bit ADC, and the value of the pressure sensor is acquired in the range of 0-5V. 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 **Fig. 4**. The urethane sponge was cut and a pressure sensor was inserted into the cut line, as illustrated in **Fig. 5**.

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 **Fig. 6**. 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 **Fig. 7** and **Fig. 8**. They were bolted to both of the cheek a[illegible]sing a threaded hole drilled to secure the helmet shield, and w[illegible]ixed and removable.

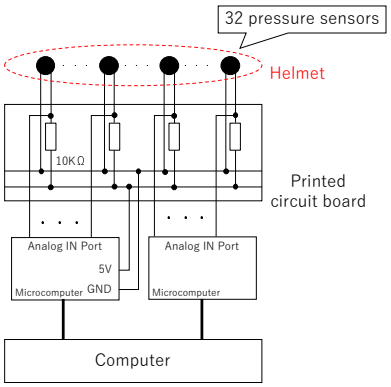

Fig. 2 Structure of device.

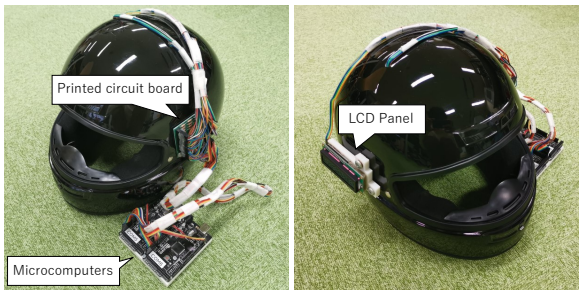

Fig. 3 Appearance of the prototype device.

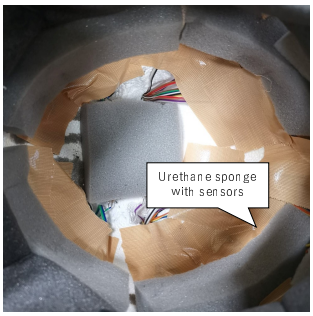

Fig. 4 Interior of the prototype device.

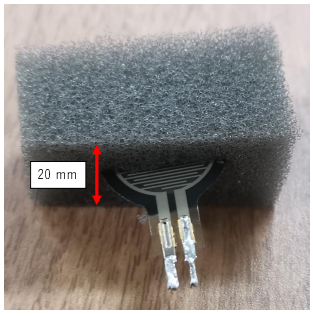

Fig. 5 Pressure sensor mounted in the helmet using urethane sponge.

The size of the helmet is shown in **Fig. 9**. The height, width, and depth of the helmet are 260 mm, 213 mm, and 282 mm, respectively, and the weight including a PCB and a LCD display is 1456 g.

The straps should be tightened until it is snug, so that no more than one or two fingers fit under the strap.[21] However, it is not necessary to tighten the straps so tightly that the neck becomes tight. We did not use the straps in the prototype device because we thought the effect of the straps tightening on the sensor value would be small.

3.3 User Identification Method

3.3.1 Preprocessing.

Data acquisition begins when a user puts on the helmet. Data from 32 pressure sensors $\boldsymbol{p}(t) = [p_1(t), \cdots, p_{32}(t)]$ are acquired at time t. The voltage values of all pressure sensors are almost 5V when the helmet is not worn, therefore the sum of the data stream $\sum_{i=1}^{32} p_i(t) \approx 160[V]$. When the helmet is put on, $p_i(t)$ decreases, and if $\sum_{i=1}^{32} p_i(t) < V_{wakeup}[V]$, the system enters the detection

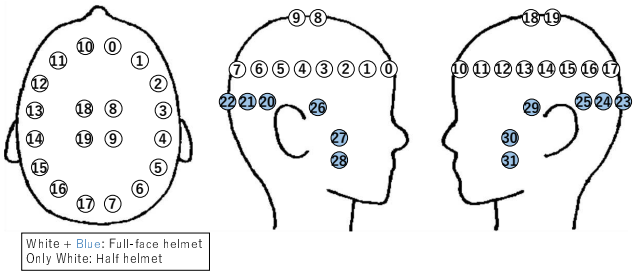

Fig. 6 Position of pressure sensors.

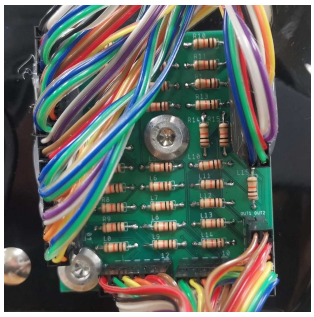

Fig. 7 Printed circuit board connected to 32 pressure sensors.

Fig. 8 LCD display to show name.

Fig. 9 Size of the prototype device.

state. The user decides in advance the pressure $V_{wakeup}[V]$ to wake up the system. The system segments the data over a 2-second 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 $V_{start}[V]$ for N_{start} consecutive samples ($\approx N_{start}/30$ second as the sampling rate is approximately 30 Hz), i.e. $\sum_{i=1}^{32} |p_i(t) - p_i(t-1)| < V_{start}[V]$ $(i = T_s, \cdots, T_s - N_{start} - 1)$. The user decide in advance the sample number N_{start} and the pressure $V_{start}[V]$. When N_{start} is small or $V_{start}[V]$ is large, the authentication process starts quickly, but it may be more prone to false recognition. 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 $\boldsymbol{x}(t) = [x_1(t), \ldots, x_{32}(t)]$ 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 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 $\boldsymbol{\Sigma}$ 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).

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

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 $\boldsymbol{\Sigma}$.

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, for the SVM, `sklearn.svm.SVC` of the scikit-learn [*1] 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 computed the variance-covariance matrix using `sklearn.covariance.MinCovDet`.

[*1] `https://scikit-learn.org`

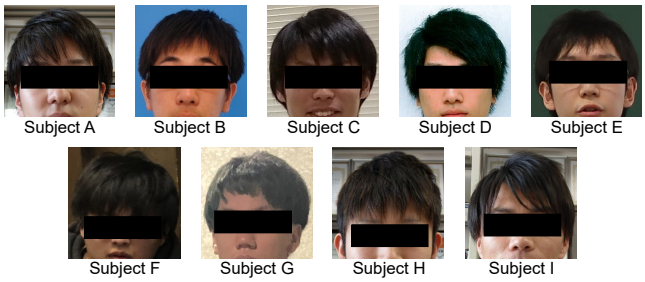

Fig. 10 Head photographs of the nine subjects.

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 [22], a faster version of MCD. `scipy.spatial.distance` is a SciPy [*2] 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 old) to wear the helmet implemented in Section 3 and collected sensor data. Head photographs of the nine subjects are shown in **Fig. 10**. The sampling rate was approximately 30 Hz. The subjects put the helmet on for 2 seconds to collect data, then took it off and put it on again for 2 seconds 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 seconds, 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 Fig. 6. In 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

[*2] `https://scipy.org`

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

half helmet is presented in **Table 1** and **Table 2**. The numbers listed in the "Sensors used" column are the number of sensors in Fig. 6. 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 sensors 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. The half-helmet model showing slightly higher accuracies in some cases in Table 1 and Table 2, but this is probably due to the random division of the cross validation set, which resulted in slight differences in accuracy between the full-face and half-helmet models.

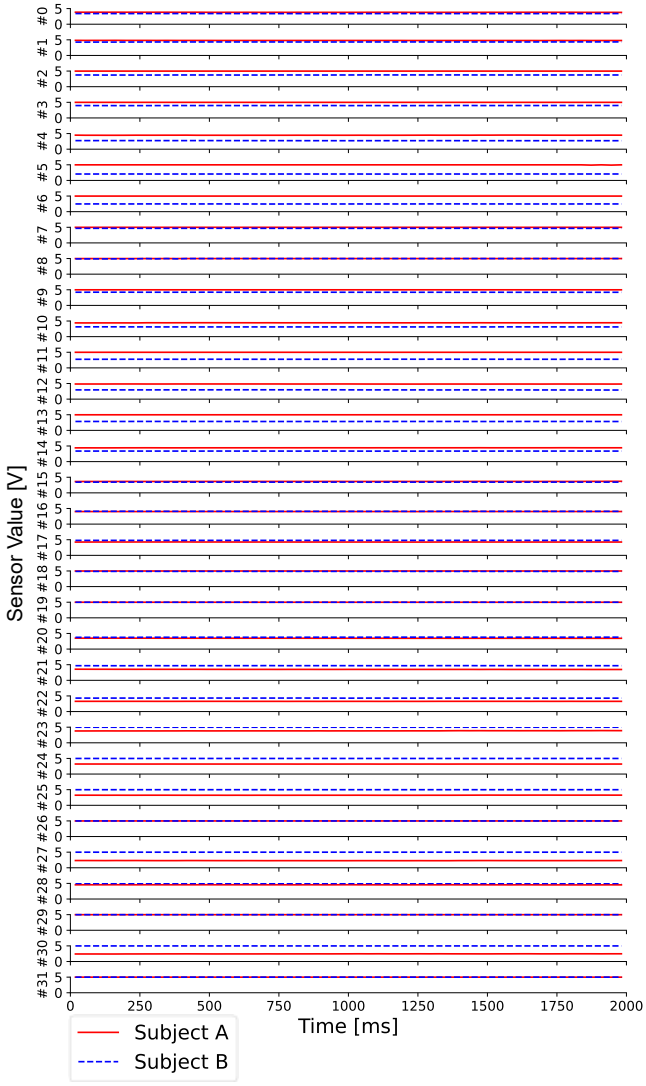

Fig. 11 The 2-second time series values obtained from the 32 sensors for subjects A and B wearing the helmet.

For the sensors used for the full-face helmet, most were numbered under #20, indicating that sensors in the top half were significant. For #20 and above, #24 and #25 are shown as effective sensors in Table 1. In fact, no difference in performance exists between #20-#25, but they may have been selected because they were particularly close to the subject's head. #26-#31 were placed around the cheeks, so the face and the sensor were in contact but not in strong contact for some people. **Fig. 11** shows the 2-second time series values obtained from the 32 sensors of subjects A and B wearing the helmet. The horizontal axis is time, and the vertical axis is the sensor value. The sensor value is a voltage value in the range of 0-5V. The more the head is pressed against the sensor, the closer the value is to 0V. On the other hand, when the head is not touching the sensor, the value is almost 5V. From Fig. 11, we can see that the sensor values of #26-#31 of subject B hardly changed. The values of #26-#31 did not differ greatly from one wearer to another, and the effect was small.

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 equation (4) in section 3.4.3 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 **Fig. 12**. 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. [23]; 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 component by principal component analysis (PCA). The results of the data plotted on a two-dimensional plane are presented in **Fig. 13**. The plots for subject C indicate that one sample

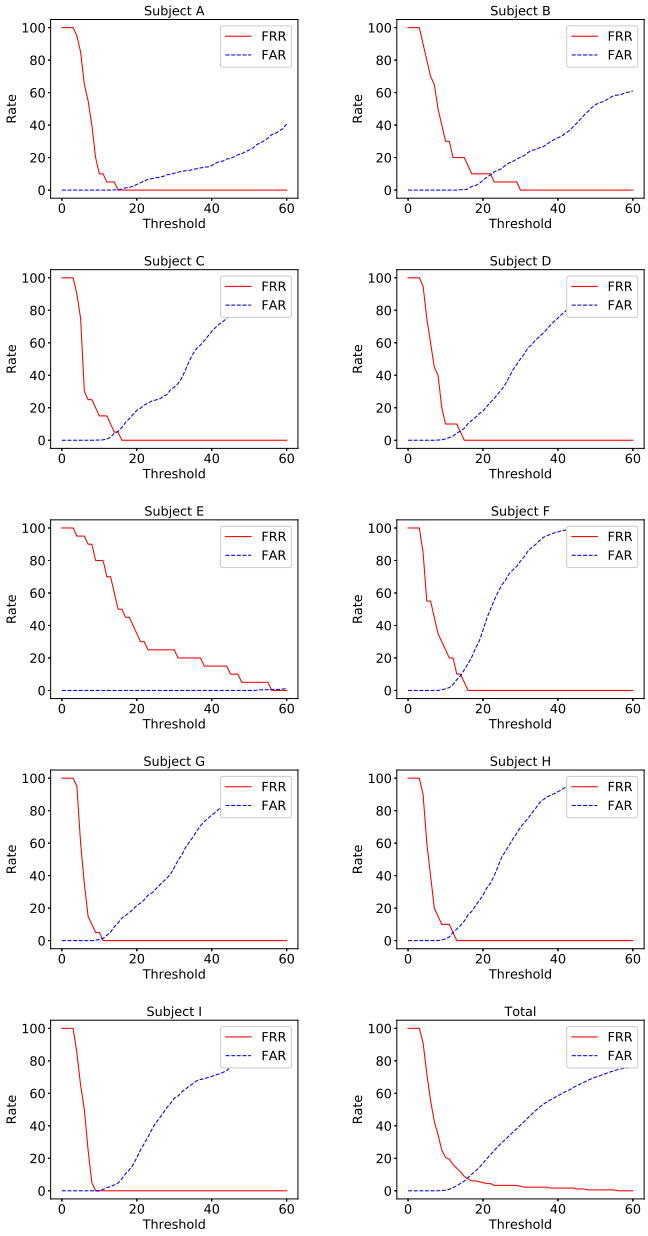

Fig. 12 False rejection rate (FRR) and false acceptance rate (FAR) for subjects in user authentication.

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 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

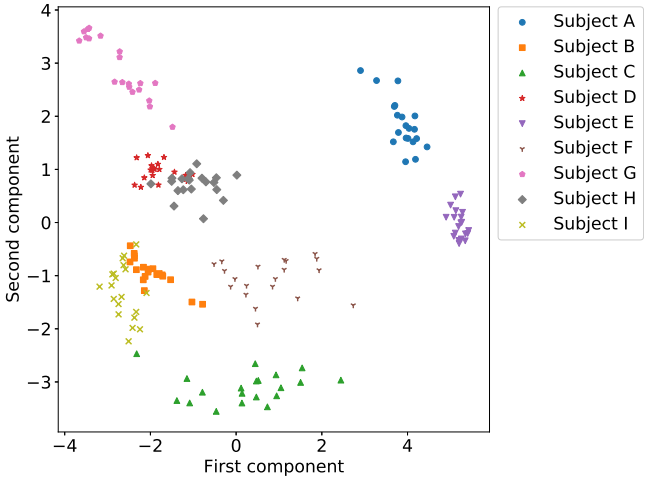

Fig. 13 Principal component distribution of 32-dimensional features compressed into two dimensions by principal component analysis.

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 Fig. 12, 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. An authentication method with grip gestures using pressure sensors[20] reported the average EER of 0.02. Our method is not as accurate as this method.

5. Limitation

From the results in Section 4, it can be seen that we were able to identify the subjects with high accuracy in the experimental environment. This section discusses the limitation of the proposed method.

5.1 Restrictions on subjects and helmets

In this method, the strength of the contact between the head and the helmet is obtained as the feature values using a pressure sensor. Therefore, if there is no change in the shape of the head, it can always be identified correctly regardless of age, gender, or body size. On the other hand, if the hairstyle changes, the strength of the contact between the head and the helmet will change, and the system will not be able to correctly identify the user. If the sensor mounting position is moved, the accuracy may decrease because the feature values changes. For the same reason, it is not possible to use the same registration data for different helmets, because the feature values are affected by the size and weight of the helmet. User registration phase is required for each helmet. In the future, it is necessary to consider a calibration method based on helmet size and weight data.

5.2 Helmet size adjustment

In this experiment, the helmet size was not adjusted for each subject, and all subjects used the same helmet to collect data. We think that when helmets are shared, the size is not adjusted for each user. On the other hand, if multiple sizes of helmets are given, such as S/M/L, the data with the helmet to be used must be registered. In the case of a personal helmet, the evaluation should be done by preparing a helmet that fits each wearer individually. However, only one type of helmet was used in this experiment. If the best helmet is used for each subject, the system will be able to obtain accurate data on the head shape of the registrant, and the system will not be able to obtain accurate data on the head shape of the non-registrant (e.g. thief) whose helmet size does not fit. Therefore, we think that the performance of the proposed method will be improved. In the future, we will evaluate the proposed method in these environments.

5.3 Identifiable scale

In a large construction site, approximately 1,000 workers may work together. Zhuang et al.[24] reported that they could classify 1,169 people with 90% accuracy using 50 data points obtained from 3D head data. Therefore, if we use a large number of pressure sensors, we may be able to classify nearly 1,000 people. The number of sensors can be increased because there is enough space between the pressure sensors in the prototype device. To find effective sensor positions, it is necessary to increase and verify the data.

5.4 Comparison with common authentication methods

An authentication method based on individual differences in the head[11] reported an EER of 6.9%. The average EER of our method was 0.076 (7.6%), which is roughly equivalent to the accuracy of the previous method. In the previous method, they played white noise from a bone conduction speaker attached to the side of the head, received signals using a microphone, and identified the subjects based on their characteristics. However, the helmet may be used in noisy environments such as construction sites, so this authentication method may be affected by noise. On the other hand, since our method is based on the shape of the head, it is not susceptible to noise from sound. A fingerprint authentication method using geometric features[25] reported an EER of 0.8%. It can be seen that our method is inferior to fingerprint authentication in terms of accuracy and robustness. An authentication method based on the features of three-dimensional shapes is difficult to break through by replication, but the reproducibility of the data is low.

5.5 Determination of the threshold

In an actual environment, the data of multiple users should be obtained in advance at the development stage. Then, the threshold value at which the EER is obtained can be calculated when the user's data is registered multiple times. However, the threshold value in a real environment should be determined based on the purpose of its use, just like any other biometric authentication. In the "User authenticate when riding motorcycle" example, vehicle theft needs to be firmly prevented. In this case, the FAR needs to

be reduced, so the threshold should be determined to be small.

6. 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 seconds 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] Attewell, R., Glase, K. and McFadden, M.: Bicycle helmet efficacy: a meta-analysis, *Accident Analysis & Prevention*, Vol. 33, No. 3, pp. 345–352 (2001).

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

[3] Gehlot, A., Kuchhal, P., Singh, A. and Singh, R.: Development and Analysis of FSR and RFID Based Authentication System, *Proceeding of International Conference on Intelligent Communication, Control and Devices*, pp. 1145–1151 (2017).

[4] Chen, Y., Sun, J., Jin, X., Li, T., Zhang, R. and Zhang, Y.: Your face your heart: Secure mobile face authentication with photoplethysmograms, *IEEE INFOCOM 2017*, pp. 1–9 (2017).

[5] Ajay Siddharth, J., Hari Prabha, A. P., Srinivasan, T. J. and Lalithamani, N.: Palm Print and Palm Vein Biometric Authentication System, *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, pp. 539–545 (2017).

[6] Sayo, A., Kajikawa, Y. and Muneyasu, M.: Biometrics authentication method using lip motion in utterance, *ICICSP 2011*, pp. 1–5 (2011).

[7] Kim, D. and Hong, K.: Multimodal biometric authentication using teeth image and voice in mobile environment, *IEEE Transactions on Consumer Electronics*, Vol. 54, No. 4, pp. 1790–1797 (2008).

[8] Bednarik, R., Kinnunen, T., Mihaila, A. and Fränti, P.: Eye-Movements as a Biometric, *Image Analysis*, pp. 780–789 (2005).

[9] Barros Barbosa, I., Theoharis, T. and Abdallah, A. E.: On the use of fingernail images as transient biometric identifiers, *Machine Vision and Applications*, Vol. 27, No. 1, pp. 65–76 (2016).

[10] Nogueira, R. F., de Alencar Lotufo, R. and Campos Machado, R.: Fingerprint Liveness Detection Using Convolutional Neural Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 6, pp. 1206–1213 (2016).

[11] Schneegass, S., Oualil, Y. and Bulling, A.: SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull, *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, p. 1379–1384 (2016).

[12] Dai, H., Wang, W., Liu, A. X., Ling, K. and Sun, J.: Speech Based Human Authentication on Smartphones, *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9 (2019).

[13] Jian, M. and Yongmei, L.: An embedded voiceprint recognition system based on GMM, *2015 10th International Conference on Computer Science Education (ICCSE)*, pp. 38–41 (2015).

[14] Zhang, J.: The Algorithm of Voiceprint Recognition Model based DNN-RELIANCE, *2020 International Conference on Computer Engineering and Application (ICCEA)*, pp. 250–253 (2020).

[15] Izuta, R., Murao, K., Terada, T., Iso, T., Inamura, H. and Tsukamoto, M.: Screen Unlocking Method using Behavioral Characteristics when Taking Mobile Phone from Pocket, *MoMM 2016*, pp. 110–114 (2016).

[16] Guerra-Casanova, J., Sánchez-Ávila, C., Bailador, G. and de Santos Sierra, A.: Authentication in mobile devices through hand gesture recognition, *International Journal of Information Security*, Vol. 11, No. 2, pp. 65–83 (2012).

[17] Chen, R., She, M., Wang, J., Sun, X. and Kong, L.: Driver verification based on handgrip recognition on steering wheel, *2011 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 1645–1651 (2011).

[18] Chen, R., She, M. F., Sun, X., Kong, L. and Wu, Y.: Driver Recognition Based on Dynamic Handgrip Pattern on Steeling Wheel, *2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp. 107–112 (2011).

[19] Iso, T. and Horikoshi, T.: Statistical approaches for personal feature extraction from pressure array sensors, *2013 5th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, pp. 129–132 (2013).

[20] Murao, K., Tobise, H., Terada, T., Iso, T., Tsukamoto, M. and Horikoshi, T.: Mobile Phone User Authentication with Grip Gestures Using Pressure Sensors, *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*, p. 143–146 (2014).

[21] Carter, K. A., Brewer, K. L. and Garrison, H. G.: Awareness of the Bicycle Helmet Law in North Carolina, *North Carolina Medical Journal*, Vol. 68, No. 4, pp. 225–230 (2007).

[22] Rousseeuw, P. and Driessen, K. V.: A Fast Algorithm for the Minimum Covariance Determinant Estimator, *Technometrics*, Vol. 41, No. 3, pp. 212–223 (1999).

[23] Arakawa, T., Koshinaka, T., Yano, S., Irisawa, H., Miyahara, R. and Imaoka, H.: Fast and Accurate Personal Authentication using Ear Acoustics, *APSIPA 2016*, pp. 1–4 (2016).

[24] Zhuang, Z., Shu, C., Xi, P., Bergman, M. and Joseph, M.: Head-and-face shape variations of U.S. civilian workers, *Applied Ergonomics*, Vol. 44, No. 5, pp. 775–784 (2013).

[25] Shreyas, K. K. M., Rajeev, S., Panetta, K. and Agaian, S. S.: Fingerprint authentication using geometric features, *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–7 (2017).