Personal identification method 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 widely used in social life. In this study, a helmet equipped with 32 pressure sensors was used to identify individuals based on their head shape. We propose a method to distinguish between the two. The proposed method can be used to display the name on a display mounted on top of the helmet, or to label the operator to eye tracking data. It can also be used as a door key in factories when access to the room is restricted by job title or other reasons. The proposed method has two mechanisms: personal identification, which identifies a person when registered he or she wears a helmet, and identity authentication, which authenticates the person wearing the helmet if he or she is a registrant and rejects it if he or she is not. After implementing a prototype device and software for analysis, we collected data from 9 subjects and obtained an accuracy of 100% for personal identification and an average EER of all subjects of about 7.6% for identity authentication.

CCS CONCEPTS

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

KEYWORDS

datasets, neural networks, gaze detection, text tagging

ACM Reference Format:
Atsuhiro Fujii and Kazuya Murao. 2018. Personal identification method using a helmet with pressure sensors. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Helmets are used in sports, leisure, motorcycle riding, factory, disaster site, etc. It is widely used. These are all worn to protect the head in the event of an accident[2]. It is considered important from a safety point of view that there is no gap between the head and the helmet.

Almost all workers in factories and disaster sites wear helmets. In addition, various people who do not know each other, such as short-term workers and vendors, come and go. If each person has one helmet, a tape with his or her name on the helmet allows the helmet wearer to be identified from a distance or overhead. If you own one helmet per person, tape your name on the helmet. This makes it possible to distinguish between them from a distance or overhead, even while wearing a helmet. Since the qualifications and the work to be engaged in vary from one worker to another, it is necessary to indicate the qualifications held by the worker. A sticker wrote the qualifications is available for sale and can be affixed to the helmet of such a worker so that he or she can be identified. However, in the case of a loaned helmet, the helmet is not marked with the name. No one can determine who it is, and a suspicious person could easily get in. Even if your name is displayed, the name on the helmet may be wrong.

In this study, we propose a method for identifying individuals from the shape of their heads by mounting pressure sensors inside a helmet. The proposed method allows names and credentials to be displayed on a display attached to the top of the helmet. Therefore, they can recognize each other even if they share helmets, and they cannot be mistaken for each other. In addition, the data from cameras, eye tracking devices and various sensors attached to the helmet can be automatically the operator labeled. Furthermore, by attaching a GPS module and an antenna[11], the name and location of the worker can be determined in real time. If the information can be transmitted, it will be easier to understand the overall situation in the field. Furthermore, information on the gap and pressure between helmet and head can be obtained by acquiring the head shape, and it is possible to check whether the shape of the head matches that of the helmet.

In addition, the proposed helmet can be used as a key for the door of a factory or other facility where access to the room is restricted due to position or qualification. It can also be used as a key for a motorcycle. Using the helmet for identification, which reduces the risk of key theft and vehicle theft.

There are several methods to identify individuals: passwords, PINs, and stroke patterns; and physical characteristics such as face, fingerprints, handwriting, voice prints, and glitter; and behavioral characteristics such as handwriting and gait. Using only passwords, PINs, and stroke patterns that can be freely set by individuals to identify a large number of people has a risk of spoofing by brute force attacks and password duplication.

For physical characteristics, Chen et al.[4] propose a method to authenticate using the user's face and fingertips video images captured from the front and rear cameras of a mobile device. We thought to be able to identify the wearer using a camera pre-mounted on the outside of the helmet. However, the recognition accuracy may be reduced in dark places and in rainy weather. Also, it is troublesome to take a picture of one's own face before wearing

Woodstock '18, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

the helmet each time. In fingerprint authentication[13], there is a risk that fingerprints can be easily duplicated from photographs. The head shape used in this study has physical characteristics for each individual. In addition, it is difficult to replicate because of its three-dimensional shape.

In the case of using a behavioral characteristics, it may be possible to authenticate from the action of wearing a helmet. The authors proposed a method that is authenticate a smartphone from acceleration sensor data when taking it out of the pocket in the past[8]. Although the number of occasions to take a smartphone is limited, such as in a pocket or on a desk, the number of occasions to take a helmet is varied, so it is considered difficult to apply this method to a helmet.

In the following sections, we will introduce the related studies in Section 2, explain the proposed method in Section 3, evaluate the proposed method with a discussion of the experiments and results in Section 4, and we conclude this study in Section 5.

2 RELATED WORK

In this section, we introduce research on personal identification, wareable devices, and head state recognition.

2.1 Personal Authentication Method

Bednarik et al.[3] proposed a biometric identification system that uses eye movements such as pupil size and variation, gaze velocity, and distance of the infrared reflection of the eye. Chen et al.[4] propose a method for authentication based on the consistency of two photopletismograms extracted from video images of the face and fingertips captured simultaneously by the front and rear cameras of a mobile device. Siddharth et al.[1] proposed a biometric 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 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.[9] proposed an authentication method that combines dental images and voice.

For such a camera-based approach, if the camera is mounted 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. If it can be attached a camera to the side of the helmet's head, and grasping it when wearing the helmet, it is possible implement of palm print and palm vein authentication. However, this method also requires the user to hold the camera each time it is worn. In the case of a full-face 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 helmet is limited, and it is difficult to distinguish the shape and movement of around the mouth with a single camera. In addition, there is the hassle and economic problem of mounting a camera on every helmet. In addition, it is not practical, as it has to be considered using in the dark and submerging in water due to bad weather.

Guerra-Casanova et al.[5] proposed a method to authenticate users by gestures of their hands using a mobile device with an embedded accelerometer.

In the case of gesture 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 that we take data and learn from all the people who might wear it in different situations.

Nogueira et al.[13] used convolutional neural networks (CNN) for fingerprint authentication, and achieved a high classification accuracy. However, there is a risk that fingerprints can be easily duplicated from photographs.

2.2 Body Part Mounted Devices

Ham et al.[6] proposed a wristband device as an input device for smart glasses. This device has a touch screen panel (TSP) and inertial measurement unit (IMU), and it is manipulated by touching and the twisting of your wrist. Since the device can be worn on the wrist, the user is not restricted in his or her movements and has a high degree of freedom of movement. In addition, a touch panel is used for pointing to improve the stability of input. Hernandez et al.[7] proposed a method for recognizing pulse and respiration rates from accelerometers, gyroscopes, and cameras embedded in Google Glass, a head-worn wearable device. Nishajith et al.[12] designed and implemented a head-worn wearable device which is named smart cap for assist visually impaired people with situational awareness. This devices are consists of Raspberry Pi 3, Raspberry Pi NoIR Camera V2, and an earpiece and power supply. Raspberry Pi NoIR (No Infrared) Camera V2 is an infrared camera module for Raspberry Pi. An audio description of the object detected in the image obtained from this infrared camera is given through the earpiece.

These are all studies on wearable devices worn on body parts, and the shape of device is varied. Head-worn wearable devices such as cap and eyeglass exist, but there are no studies using helmets to the best of our knowledge.

2.3 Head State Recognition

Electroencephalogram (EEG) headsets are used to measure brain waves. However, since the measurement is performed by placing electrodes on the scalp, the muscle signals are detected locally. Although it is often removed as noise, Toth et al.[19] focused on this muscle signal, and six different facial expressions were classified using the muscle signals and the gyroscope values which were got from a cheap Electroencephalogram (EEG) headset. It uses of only existing EEG devices for classification of facial expressions. Then we don't need addition EMG sensor, and can build more hybrid brain-computer interface (BCI) system. Kwon et al.[10] designed a spectacle-type wearable device which is used to detect the user's emotions based on facial expressions and physiological reactions. The designed device can capture facial expressions with a built-in camera. In addition, it can obtain physiological responses such as

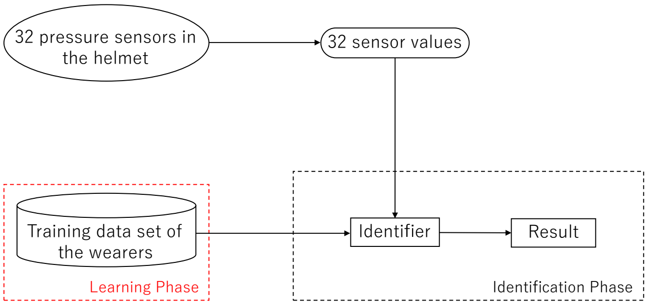

Figure 1: Structure of the Personal Identification System

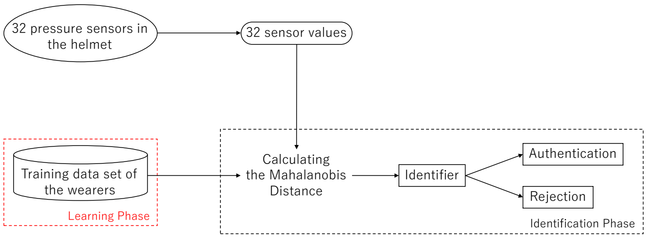
32 pressure sensors in the helmet
32 sensor values
Training data set of the wearers
Learning Phase
Calculating the Mahalanobis Distance
Identifier
Authentication
Rejection
Identification Phase

Figure 2: Structure of the Identity Authentication System

photopletis mogram (PPG) and electrodermal activity (EDA). These are used to detect the user's emotions.

These researches acquire dynamic information such as facial expressions and physical responses in the face area. On the other hand, our research differs from them in that it obtains static features of the head shape.

In this paper, we propose a method to identify individuals by acquiring their head shape by wearing a helmet with a pressure sensor in the interior. This method does not require any special behavior for personal identification, and you are not limited movement by the device. In addition, it is necessary to know the exact three-dimensional shape of the head in order to replicate the head shape, and that makes difficult to replicate the head shape.

3 PROPOSED METHOD

This section describes the details of the proposed method.

3.1 Overview

In the proposed method, the user wears a helmet equipped with a pressure sensor and acquires the shape of his or her head. It identifies the wearer is pre-registered person or not. In this study, two usage environments are assumed. As shown in **Figure 1**, the first is an environment in which multiple persons are registered and when one of the registered persons wears a helmet, the system recognizes who has worn it. As shown in **Figure 2**, the second environment has one or more persons registered in it. When a person including a non-registered wears a helmet, he or she who is a registered person is authenticated. On the other hand, he or she who is non-registerd person is rejected. The former environment is called personal classification and the latter environment is called identity authentication.

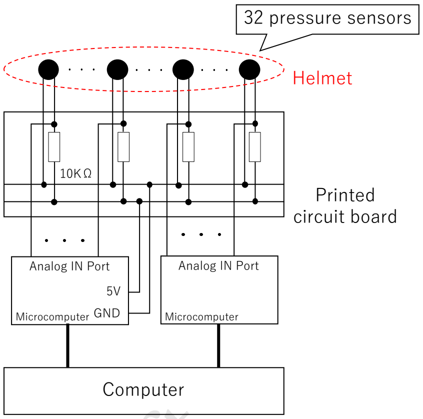

Figure 3: Structure of the device

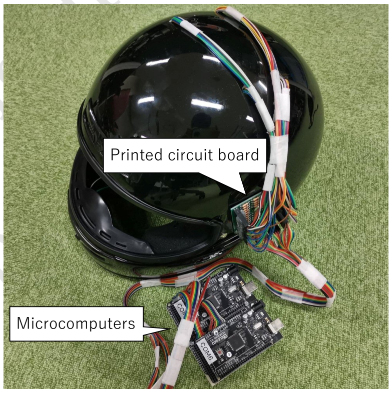

Figure 4: Appearance of the device

The inner side of the helmet contains 32 pressure sensors to acquire data in 32 dimensions. The proposed system provides helmets to people who are expected to wear helmets at work in advance. We ask the user to wear a helmet and collect pressure sensor data as training data. In individual identification, all users are asked to wear a helmet several times and collected 32 dimensions pressure sensor data as training data. Then, the system uses the Support Vector Machine (SVM) to build a recognition model from the training data. This model is used to obtain identification results from the features of the input data of an unknown registrant in the identification phase. On the other hand, in identity authentication, the user is asked to wear a helmet several times and collected 32 dimensions pressure sensor data as training data. Then, Mahalanobis' Distance between the training data and the input data of the person including non-registrants is calculated in the identification phase. If this distance is less than or equal to the threshold, the user is authenticated.

3.2 Hardware

We implemented a helmet equipped with a pressure sensor used in the proposed method. **Figure 3** shows the configuration of the device and **Figure 4** shows the appearance of the device.

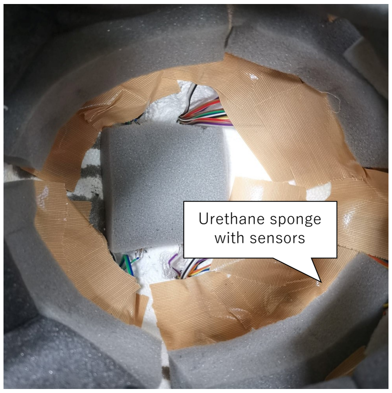

Figure 5: Inside of the device

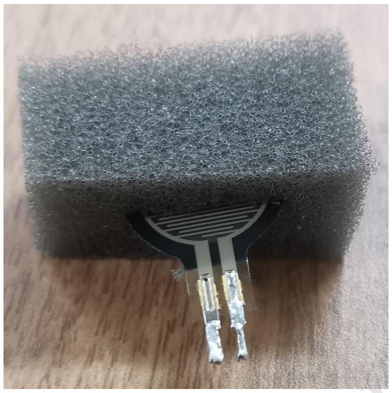

Figure 6: Mounting Method for Pressure Sensors

The head of the helmet wearer must be in close contact with the sensor to obtain the correct pressure value. Therefore, a full-face helmet (BB100 manufactured by B&B) with high adhesion was used. The pressure sensors were FSR402 and FSR402 ShortTail manufactured by Interlink Electronics, Inc. The Arduino MEGA2560 R3 was used as a microcomputer. The helmets used were free size, and it was difficult to attach and remove the interior. Therefore, we removed the interior of the top of the head and installed a thick urethane sponge as shown in **Figure 5**. In addition, a cut was made in the center of the urethane sponge and a pressure sensor was inserted as shown in **Figure 6**. There are 4 pressure sensors at the top of the head, 16 around the top of the head, 6 at the back of the head, and 6 at the cheek pads on both sides. A total of 32 units were installed. The wiring for the pressure sensor goes 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 Arduino MEGA2560 R3 via a printed circuit board with a 10KΩ resistor which is mounted outside the helmet. The printed circuit board attached to the outside of the helmet is shown in **Figure 7**. The printed circuit board is bolted to the left cheek area using a threaded hole drilled for securing the helmet shield. It is fixed and removable.

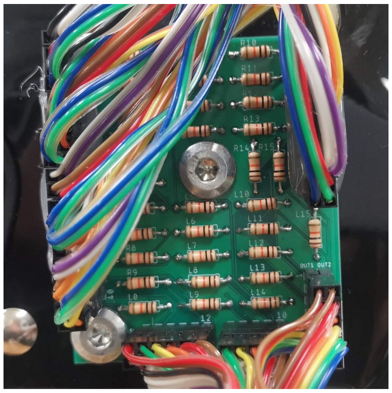

Figure 7: A printed circuit board connected to 32 pressure sensors

3.3 Personal Identification Method

In an environment which multiple persons are registered in the system and a helmet-wearing person is identified among them, we use the Support Vector Machine (SVM) which is a machine learning algorithm. The SVM is a pattern recognition model using supervised learning that can be applied to classification and regression. In the proposed method, the SVM is trained by the data with the registrant labels in advance. The data of one of the registrants is then entered, and it identifies whom the data is.

The data acquisition starts when the user puts on the helmet. The voltage values of all the pressure sensors are almost 5V without a helmet. The voltage of the pressure sensors decreases when the helmet is worn. 32 pressure sensors data $p(t) = [p_{0,t}, \ldots, p_{31,t}]$ are acquired for 2 seconds from the time $t = T_s$[s] when the values are stable. The average value $x(t) = \frac{1}{N}\sum_{t=T_S}^{T_S+N-1} p(t)$ of N samples of data obtained in 2 seconds per dimension from this 32-dimensional data is calculation. We then obtain a single 32-dimensional vector as a feature. We collect training data $[\boldsymbol{x}_i, y_i]$ $(i = 1, \ldots, m)$ by wearing a helmet m times in advance and train the SVM. y is the registrant label (such as the registrant's name and number). Then, the input data $\boldsymbol{x}$ of the user to be identified is entered into the SVM and the identification result $\hat{y}$ is obtained. In this propose method, we used linear SVM.

3.4 Identity Authentication Method

3.4.1 Calculation of distance from registered data. In an identity authentication environment, one or more users are registered in the system. When a registered person wears a helmet, he or she is authenticated. On the other hand, if an unregistered person wears a helmet, he or she is rejected as a stranger. The proposed method uses the Mahalanobis distance as a method to calculate the distance between the training data of the user and the input data of the unknown wearer. The Mahalanobis distance is one of the methods for calculating the distance between multiple variables, and it can be normalized considering the distribution of the data.

As in the case of individual identification, we obtain the pressure sensors data $p(t) = [p_{0,t}, \ldots, p_{31,t}]$ for 2 seconds from time $t = T_s$[s] when the voltage of the pressure sensors decreases and the value is stable after wearing a helmet. The average value $x(t) = \frac{1}{N}\sum_{t=T_S}^{T_S+N-1} p(t)$ of N samples of data obtained in 2 seconds per dimension from this 32-dimensional data is calculation. We then obtain a single 32-dimensional vector as a feature.

We collect training data $[\boldsymbol{x}_i, y_i]$ $(i = 1, \ldots, m)$ by wearing a helmet m times in advance. y is the registrant label (such as the registrant's name and number). The mean vector $\boldsymbol{\mu}$ and the variance-covariance matrix Σ of the training data are calculated by Equations 1 and 2.

$$\boldsymbol{\mu} = \frac{1}{m}\sum_{i=1}^{m} \boldsymbol{x}_i \qquad (1)$$

$$\Sigma = \frac{1}{m}\sum_{i=1}^{m} (\boldsymbol{x}_i - \boldsymbol{\mu})(\boldsymbol{x}_i - \boldsymbol{\mu})^T \qquad (2)$$

Let $\boldsymbol{x}$ is the input data of the user to be identified. In this case, if the input data are got from the pre-registered user, the input data $\boldsymbol{x}$ and the training data $\boldsymbol{x}_i$ follows the probability distribution of the same variance-covariance matrix Σ, so the Mahalanobis distance between the input data $\boldsymbol{x}$ and the training data $\boldsymbol{x}_i$ can be defined as Equation 3.

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

3.4.2 Authentication Decision. Let θ is the threshold value, and if Equation 4 is satisfied, the input data $\boldsymbol{x}$ is determined to be got from one of the registered users and the user is authenticated. On the other hand, if Equation 4 is not satisfied, the input data $\boldsymbol{x}$ is determined to be got from non-registered user and the user is rejected. When multiple users are registered, the mean vector $\boldsymbol{\mu}$ and the variance-covariance matrix Σ of each is computed in the same way. It computes the Mahalanobis distance between the input data and each registrant's data set. Then, if Equation 4 is satisfied at least once, it is authenticated, and if it is not satisfied at least once, it is rejected.

$$\theta \geq min_i(d(\boldsymbol{x}, \boldsymbol{x}_i)) \ (i = 1, \ldots, m) \qquad (4)$$

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 individual identification environment, the system read the csv file of the pre-collected sensor data and train and identify using sklearn.svm.SVC. sklearn.svm.SVC is a scikit-learn[16] library which is implemented the standard soft margin SVM. We also used sklearn.model_selection.cross_val_score which is a library for cross-validation and sklearn.model_selection.GridSearchCV which is a library for grid search, for evaluation.

In the authentication environment, the system read the csv file of the pre-collected sensor data and compute the variance-covariance matrix using sklearn.covariance.MinCovDet. The system compute the Mahalanobis distance of the input data $\boldsymbol{x}$ for all training data $\boldsymbol{x}_i$ from the inverse of the variance-covariance matrix using scipy.spatial.distance. 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

In this section, we describe the experiments we conducted to evaluate the effectiveness of the proposed method.

4.1 Data Collection

We asked 9 subjects (A I, all male, mean age 23 years) to wear helmets implemented in Section 3 and collected sensor data. The sampling rate is approximately 30 Hz. Put it on for 2 seconds to collect data, then remove it and put it back on for 2 seconds to collect data as a set (2 samples). A total of 180 samples (2 seconds×20 samples×9 subjects) were collected from 10 sets on different days. In order to collect data on the various positions of the sensor and head as the helmet was worn, a rest period of at least 30 minutes was provided between sets. A maximum of four sets of data were collected per person per day.

4.2 Personal Identification Method

4.2.1 Evaluation Environment. We evaluated the proposed method by 5-fold cross-validation that 80% (16 samples) of data collected from each subjects were trained and 20% (4 samples) were test data. In order to investigate the effect of the number of sensors used, we performed the trials described above for all combinations of sensors from 1 sensor to 32 sensors.

To simulate a half helmet used at a construction site, we evaluated all combinations of sensors from 1 to 20 sensors in the same way, with only 4 sensors at the top of the head and 16 sensors around the top of the head out of 32 sensors. In this evaluation, we call a full-face helmet when 32 sensors are used and a half helmet when 20 sensors are used.

4.2.2 Results and Discussion. The accuracy of individual identification by full-face helmets is shown in **Table 1**. When the number of sensors is 32, the accuracy is in one way using all 32 sensors, and when the number of sensors is 31, the highest accuracy is recorded among the $_{32}C_{31} = 32$ ways using the 31 sensors out of 32. We evaluated the accuracy with 32 or 31 sensors and found that it was 1.00. Therefore, the number of sensors was increased from one, and the accuracy was evaluated until it reached 1.00.

From the results, we succeeded in identifying 9 people with 100% accuracy when the number of sensors was 5. The accuracy of 99.4% with 4 sensors, 97.2% with 3 sensors, and 92.2% with 2 sensors was high. However, the accuracy dropped significantly to 60% when the number of sensors was one. In this case, the combination of sensors with the highest accuracy for each number of sensors of 5 or less is recorded. Then, the parameters are searched for using the grid search in the combination, and the highest results are shown in **Table 1**.

The accuracy of individual identification by half-face helmets is shown in **Table 2**. We evaluated the accuracy with 20 or 19 sensors and found that it was 1.00. Therefore, the number of sensors was

Table 1: Personal identification accuracy when the number of sensors on a full-face helmet is reduced from 32 to 1

Sensor Number	Accuracy
32	1.000
31	1.000
⋮	⋮
5	1.000
4	0.994
3	0.972
2	0.922
1	0.600

Table 2: Personal identification accuracy when the number of sensors on a half helmet is reduced from 20 to 1

Sensor Number	Accuracy
20	1.000
19	1.000
⋮	⋮
5	1.000
4	0.994
3	0.967
2	0.900
1	0.600

increased from one, and the accuracy was evaluated until it reached 1.00 as well as the environment in a full-face helmet.

From the results, we succeeded in identifying 9 people with 100% accuracy when the number of sensors was 5. The accuracy of 99.4% with 4 sensors, 96.7% with 3 sensors, and 90.0% with 2 sensors was high. However, the accuracy dropped significantly to 60% when the number of sensors was one. In this case, the combination of sensors with the highest accuracy for each number of sensors of 5 or less is recorded. Then, the parameters are searched for using the grid search in the combination, and the highest results are shown in **Table 2**.

Both of the full-face helmet and the half-helmet used 5 sensors for 100% accuracy from the data set used in this experiment. However, the number of sensors required to achieve high accuracy may more increases as the number of registrants increases.

4.3 Identity Authentication Method

4.3.1 Evaluation Environment. Of the data collected, one subject was considered to be the individual and the remaining eight subjects were considered to be strangers. 80%(16 samples) of the individual data were registered as training data, and the remaining 20%(4 samples) data were used as test data. The authentication accuracy of the person was measured by 5-fold cross-validation. In addition, we measured the authentication accuracy of others' using data from all eight strangers(160 samples) for the five patterns of training data used in cross-validation. All nine subjects were evaluated on a rotation basis.

Table 3: EER of each subject and the average EER of all subjects in the identity authentification

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
Total	0.076

FRR, FAR, and EER are used as evaluation indicators of authentication accuracy. FRR(False Reject Rate) is the rate at which a registered person is mistakenly considered to be a stranger and rejected. FAR (False Accept Rate) is the rate at which a stranger is mistakenly considered to be a registered person and authenticated. The smaller the threshold value is set, the stricter the authentication decision becomes. Then FRR increases. On the other hand, the larger the threshold value is set, the looser the authentication decision becomes. Then FAR increases. 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 authentification methods, and the smaller EER, the better the performance.

4.3.2 Results and Discussion. EER of each subject is shown in **Table 3**. FRR and FAR of each subject with varying thresholds are shown in **Figure 8**. "Total" indicates the mean of all subjects. **Table 3** shows that EER of subjects A, E, G, and I was roughly less than 0.01, which is a good result. This means that in the dataset used for evaluation, the individual fails to authenticate less than once in 100 times, and the strangers break through the authentication less than once in 100 times. EER of 0.012 for face authentification was reported in reference [18]. Therefore, comparable performance was achieved in these subjects. **Figure 8** shows that for subject E, FRR and FAR crossed at a threshold of about 60, which is greater than the other subjects. This is because there were outliers in the collected pressure data samples, and it was necessary to increase the threshold value to authenticate the outliers correctly.

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, all collected data were compressed to the first principal component and the second principal component by principal component analysis. The results of this data plotted on a two-dimensional plane are shown in **Figure 9**. Looking at subject C's data in **Figure 9**, one sample of subject C's data group is in close proximity to subject I's data group, but there is no overlap with the other subjects' data groups. However, the dispersion in the first principal component direction is large. On the other hand, the data groups of subjects D and H overlapped each other significantly, which may affected the accuracy of the both subjects.

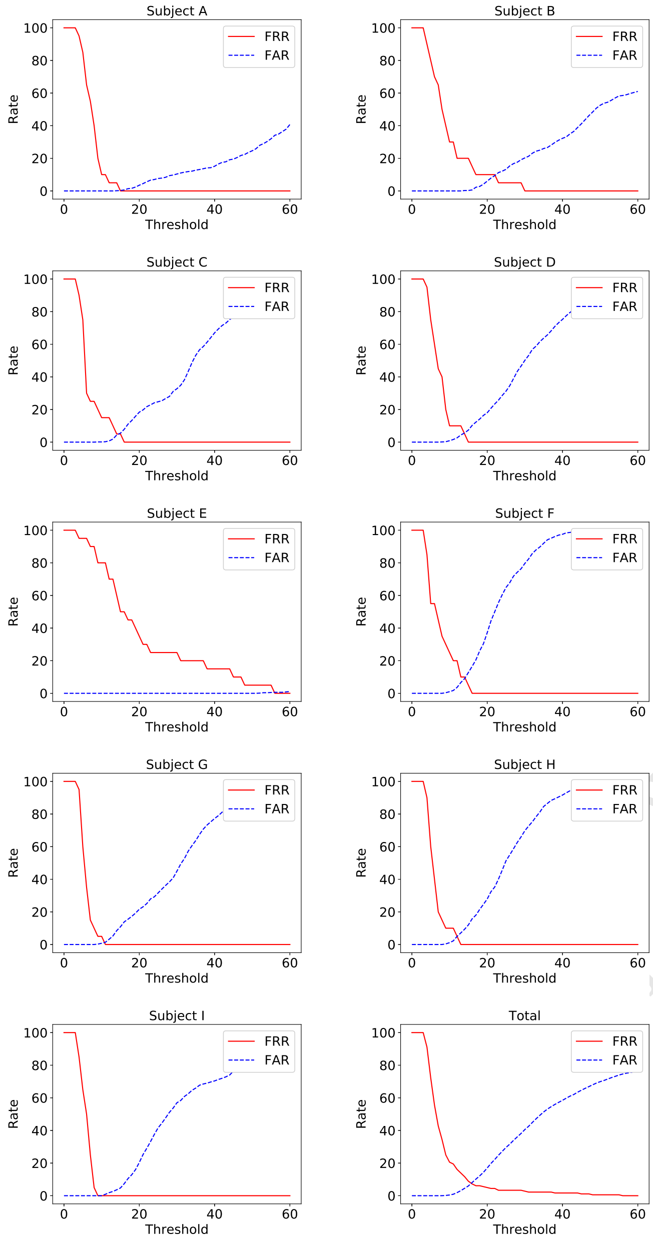

Figure 8: FRR and FAR

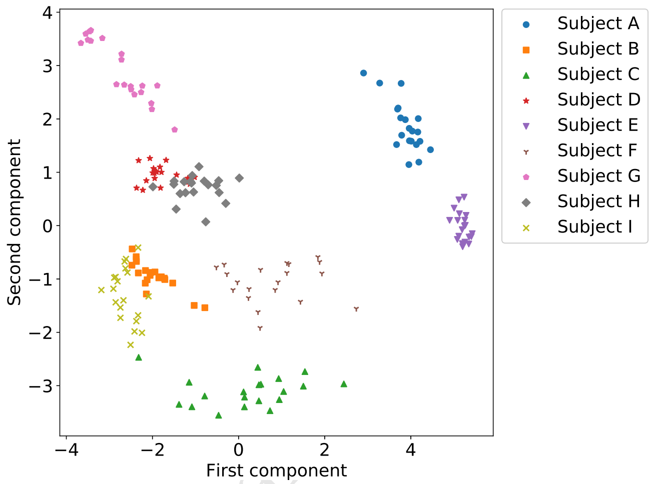

Figure 9: Principal component distribution of 32-dimensional features compressed into two dimensions by PCA

The least accurate subjects are B and F, with EER of approximately 0.095. Subject B's data group has a small variance, but there is some overlap with subject I's data group. However, subject I's EER in the dataset used for evaluation was 0. This means that it was authenticated without error. 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 group does not show any overlap with the other subjects' data groups, but there is a large variance to both directions for the first and second principal components. Considering the effect of data compression by principal component analysis, 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.

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. The proposed method uses the distance between the training data and the input data for authentication, so that the accuracy is expected to be improved by increasing the number of training data. In addition, we will also examine a method for authentication using time series pressure data during helmet wearing operation.

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 inside. Then, we implemented the prototype device and evaluated the proposed method. The prototype device is a commercial full-face helmet with a pressure sensor attached. In the evaluation, we created a data collection program to acquire data from the prototype device and obtained the sensor value for 2 seconds 20 times from all 9 subjects as head shape data. Using the acquired data, we evaluated the accuracy of individual identification to determine who is wearing the helmet among the registrants and the accuracy of identity authentication to determine whether the helmet wearer is the registrant or not.

Since the accuracy was very high in the individual identification environment in the evaluation experiments, we tested how the discrimination accuracy changed by decreasing the number of sensors used for identification. The results showed that the most efficient number of sensors to identify the data set used in this experiment was five for both full-face and half helmets. EER of 4 out of 9 subjects was less than 0.012, and the average EER was 0.076 in the environment of the authentication. These results suggest that our method is effective as a personal 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] 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

[3] 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.

[4] 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.

[5] 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

[6] Jooyeun Ham, Jonggi Hong, Youngkyoon Jang, Seung Hwan Ko, and Woontack Woo. 2014. Smart Wristband: Touch-and-Motion–Tracking Wearable 3D Input Device for Smart Glasses. In *Distributed, Ambient, and Pervasive Interactions*, Norbert Streitz and Panos Markopoulos (Eds.). Springer International Publishing, Cham, 109–118.

[7] J. Hernandez, Y. Li, J. M. Rehg, and R. W. Picard. 2014. BioGlass: Physiological parameter estimation using a head-mounted wearable device. In *2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*. 55–58.

[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] 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.

[10] 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.

[11] 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.

[12] A. Nishajith, J. Nivedha, S. S. Nair, and J. Mohammed Shaffi. 2018. Smart Cap - Wearable Visual Guidance System for Blind. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*. 275–278.

[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] Qian Tao and Raymond N.J. Veldhuis. 2006. Biometric authentication for a mobile personal device. In *Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services Workshops*. 1–3.

[19] 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.