Validation of EEG Authentication Accuracy with Electrode Slippage

Yu Ishikawa, Kaori Nishibata, Masami Takata, Hiroyasu Kamo and Kazuki Joe
Nara Women's University, Nara, 630-8506, Japan

Abstract - *The Brain-Machine Interface (BMI) researches on device operation using electroencephalogram (EEG) have advanced in various fields. Furthermore, improvement of authentication technology for privacy protection is required with the development of Internet of Things (IoT) technology. Therefore, the biometric authentication using EEG has been devised. Research on EEG authentication has already advanced from various fields, and many effective methods have been proposed. At the time of EEG authentication, it is necessary to apply the electroencephalograph at the appropriate position, but it is difficult and takes a long time to apply it without electrode slippage every time. Thus, to be available on a daily basis, an authentication method that takes electrode slippage into account is necessary. However, existing EEG authentication methods do not take into consideration electrode slippage which is generated at the time of EEG measurement. Therefore, in this paper, we validate authentication accuracy with electrode slippage.*

Keywords: Biometric authentication, EEG, Electrode slippage, AdaBoost

1 Introduction

Interest in the Brain-Machine Interface (BMI) technology has increased not only in the welfare and medical fields but also in various fields in recent years [1]. BMI is a technology that links directly brain and machine. In particular, research and development of non-invasive BMIs using electroencephalogram (EEG) obtained by measuring the electric potential on the scalp have advanced. BMI technology related to device operation using EEG, such as artificial arms operated by EEG [2] and devices operated by sensing human emotions from EEG [3], has improved. Usually, computers are operated by mouses and keyboards. However, it is considered that computer operation using EEG is becoming possible with the development of BMI technologies. In addition, with the development of Internet of Things (IoT) technologies, opportunities to deal with important information have increased on the Internet. Because of that, privacy protection is emphasized, and it is necessary to achieve a system that allows only authorized persons to handle information. Therefore, improvement of the authentication technology for identifying individuals is required [4]. To login to a device, knowledge-based authentication by a password or a security code is used. However, when a computer is operated by EEG, EEG authentication utilizing individual differences of features obtained from EEG is reasonable than the knowledge-based authentication.

Researches on EEG authentication have advanced in various fields, and it has been clarified that EEG present different features depending on individuals. Moreover, since EEG are very complex internal information unlike biometric information such as fingerprints and irises, EEG have the potential to realize biometric authentication with high confidentiality. Various features and classification methods that can be used for EEG authentication have been studied and many effective methods have been proposed [5]. In addition, the development of electroencephalographs is remarkable, and there are various electroencephalographs from expensive and high-precision equipment for medical use to inexpensive equipment for individual use in daily life. For that reason, it is possible to use electroencephalographs selectively in accordance with the situation. In EEG authentication systems, measurement is performed by an electroencephalograph for individuals because it is generally considered that the systems are used in daily life. As the electroencephalographs for individuals, there are many electroencephalographs of head set type and head cap type [6-9]. Since the electroencephalographs do not need to determine the position of each electrode for each subject, they can be used by users who do not have expert knowledge. To acquire accurate EEG by using the electroencephalographs, it is necessary to apply a head set or a head cap at the appropriate position. However, at the time of measurement, it is difficult to properly apply it without electrode slippage every time. Furthermore, if the application position is wrong, it is considered that slippage will occur in measurement position of all electrodes and the EEG obtained from each electrode is influenced. Therefore, we aim to construct a system that can authenticate even if there is some slippage in measurement position, and in this paper, we validate the influence of authentication accuracy due to electrode slippage.

The rest of the paper is organized as follows: Section 2 describes EEG and a measurement method. Section 3 reviews the related works about authentication using EEG. Section 4 explains the EEG authentication method using validations in this paper. Section 5 validates the influence of authentication

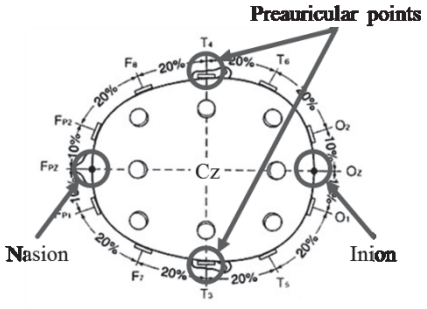

Fig 1 Method of determining electrode positions by International 10-20 system

accuracy due to electrode slippage using the method in Section 4. Section 6 concludes by discussing future work.

2 EEG Measurement

EEG [10] is the electrical activity of numerous neurons in a cerebral cortex. The cerebral cortex is composed of cerebral sulci and gyri complicatedly. For that reason, the potential generated from the cerebral cortex propagates not only the scalp just above it but also through the skull and the scalp in various directions. The EEG generated in the cerebral gyri becomes the maximum potential at the position of the scalp just above it. On the other hand, since the EEG generated in the cerebral sulci cannot be measured at the scalp just above it, the EEG is detected on the scalp which forms a solid angle from the cerebral sulci. Thus, it is considered that the electrode slippage greatly affects the obtained EEG. Because of the spread of BMI, many electroencephalographs that can be used easily are developed. However, to properly record EEG, sufficient preparation and knowledge is necessary. When performing EEG measurement, it is necessary to determine all electrode positions. The electrode placement is usually based on the International 10-20 system [11]. The international 10-20 system is an electrode placement method which is regarded as the world standard, and it is adopted in various electroencephalographs. As the procedure, first, a central (Cz) electrode to be the reference position is derived from the midpoint between the nasion and the inion and the midpoint between the preauricular points of the left and right of a subject. Next, the interval between the nasion and the inion and the interval between the preauricular points of the left and right are divided into 10% ,20%, 20%, 20%, 20%, and 10%. In that way, the total of 21 electrode positions are determined. Fig 1 shows the division method by the International 10-20 system. By determining all electrode positions according to the procedures, it is possible to place the electrodes at constant intervals regardless of head sizes.

The commercially available electroencephalographs that can be used in daily life include MindWave [6], EMOTIV [7], ENOBIO [8] and BioSemi [9], and so on. Many electroencephalographs are a head set type or a head cap type, and are designed to be easily applied on the head. Among them, the head set type electroencephalographs are MindWave and EMOTIV, which are common in electroencephalographs with

Fig 2 Head set type (EMOTIVE) and head cap type (ENOBIO) electroencephalographs

a small number of mounting electrodes. The head set type is electroencephalographs in which electrodes are fixed in advance to the head set. On the other hand, ENOBIO and BioSemi are head cap type electroencephalographs, and they are common in multichannel electroencephalographs. The head cap type is an electroencephalograph in which electrodes are placed by users on the head cap to which all electrode positions are indicated. As an example, Fig 2 shows EMOTIV of a head set type and ENOBIO of a head cap type electroencephalographs. The electroencephalographs adopt the international 10-20 system, and are designed to specification that all electrodes are easily placed using a head set, a head cap and the like. Therefore, the time cost of accurately measuring and dividing the head circumference can be shortened, and even an electroencephalograph having a large number of mounting electrodes can be applied in a short time. Both types of electroencephalographs can determine the relative electrode positions. However, to obtain accurate EEG, the procedure for deriving the accurate reference position cannot be omitted. When the reference position is slipped, a relative slippage occurs in all electrode positions. Moreover, when considering application of the electroencephalograph at the time of EEG authentication, it is desired that the user himself applies the electroencephalograph. At that time, it is difficult to apply it to the correct position while visually checking the reference position, so there is a high possibility that the electrode slippage occurs. Furthermore, since many electroencephalographs measure in a state where electrodes are in contact with the scalp, there is a possibility that the electrode slippage occurs due to the body movement of the user under measurement. From the above, it is impossible to measure without electrode slippage every time during authentication. Therefore, an EEG authentication system that can be authenticated at the time of electrode slippage is required.

3 Related work on EEG authentication

First, existing EEG authentication methods are described. EEG authentication, like general biometric authentication, consists of a registration phase for registering biometric information of users who use the authentication system and an authentication phase for determining whether or not the input data is a user registered in the authentication system. The important process is the determination of biometric information to be registered. In EEG authentication, the waveform of EEG itself is rarely registered as information. Instead, the necessary features are acquired from the EEG and are used as personal biometric information. Various methods

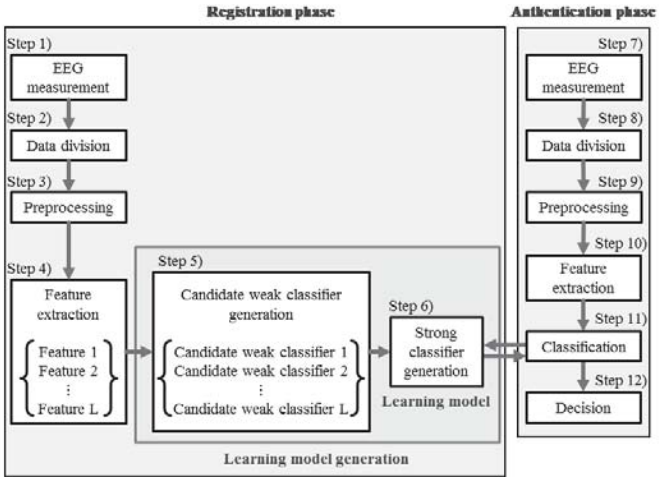

Fig 3 Authentication system flow

have been studied for extracting features [5]. Many methods using spectrum information, correlation information, autoregressive (AR) coefficients, etc. are proposed as feature extraction methods.

In the existing methods, there are researches that attempt to improve authentication accuracy by performing authentication using the multiple features. The first is the research by Riera et al. in 2008 [12]. Features used for authentication are five types: AR model, spectrum information, coherence, mutual information, and cross correlation coefficient. All of the features are regarded as features that identify individuals, and are classified using discriminant analysis (DA). It is reported that EER 3.5-5.5% and classification rate 97.5-98.1% are obtained from the EEG of 51 registrants and 36 intruders during rest. The second is the research by Safont et al. in 2012 [13], and like the Riera et al., multiple features obtained from EEG at rest are used. Features to be used are AR model, spectrum information, cross correlation coefficient, mutual information, coherence, skewness and kurtosis, independent component analysis, autocovariance, time reversal, and so on. The multiple features are classified using DA, classification trees, and a simple copula-based classifier. As a result of the authentication, EER 2.4% and classification rate 93.8 % are obtained from EEG of 50 registrants and 20 intruders. In this paper, similarly to the researches, we perform the validation using a system [14] which improves authentication accuracy by combining multiple features. The details of the authentication method are described in Section IV.

Next, a method of acquiring EEG data by using existing researches is described. In existing researches, mainly continuous data is divided into multiple pieces, and the divided data are handled separately as data to be used for registration and authentication [4]. When that method is used, changes in temporal and spatial EEG are not considered. In other words, the existing method has the following problems. First, since data on the same day are used, changes in EEG over time cannot be obtained. Furthermore, since data are continuously measured without removing the electroencephalograph applied to the subject, spatial changes (slippage) which can occur when the electroencephalograph is applied cannot be obtained. There is the existing research that validates temporal changes. It is reported by Marcel et al. in 2007 [15], and they perform EEG authentication at the tasks over multiple days. In the authentication results, EEG of the data obtained on the same day as the registration data is 7.1%, but EER of the data obtained on different days is 34.9-36.2%. In that way, it is shown that temporal changes have a large influence on EEG authentication. However, there is no research report on spatial changes, and the influence of electrode slippage on EEG authentication has not been validated. Therefore, in this paper, we validate spatial changes.

4 Authentication method

The authentication system used in this paper is described. The system is proposed in [14] and consists of a registration phase and an authentication phase. The point of the system is improvement of authentication rate by combination of multiple features using ensemble learning and comprehensive determination of results by division of measurement data. The system flow is shown in Fig 3.

In the registration phase, a learning model to be used in the authentication system is generated using data of registrants. First, in step 1), EEG of the registrant at rest is measured for a certain period, and in step 2), the obtained measurement data is divided into multiple data. The obtained data are called divided data. Next, in step 3), preprocessing is performed on each divided data. As the preprocessing, three processes are applied to the divided data: a bandpass filter for obtaining only the necessary frequency bands, removal of biometric information other than EEG and noise caused by environment, and normalization for correcting the difference of each data. Then, in step 4), the features are extracted from each divided data after the preprocessing. In this paper, we use four features that have obtained high authentication accuracy from the results of existing researches: spectrum information, coherence, cross correlation coefficient, and mutual information. The learning model is generated using the four features. Since L value in Fig 3 is the number of features used at ensemble learning, L is 4 in this paper. In the generation of the learning model, in step 5), candidate weak classifiers are generated from the four features obtained in step 4). By learning features using support vector machine (SVM) which is a machine learning with high classification accuracy, the candidate weak classifiers of respective features are generated. Then, in step 6), some of all candidate weak classifiers are combined using AdaBoost which is a type of ensemble learning. By the method, a strong classifier which is a learning model of the authentication system is generated.

In the authentication phase, input data is authenticated using the learning model generated in the registration phase. First, similarly to the registration phase, in step 7), EEG of the user at rest is measured for a certain period, and it is divided

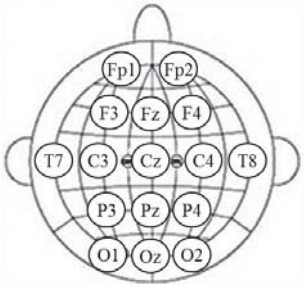

Fig 4 Electrode positions of BioSemi

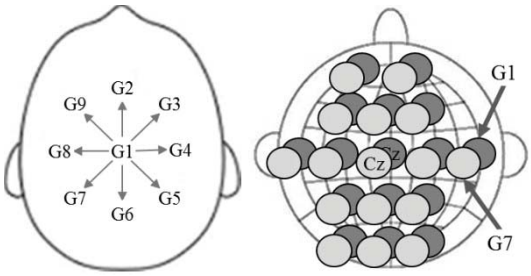

Fig 5 Electrode slippage directions

into multiple data in step 8). After that, preprocessing is applied to each divided data in step 9), and the multiple features are extracted in step 10). Next, in step 11), the learning model generated in the registration phase is applied to the features obtained in step 10). The model classifies the input data as one of registrants because it is not an authentication method but a classification method. The classification is performed by all weak classifiers selected by AdaBoost. By classifying each divided data using all weak classifiers, the probability that each divided data is the valid user is obtained. The probability is the reliability calculated at AdaBoost and is calculated for each divided data. The reliability of the input data is obtained by taking the average of the reliabilities of all the divided data. In step 12), by comparing the reliability of the input data with the preset threshold value, determination of acceptance or rejection of the user is carried out.

5 Validations

5.1 Validation method

In this paper, we use BioSemi of head cap type for EEG measurement. Fig 4 shows the electrode positions of BioSemi. The sampling frequency is 2048 Hz, and the number of electrodes is 16. Using the electroencephalograph, experimental data assuming electrode slippage at the time of application are generated. The data when the position of Cz electrode, which is regarded as the reference electrode by the International 10-20 system, is moved by 3 cm in eight directions including front, back, left and right and diagonal directions is handled as electrode slippage data at the time of application. The right figure in Fig 5 shows the reference position of the Cz electrode and the directions to move it. The reference position without slippage is G1, and G2-G9 with slippage is defined as shown in the figure. The left figure in Fig 5 is an example of the all electrode positions when G1 is moved in G7 direction. The number of subjects is ten, and a ten-second measurement is performed ten times at each position per subject. The subjects are measured in a sitting state and a relaxing state. To evaluate the authentication accuracy when there is the electrode slippage in measurement data by using the above data, we perform two validations.

Table 1 Data position of Validation 1

Experiment	Registration data position	Authentication data position
1	G1	G1
2	Gi	Gi
3	G1	G2-G9

Authentication accuracy is evaluated from the results of Equal Error Rate (EER) and classification rate. When EEG is calculated, experiments are performed by dividing the ten subjects into seven registrants and three intruders. When classification rate is calculated, experiments are performed using all ten subjects as registrants. 10 cross-validation is used in all experiments and the results are expressed as a percentage of the average value after cross-validation.

5.2 Validation 1

In the Validation 1, three experiments focused on registration data position and authentication data position are performed:

Experiment 1. The case where there is no electrode slippage in the registration data and the authentication data,

Experiment 2. The case where there is electrode slippage in the registration data and the authentication data,

Experiment 3. The case where there is no electrode slippage in the registration data and there is electrode slippage in the authentication data.

Table 1 shows the registration data positions and the authentication data positions of each experiment. First, Experiment 1 confirms authentication accuracy by the same method of acquiring EEG data as the existing researches. Both the registration data position and the authentication data position in Experiment 1 are G1, and there is no electrode slippage. In Experiment 2, authentication accuracy is validated when the registration data and the authentication data are in the same positions and have electrode slippage. By the experiment, it is possible to validate the authentication accuracy in a state where there is no difference between the registration data and the authentication data positions even in the case of electrode slippage. In Experiment 2, validation is performed at eight positions from G2 to G9 ($i = 2, \cdots, 9$ in Table 1). In Experiment 3, G1 without electrode slippage is used as registration data and G2-G9 with electrode slippage is used for authentication data. Usually, data registration is one time, and even when it takes time to apply an electroencephalograph, the burden on the user is small. Therefore, it is possible to carefully

Table 2 EER and classification rate of Validation 1

(%)	EER			Classification rate		
	Experiment			Experiment		
	1	2	3	1	2	3
fft	4.95	2.65	15.41	91.00	91.63	57.75
coh	5.38	2.78	15.49	86.00	91.25	58.63
cc	0.40	0.66	24.48	96.00	98.25	36.38
mi	2.26	0.38	23.72	96.00	98.75	47.13
ada	0.18	0.15	13.30	100.00	98.50	56.88

apply an electroencephalograph to the correct position. However, since data authentication requires measurement every time at the time of authentication, it is desirable to apply electroencephalograph in a short time rather than at the correct position. Experiment 3 confirms the accuracy of authentication performed on the above condition.

The results of Experiment 1-3 are described below. Table 2 shows the EER and the classification rate of Experiment 1-3. The results represent authentication accuracy of four features and AdaBoost combining them. In this paper, we use abbreviations of the features in the graphs and the tables: spectrum information is fft, coherence is coh, cross-correlation coefficient is cc, mutual information is mi, and AdaBoost is ada. First, in Experiment 1, the EER is 0.18% and the classification rate is 100% at AdaBoost. From the results, it can be confirmed that the authentication method used in this paper is effective in existing method of acquiring data. In each feature, the accuracy of the spectrum information and coherence is relatively poor, and the accuracy of the mutual information and the cross-correlation coefficient are good results. In addition, from the results of AdaBoost, it can be confirmed that the best accuracy is obtained by combining four features.

Next, the results of Experiment 2 are shown below. From Table 2, the EER is 0.15% and the classification rate is 98.50% at AdaBoost. Focusing on each feature, Experiment 2 has higher accuracy than Experiment 1 except for cross-correlation coefficient in the EER. Moreover, in the classification rates, Experiment 2 has higher accuracy with all features. The detailed results of the classification rate from G1 to G9 in Experiment 1-2 are shown in Fig 6. The graph shows that the results of G5, G6, G7, G9 are particularly good. Since G5-G7 are positions moved from the reference position G1 to the rear, the influence of noises such as eye movements is small. Perhaps, that is why that high authentication accuracy is obtained at G5-G7. Even at other positions, the classification rates at AdaBoost are 96% or more, and high authentication accuracy is obtained. Thus, if the registration data and the authentication data are at the same positions, it can be confirmed that authentication is possible. However, since there is electrode slippage such as G2, G3, G4, G7 in which accuracy is degraded by using AdaBoost rather than each feature, the method using AdaBoost is not always suitable for electrode slippage.

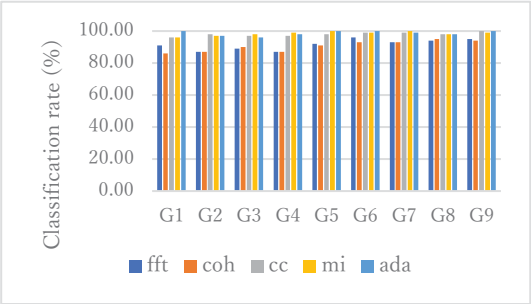

Fig 6 Detailed results of Experiment 1-2

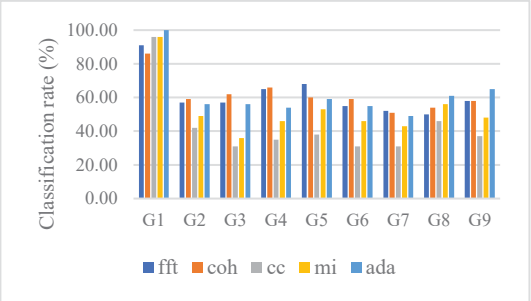

Fig 7 Detailed results of Experiment 3

Next, the results of Experiment 3 are shown below. From Table 2, it is confirmed that the EER is 13.30% and the classification rate is 56.88% at AdaBoost. The detailed results of the classification rate from G2 to G9 in Experiment 3 are shown in Fig 7. The results of G1 are also shown in the graph, which are the same results as Experiment 1. It is clear that the authentication accuracy is lower than that of G1. In the results of Experiment 1-2, it is impossible to confirm a large change in the authentication accuracy depending on the measurement positions, but in Experiment 3 the change with the measurement positions is remarkable. In addition, in G2-G7, the accuracy is lowered by AdaBoost, and the classification rate is reduced by 12% compared with the best feature in G4. That is caused by low classification rates of cross-correlation coefficient and mutual information. The two features do not exceed the classification rate of 50%. Furthermore, the results of cross-correlation coefficient and mutual information are higher in Experiment 1-2 compared with the results of spectrum information and coherence but are lower in Experiment 3. From the result, it is highly likely that cross-correlation coefficient and mutual information capture not only the individual differences but also the features due to the measurement position. Therefore, even if the measurement is performed at the reference position at the time of data registration, if the electrode slippage occurs at the time of authentication, correct authentication becomes impossible. That is because the differences due to electrode slippage are larger than individual differences obtained from EEG. In addition, in Experiment 3, it can be considered that the EEG at the time of electrode slippage cannot be correctly authenticated because the learning model is generated only with G1. Thus, in Validation 2, further validation is performed by adding data at electrode slippage to the learning model.

Table 3 Data position of Validation 2

Experiment	Registration data position	Authentication data position
4	G1-G9	G1-G9
5	Except Gi	Gi
6	G1, G3, G5, G7, G9	G2, G4, G6, G8
	G1, G2, G4, G6, G8	G3, G5, G7, G9

Table 4 EER and classification rate of Validation 2

(%)	EER			Classification rate		
	Experiment			Experiment		
	1	2	3	1	2	3
fft	4.75	9.20	19.98	88.22	79.25	79.38
coh	4.56	8.48	18.92	88.33	79.50	78.00
cc	2.89	10.36	19.34	93.89	69.25	69.25
mi	1.58	9.34	20.08	95.67	74.25	72.50
ada	1.75	2.96	6.94	96.56	83.25	82.00

5.3 Validation 2

In Validation 2, three experiments by changing the registration data to add to the learning model are carried out:

Experiment 4. The case where the registration data include all electrode slippage data,

Experiment 5. The case where the registration data include electrode slippage other data than the authentication data positions,

Experiment 6. The case where the registration data include electrode slippage in four directions.

Table 3 shows the registration data positions and the authentication data positions of each experiment. First, in Experiment 4, the authentication accuracy when all electrode slippage data is used as registration data is validated. Therefore, both the registration data and the authentication data positions are G1-G9. By the experiment, the authentication accuracy when the registration data include data of the same electrode slippage as the authentication data is confirmed. In Experiment 4, only eight types of electrode slippage are validated as examples. However, it is impossible to register all possible electrode slippage during authentication. Therefore, Experiment 5 confirms the authentication accuracy when the electrode slippage that has not been registered occurs by using the electrode slippage data other than the authentication data as the registration data. The authentication data position is eight kinds from G2 to G9. When the authentication data position is G2, the registration data positions are G1 and G3-G9. Finally, Experiment 6 confirms the authentication accuracy when the number of registration data position is reduced as compared with Experiment 5. In Experiment 6, two types of experiments are performed in which the electrode slippage is divided into even numbers (G2, G4, G6, G8) and odd numbers (G3, G5, G7, G9) and each is set as registration data and authentication data positions. G1 is added to the registration data position. Experiment 6a is the case where the registration data position is odd number, and Experiment 6b is the case where the registration data position is even number. By the experiments, the authentication accuracy is validated by giving the learning model the electrode slippage in four directions.

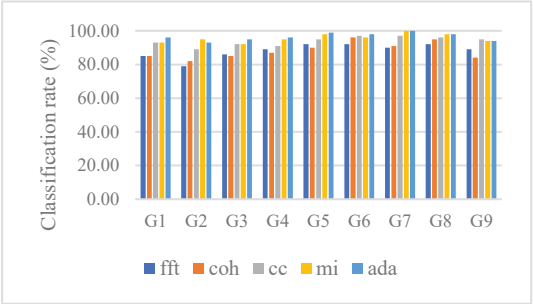

Fig 8 Detailed results of Experiment 4

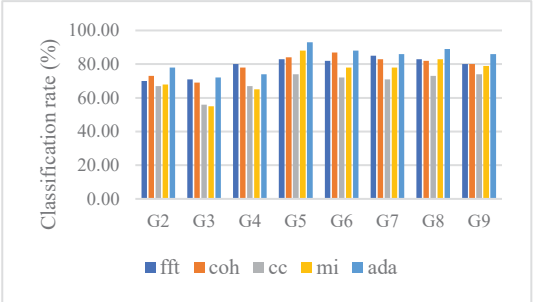

Fig 9 Detailed results of Experiment 5

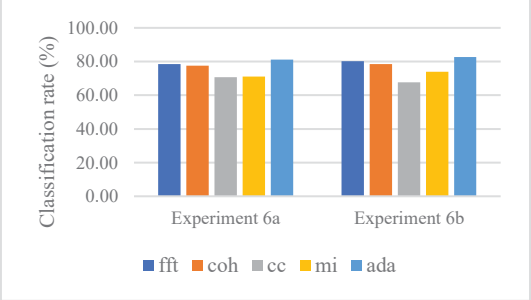

Fig 10 Detailed results of Experiment 6

The results of Experiment 4-6 are described below. Table 4 shows the EER and the classification rate of Experiment 4-6 as in Validation 1. In Experiment 4, the EER is 1.75% and the classification rate is 96.56% at AdaBoost. As compared with Experiment 1, the both results are somewhat worse, but it is clear that when compared with Experiment 3 the accuracy is improve very much. Comparing the results of each feature, as in Experiment 1-2, high authentication accuracy is obtained by mutual information and cross-correlation coefficient rather than spectrum information and coherence. The detailed results of the classification rate from G1 to G9 in Experiment 4 are shown in Fig 8. Overall the authentication accuracy is inferior, but the graph with the same shape as in Fig 6 is confirmed. Registration of electrode slippage other than the authentication data position possibly lower authentication accuracy. However, at the results of AdaBoost, the classification rate of 93% or more is obtained at all measurement positions. Thus, it can be confirmed that the authentication accuracy greatly increases by registering electrode slippage data in advance.

Next, the results of Experiment 5 are described below. From Table 4, the EER is 2.96% and the classification rate is 83.25% at AdaBoost, and the authentication accuracy is lower than that of Experiment 4. However, when comparing authentication accuracy by each feature and AdaBoost, it is clear that the accuracy is highly improved at EER. The detailed results of the classification rate from G2 to G9 in Experiment 5 are shown in Fig 9. Variation in authentication accuracy can be confirmed by measurement positions. There is a tendency similar to Experiment 3, and comparing each feature, the decrease of the classification rates of mutual information and cross-correlation coefficient is noticeable. Next, as the results of Experiment 6, the EER is 6.94% and the classification rate is 82.00%, and the authentication accuracy is lower than the results of Experiment 5. Fig 10 shows the detailed results of the classification rates of Experiment 6a and Experiment 6b. From the graph, there is no big differences in the both results. Therefore, it is considered that the position of the registration data has less influence on the authentication accuracy. By the results of Experiment 5-6, it can be confirmed that as the number of registration data positions increases, versatility of the learning model is heightened and authentication accuracy is improved.

6 Conclusions

In this paper, we validated the influence of measurement electrode slippage which can occur during EEG authentication on authentication accuracy. From the validation results, it turned out that the influence of measurement electrode slippage on EEG authentication is significant. However, by registering electrode slippage data in advance, the versatility of the learning model for EEG authentication has increased, and it is possible to suppress the influence of electrode slippage to some extent. In addition, it became clear that there are some features with a large influence of electrode slippage. Among the four features used in this paper, it was confirmed that mutual information and cross-correlation coefficient have dependent relationship with the measurement positions.

In this paper, despite the small number of subjects as 10, the classification rate at electrode slippage is about 80%. From the results, another approach is needed in the future. As countermeasures, the method of modeling EEG at electrode slippage based on the brain structure, or the method of constructing a network that extracts features without affecting electrode slippage by using deep learning can be considered.

Acknowledgments

This work was partly supported by Grant-in-Aid for JSPS Fellows (16J10436).

References

[1] Lebedev, M. A., and Nicolelis, M. A.. Brain–machine interfaces: past, present and future. TRENDS in Neurosciences, 2006, vol. 29, no. 9, p. 536-546.

[2] Hotson, G., McMullen, D. P., Fifer, M. S., Johannes, M. S., Katyal, K. D., Para, M. P., and Crone, N. E., et al.. Individual finger control of a modular prosthetic limb using high-density electrocorticography in a human subject. Journal of Neural Engineering. 2016, vol. 13, no. 2, 026017.

[3] nekomimi http://neurowear.com/projects_detail/necomimi.html accessed 2017-05-24 (online).

[4] Wayman, J., Jain, A., Maltoni, D., and Maio, D.. An introduction to biometric authentication systems. Biometric Systems, 2005, p. 1-20.

[5] Kumari, P., and Vaish, A.. Brainwave based authentication system: research issues and challenges. International Journal of Computer Engineering and Applications. 2014, vol. IV, Issue I & II, p. 89-108.

[6] MindWave https://store.neurosky.com/pages/mindwave accessed 2017-05-24 (online)

[7] Emotive https://www.emotiv.com/ accessed 2017-05-24 (online)

[8] Enobio http://www.neuroelectrics.com/ products/enobio/ accessed 2017-05-24 (online)

[9] BioSemi http://www.biosemi.com/products.htm accessed 2017-05-24 (online)

[10] Niedermeyer, E., and da Silva, F. L. (Eds.).. Electroencephalography: basic principles, clinical applications, and related fields. Lippincott Williams & Wilkins. 2005

[11] Jasper, H. H.. The ten twenty electrode system of the international federation. Electroencephalography and clinical neurophysiology. 1958, 10, p. 371-375.

[12] Riera, A., Soria-Frisch, A., Caparrini, M., Grau, C., and Ruffini, G.. Unobtrusive biometric system based on electroencephalogram analysis. EURASIP Journal on Advances in Signal Processing. 2008, vol. 1, p. 1-8.

[13] Safont, G., Salazar, A., Soriano, A., and Vergara, L.. Combination of multiple detectors for EEG based biometric identification / authentication. IEEE International Carnahan Conference on Security Technology. 2012, p. 230-236.

[14] Yu Ishikawa, Kaori Nishibata, Masami Takata, Hiroyasu Kamo, Kazuki Joe.. Biometric Authentication based on Multi-feature Combination using EEG. International Conference on Parallel and Distributed Processing Technologies and Applications. 2016, p.394-400

[15] Marcel, S., and Millán, J. D. R.. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE transactions on pattern analysis and machine intelligence. 2007, vol. 29, no. 4, p. 743-752.