Computers & Security 129 (2023) 103198

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Brainwave-based authentication using features fusion

Mahyar TajDini [1], Volodymyr Sokolov [1], Ievgeniia Kuzminykh [2,3,*], Bogdan Ghita [4]

[1] Department of Information and Cyber Security, Borys Grinchenko Kyiv University, Kyiv 04212, Ukraine
[2] Department of Informatics, King's College London, London WC2R 2ND, UK
[3] Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkov, Nauki av.14, 61000, Ukraine
[4] School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth PL4 8AA, UK

ARTICLE INFO

Article history:
Received 10 May 2022
Revised 3 March 2023
Accepted 21 March 2023
Available online 22 March 2023

Keywords:
brainwaves
electroencephalogram
EEG
brain-computer interface
BCI
biometrics
authentication
machine learning
coherence
feature extraction

ABSTRACT

This article investigates the use of human brainwaves for user authentication. We used data collected from 50 volunteers and leveraged the Support Vector Machine (SVM) as a classification algorithm for the case study. User recognition patterns are taken from a combination of blinking, attention concentration, and picture recognition emotion sequences. These actions impact alpha, beta, gamma, and theta brain waves, which are measured using several electrodes. Ten different electrode placement patterns are explored, with varied positioning on the head. For each placement position, four features are examined, for a total of 40 extracts in the learning model. Features are: 1) spectral information, 2) coherence, 3) mutual correlation coefficient, and 4) mutual information. Each feature type is trained by the SVM algorithm, and the 40 weak classifier candidates. Adaptive Boosting (AdaBoost), a type of machine learning, is then used to generate a robust classifier, which is subsequently used to create a model, and select features, used to accurately identify individuals for authentication purposes. Upon verifying the proposed method using 32 legitimate users and 18 intruders, we obtained an authentication error rate (ERR) of 0.52%, and a classification rate of 99.06%.

© 2023 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

1. Introduction

Brain-Computer Interface (BCI) technology creates the ability for humans to communicate directly with machines. Researchers expect a lot from this technology, with anticipated applications such as monitoring health, emotions, controlling state-critical objects, and military purposes. Using brain activity signals, non-invasive BCI is being developed as a method that can be used safely and efficiently for health purposes. Currently, BCI studies are underway in various fields such applications as the manipulation of artificial limbs operated by brainwaves, wheelchair control systems that read brainwaves and move autonomously, and direct communication of brainwaves from person to person.

In addition, there are BCI technologies already on the market, such as the device "necomimi" [1] that senses human emotions and moves, and the application MindRDR [2] that operates Google Glass with brainwaves. With the development of BCI technology in the future, brainwaves as a user interface are conceivable.

Improved authentication technology is required to securely access and operate computers, and brainwaves with BCI technology may be able to facilitate this effort. Currently, unconventional authentication technologies, personal authentication using identifiers, and passwords are mainly used. However, plagiarism or brute force authentication attempts can easily be spoofed; Therefore, conventional methods are not always reliable. In recent years, biometric authentication has been used to address the gaps of conventional authentication; however, this method, although an improvement, has its own problems.

Biometric authentication is personal authentication using biometric information. Biometric authentication of fingerprints, irises, faces, voiceprints, etc., has been widely researched and developed, and authentication using this biometric information is more challenging to steal than conventional password authentication. Fingerprints and irises have especially high authentication performance and have been practical to use. However, the authentication system may be spoofed [3–5] and replicated. One of the reasons is that the information about fingerprints and irises required for authentication is constantly exposed.

Due to the dynamic nature of brainwaves which require special conditions and tools for reliable measurement, e.g., short distance, brain electrical activity cannot be easily replicated; additionally,

* Corresponding author.
E-mail addresses: v.sokolov@kubg.edu.ua (V. Sokolov), ievgeniia.kuzminykh@kcl.ac.uk (I. Kuzminykh), bogdan.ghita@plymouth.ac.uk (B. Ghita).

https://doi.org/10.1016/j.cose.2023.103198
0167-4048/© 2023 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

unlike other biometric methods, the subject must be alive. Therefore, biometric authentication using brainwaves has a series of advantages when compared to other biometric methods. Research on biometric authentication using an electroencephalogram (EEG) has already been carried out from various fields, and it has been clarified that it shows distinctive characteristics depending on the individual. [7–8]

In this article, we use pre-existing technologies such as BioSemi multi-channel electroencephalograph for data collection, coupled with SVM learning methods for data classification [6–14] to combine multiple features, including spectral information, coherence, and mutual information [15–22]. The authentication system in our study allowed us to receive higher performance than similar studies.

In recent years, the progress of electroencephalographs has been remarkable. Until now, multi-channel electroencephalographs have been used only in the medical field, because they are costly devices requiring specialized engineers to use them. However, at present, newer multi-channel electroencephalographs have been developed which can be used in daily life, such as for gaming, education and health home monitoring. A wide range of applications for EEG is presented in the study [23]. The survey shows that existing studies on electroencephalography use a small number of electrodes, 1–3 channels. Also, in this article, more unique features are realized by using a multi-channel electroencephalograph with 16 channels of electrodes.

The outline of this article is as follows: Section 2 introduces related research on EEG authentication, Section 3 proposes a user authentication system based on EEG features, in Section 4, the experiments are conducted to evaluate the proposed method, and the results are described.

2. Related Works

Person authentication based on brain activity should mainly consider EEG measurements, feature extraction, and classification/authentication methods. Brainwaves are not always constant, and change due to various internal and external stimuli. Therefore, EEG authentication under all measurement conditions should be studied by the researchers. Some of the conditions include brainwaves during resting [6–12,21,22], brainwaves during mental tasks [13,14,20], Visual Evoked Potentials (VEP) [15,16] and Event Related Potentials (ERP) [17,19].

The features used in EEG authentication also vary in studies, but the most popular remain spectral information obtained by frequency analysis [6,7,10,11,14,16,18,20–22]. Other features that can be met in the studies are related to channel synchronicity: a coherence to express the phase-amplitude relationship between electrodes [10–12,22], and a mutual correlation coefficient that calculates the similarity between electrodes as spatial information.

Among classification methods the researchers commonly use the autoregressive (AR) model [6–11], Discriminant Analysis (DA) [8,10,11,19], SVM [21,22], Neural Network (NN) [9,14,16].

The performance of biometric authentication is obtained from the classification rate and the Equivalent Error Rate (EER). The lower this error value is, the greater accuracy the biometric system has. The classification rate is the probability that the person is correctly classified as the person by clustering. EER is a point where the False Rejection Rate (FRR), which is supposed to be the person but not the person, and the False Acceptance Rate (FAR), which is thought to be the person despite being another person, intersects. The intersection of FRR and FAR is its EER. The existing studies [8,9,12,14–17,21] evaluate the performance only by the classification rate, and EER. There are relatively few studies [6,7,10,11,13,18–20,22] which are calculating the classification rate, but mostly only the data of the registered persons which have been already in the authentication system. Since the authentication request data is always classified as one of the legitimate users, it is considered that the intruder who is not registered in the system is not considered. On the other hand, calculating EER can evaluate using both genuine data and impostor data. Therefore, system performance that considers intruders can be obtained.

Studies that use EEG have been conducted for a long time. In a study reported by Poulos et al. in 1999 [6], classification was performed by learning vector quantization (LVQ) using spectral information obtained from brainwaves and an AR model. Authentication with four legitimate users and its 75 intruders resulted in an EER of 21% and a classification rate of 72–84%. Furthermore, by improving the method and using a computational geometry algorithm, the accuracy has been improved to an EER of 9.2% and a classification rate of 95% [7].

In 2001, Parajanpe et al. conducted an experiment in which 40 people were taken part and applied an AR model which he obtained from brainwaves to DA, achieving in this way a classification rate of 79–85% [8]. Mohammadi et al. reported that his AR model of ten brainwaves was trained in NN to obtain a classification rate of 80–100% [9]. Riera et al. performed DA using multiple features such as AR model, coherence, and intercorrelation coefficient, and EER 3.5–5.5% from the brainwaves of 51 legitimate users and 36 intruders. The classification rate of 97.5–98.1% was obtained [10]. Safont et al., like Riera et al., classified multiple features using DA, classification trees, etc. and found that 2.4% EER from the brainwaves of 50 legitimate users and 20 intruders. The classification rate was 93.8% [11]. La Rocca et al. classified the coherence between electrodes by applying the Mahalanobis distance. As a result, a classification rate of 97.5–100% was obtained from the brainwaves of 108 people [12].

In a study on brainwaves during mental tasks, in which nine authenticated people were using brainwaves during motion recall and language recall, Marcel et al. proposed a method that uses a Gaussian mixture model and a maximum a posteriori model. Similar to the above-mentioned result, an EER was 6.6–7.1% [13]. Hema et al. obtained a classification rate of 91.6–97.5% by extracting beta waves from the brainwaves of six people during reading and calculation and training them with NN [14]. In a study using VEP, Ravi et al. classified EEG by the simplified fuzzy ARTMAP and *k*-nearest neighbor method and found out that 20 people had a classification rate of 92.0–95.3% [15]. In addition, he improved the method, using spectral information and Elman NN, he improved the classification rate to 97.5–98.1% in 40 people [16]. In a study on ERP, in 2016, Ruiz Blondet et al. developed CEREBRE (Cognitive Event-Related Biometric Recognition) system using ERP obtained by showing multiple images, and 100 people in 50 people [17].

Among these existing studies, those which used a brainwave device with three or fewer electrodes are documented [6–12,14], those with 30 channels or more are in the literature at references [13,15–17], and there are much more studies targeting the state where the number of electrodes is small.

Nakanishi et al. mainly research continuous brainwave authentication during driving by verifying the optimum frequency band for authentication from the alpha wave—beta wave frequency band, he obtained the 22% of EER [18]. Karayama used a method that combined alpha waves and ERP, and as a result of an experiment with seven subjects, the classification rate was 86.8% for indoor rest, 74.8% for outdoor rest, and 68.4% for outdoor walking [19].

Summarising, prior research focused on maximizing the accuracy, following a specific combination of conditions, stimuli, data collection equipment, analysis, and interpretation. This is a valid approach, as accuracy and EER are the ultimate measures of performance in authentication, but the context also should be considered, specifically convenience, price, and exhaustive analysis.

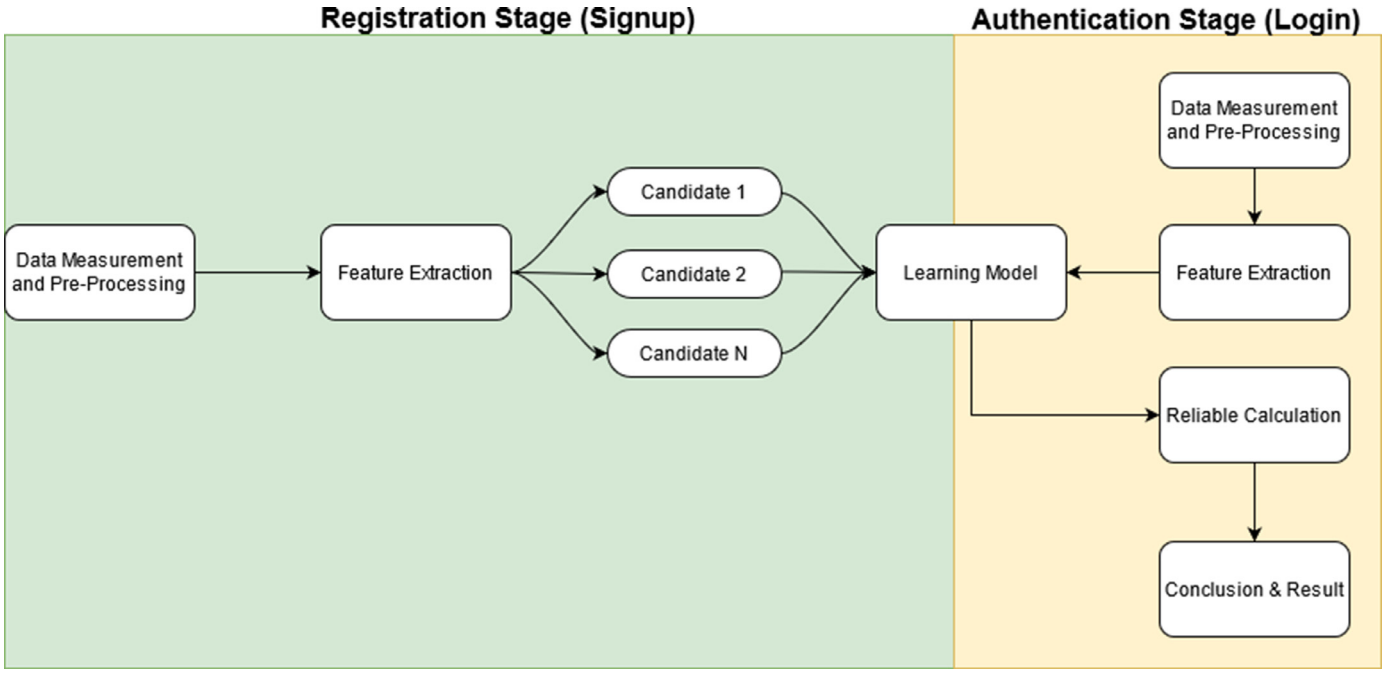


Figure 1. Authentication system flow.

Convenience may be tangentially relevant in a research context, but it represents a core requirement of any possible implementation. This is why, for a proposed method to be viable in a realistic environment, data collection should be both relatively non-intrusive and inexpensive. While prior studies achieved more accurate data collection through a combination of medical-grade or expensive equipment and sampling over long intervals, the proposed setups are less applicable to a practical use scenario. Also, as part of the process, authors placed less emphasis on data analysis by using specific methods and limited fusion of features.

In contrast to prior work, this study aims to investigate the performance of EEG for authentication through an extensive analysis of combining EEG signals in terms of frequency range, physical position, and processing. SVN is used as a core algorithm, but additional processing is added to optimise the input data, the associated features, and ultimately maximise the resulting accuracy. In addition, we aim to investigate the improvement in performance when using different electrode positioning schemes and collect different signals in order to determine the optimal trade-off configuration between convenience, accurate data collection, and resulting accuracy.

The present study is a natural evolution from our prior work. We have been conducting research using brainwaves during mental tasks and resting and, using frequency analysis of brainwaves during mental tasks and using cosine similarity from a group of ten subjects, we achieved an EER of 2.9% [20]. In addition, 26 subjects participated in an experiment using EEG at the resting time, by combining multiple features and classifying them by SVM. The classification rate was 98.6% [21]. In 2016, the method using AdaBoost was improved, leading to a decrease of the EER to 2.0% [22].

3. Methodology

3.1. Authentication System

In our research, since the goal was EEG authentication in a fleeting period (less than 60 seconds), we performed EEG readings while the subjects were resting; no mental tasks or external stimuli were required. Figure 1 shows the flow of the proposed authentication system. The system consists of a registration phase and an authentication phase.

In the registration phase, the legitimate user's brainwaves were firstly measured for a period and divided every second. Each datum was preprocessed, and feature extraction was performed. Weak classifiers were generated from the obtained features. A strong classifier was constructed by combining multiple weak classifiers using AdaBoost [20]. This is the learning model of the authentication system.

AdaBoost is a classification meta-algorithm that can be used with many other learning calculations to make strides in execution. The yield of the other learning calculations is combined into a weighted whole that speaks to the ultimate yield of the boosted classifier. AdaBoost is versatile in that ensuing frail learners are changed in favour of those occasions misclassified by past classifiers. During the data training period, it creates n number of decision trees. As the first decision tree/model is constructed, the record that was erroneously categorized during the previous model is the higher priority. Only these records are sent to the second model as input. The procedure will continue until we have decided on several foundation learners to develop.

In the authentication phase, as in the registration phase, the certifier's data was measured during a specific period, then preprocessed, after which the feature extractions were performed every second.

The learning model generated in the registration phase applies to the extraction features. The next step is the calculation of reliability that the certifier is the legitimate user. At this time, the average value of the reliability of all the measurement data is used as the reliability of the certifier. By comparing the reliability of the certifier with the preset threshold value, the acceptance/rejection of the certifier is calculated.

3.2. Data Collection and Preprocessing

The OpenBCI, a multi-channel electroencephalograph, was used in this study to measure the performance. The bipolar induction method was used to derive the reference electrode. With OpenBCI, the maximum sampling frequency of the electroencephalograph is

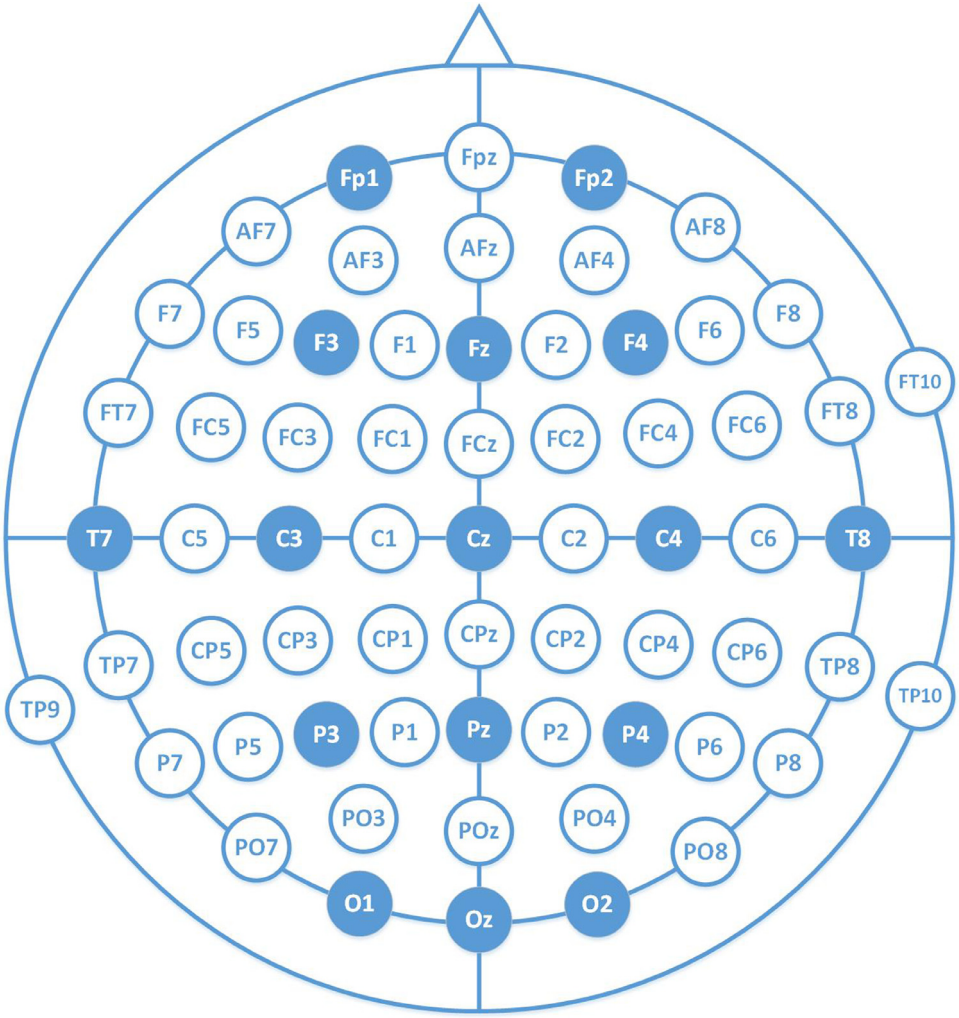


Figure 2. Electrodes placement.

2,048 Hz, and 256 channels is the maximum number of electrodes which can be mounted. In our study, the authentication system was limited; measurements were performed by using a sampling frequency of 2,048 Hz and 16 channels of electrodes. The electrodes were arranged as shown in Figure 2 (filled blue) according to the international 10–20 law [24,25].

Firstly, the brainwaves were measured for a specific period and divided every second. According to the following procedure, each datum was preprocessed (shown below) and corrected to data suitable for feature extraction:

Step 1. Bandpass filter.

Step 2. Noise removal.

Step 3. Normalization.

In Step 1, only the 4–40 Hz frequency band was extracted from the measured data with the help of a bandpass filter. This frequency band is the band where the activity of EEG is observed. 1–3 Hz is defined as a delta wave. Still, it was excluded from this article because it contains many artifacts of biological phenomena such as myoelectric potentials other than brainwaves, eye movements, and heartbeat. The bandpass filter also removes environmental artifacts such as AC disturbances at 50 and 60 Hz. A humming window is applied as a window function used in the bandpass filter.

In Step 2, the main tasks were to correct the pulse noise that appears temporarily, after the bandpass filter was applied the standard deviation of the data was obtained, and the data exceeding 3σ corrected to 3σ.

In Step 3, the denoised data was normalized to 0–1. These processes removed noises, and the data was reconstructed to be more suitable for authentication.

3.3. Feature Extraction

Features were extracted from the preprocessed data. This system uses four types of features: spectral information, coherence, mutual correlation coefficient, and mutual information. In addition, to confirm that electrodes were suitable for personal authentication, the differences in electrode placement sites were given as a feature quantity. There were ten types of electrode arrangement patterns used. The were a total of 40 combinations, (4 features $\times$ 10 electrode positions). The following sections explain each feature and electrode arrangement pattern.

3.3.1. Spectrum Information

Spectral information that uses the Fast Fourier Transformation (FFT) is applied as frequency analysis, the most common method for EEG analysis. Brainwaves are classified according to frequency, and their property differences depending on the frequency band. Therefore, frequency analysis can show if the characteristics of EEG are effective.

The amplitude spectrum is used as the spectrum information in the proposed method. When performing FFT, the humming window with size of N =30 is applied as in the preprocessing. The amplitude spectrum PS_a of the electrode can be obtained from the real part Re_a^2 and the imaginary part Im_a^2 by the following equation:

$$PS_a = \sqrt{Re_a^2 + Im_a^2}. \tag{1}$$

From the obtained spectral information PS_a, the average content rate was calculated for each frequency band of theta (4–8 Hz), alpha (8–14 Hz), beta (14–26 Hz), and gamma (26–40 Hz) waves with for each of that four feature as mentioned before (spectral information, coherence, mutual correlation coefficient, and mutual information) a feature with a vector length of 4. The average content rate is the spectral content rate per data in each frequency band. The average content is the average spectral content per data in each frequency band.

3.3.2. Coherence

Coherence is used to obtain the relation between the phase and amplitude of the waveform between the electrodes. Coherence is obtained from the amplitude spectrum and the cross-spectrum. Coherence between electrodes a and b (COH) is calculated by the following equation:

$$COH = \frac{CPS_{ab}}{PS_a \cdot PS_b} \tag{2}$$

where

$$CPS_{ab} = (Re_a Re_b + Im_a Im_b)^2 + (Re_a Im_b + Im_a Re_b)^2. \tag{3}$$

The average content of the obtained coherence was calculated for each of the four frequency bands in the same way as the spectral information and was used as a feature with a vector length of 4.

3.3.3. Mutual Correlation Coefficient

Since the similarity between electrodes was used as a feature, the mutual correlation coefficient was also used. The intercorrelation coefficient was used in various fields, such as emotion estimation of comfort and discomfort and brainwave analysis during exercise.

The mutual Correlation Coefficient (CC) between electrodes the following equation expresses a and b:

$$CC = \frac{S_{i=1}^{K}(a_i - \bar{a})\left(b_i - \bar{b}\right)}{\sqrt{S_{i=1}^{K}(a_i - \bar{a})^2}\sqrt{S_{i=1}^{K}\left(b_i - \bar{b}\right)^2}} \tag{4}$$

where K is the data length; a_i and b_i are the time-series data of the electrodes of a and b, respectively; $\bar{a}$ and $\bar{b}$ are the average value of the time-series data of the electrodes a and b. When the coefficient is positive, there is a positive correlation. When it is a zero, it means that there is no correlation.

3.3.4. Mutual Information

Mutual information is required because the interdependence between electrodes is used. Mutual Information (MI) between electrodes a and b:

$$MI = \sum_{I=1}^{K}\sum_{j=1}^{K} p\left(a_i, b_j\right) \log \frac{p\left(a_i, b_j\right)}{p(a_i)p\left(b_j\right)} \tag{5}$$

where $p(a, b)$ is the joint probability distribution function of a and b, and $p(a)$ and $p(b)$ are the peripheral probability distribution functions of a and b, respectively. It is necessary to rescale each value of the data as preprocessing.

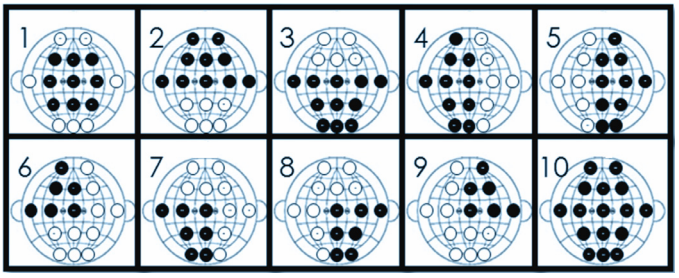


Figure 3. Different patterns for electrode placement in the study.

3.3.5. Electrode Arrangement Pattern

Figure 3 shows the electrode arrangement pattern. In this article, ten types will be tested. Table 1 shows the details of the electrode arrangement pattern. By using multiple patterns with different numbers of electrodes and different electrode positioning, the effectiveness of user authentication can be investigated.

3.4. Learning Model Generation

AdaBoost is applied to a combination of features as a method to perform personal authentication. AdaBoost is applied to a combination of weak classifiers, effectively boosting them to establish a strong classifier which can be reliably used for authentication.

AdaBoost is a type of machine learning that adaptively updates learning data weights. The clustering result is determined by a weighted majority vote of the weak classifiers. The algorithm is as follows:

1. Initialize the weight w_n of the feature x_n where $n = 1, \ldots, N$ to $1/N$.
2. Calculate L weak classifier candidates f_l where $l = 1, \ldots, L$.
3. Repeat 3.1–3.6. Let m be the number of learnings and start from $m = 1$.
   - 3.1. Repeat 3.1.1 L times.
     - 3.1.1. Calculate the error rate m of the weak classifier candidate. Let t_n be the target value of $f_l(x_n)$

$$E_m = \frac{\sum_{n=1}^{N} w_n I(f_l(x_n))}{\sum_{n=1}^{N} w_n}, \tag{6}$$

$$I(f_l(x_n)) = \begin{cases} 0, & f_l(x_n) = t_n \\ 1, & otherwise \end{cases} \tag{7}$$

   - 3.2. Select the weak classifier $y_m(x_n)$ with the lowest error rate from the weak classifier candidates. $y_m(x_n)$ is the output of the weak classifier.
   - 3.3. Calculate the reliability a_m from the error rate of the selected weak classifier.

$$a_m = \frac{1}{2}\ln\left(\frac{1 - E_m(y_m)}{E_m(y_m)}\right). \tag{8}$$

   - 3.4. If the error rate is 0.5 or more, substitute m for M and proceed to 4.
   - 3.5. Update the weight. However, the total weight should always be 1.

$$w_n^{(m+1)} = w_n^{(m)} esp(a_m H(y_m(x_n))), \tag{9}$$

$$w_n^{(m+1)} = \frac{w_n^{(m+1)}}{\sum_{n=1}^{N} w_n^{(m)}}. \tag{10}$$

   - 3.6. Add 1 to M.

Table 1
Electrode placement patterns.

No	Qty	Electrodes	Position on the Head
1	9	F3, Fz, F4, C3, Cz, C4, P3, Pz, P4	Around top head
2	10	Fp1, Fp2, F3, Fz, F4, T7, C3, Cz, C4, T8	Circumference head
3	11	T7, C3, Cz, C4, T8, P3, Pz, P4, O1, Oz, O2	Around the back head
4	10	Fp1, F3, Fz, T7, C3, Cz, P3, Pz, O1, Oz	All left hemisphere
5	10	Fp2, Fz, F4, Cz, C4, T8, Pz, P4, Oz, O2	All right hemisphere
6	6	Fp1, F3, Fz, T7, C3, Cz	Left hemisphere and all front head
7	7	T7, C3, Cz, P3, Pz, O1, Oz	Left hemisphere and back head
8	7	Cz, C4, T8, Pz, P4, Oz, O2	Right hemisphere and back head
9	6	Fp2, Fz, F4, Cz, C4, T8	Left hemisphere and circumference head
10	16	All electrode on position	Full head

4. Construct a_{sum} strong classifier (the cumulative reliability of weak classifiers):

$$a_{sum} = \sum_{m=1}^{M} a_m \tag{11}$$

In Step 1, 40 types of features in Subsection 3.2 were used. N is the number of trained data.

In Step 2, a Support Vector Machine (SVM) is applied to each of these features to generate 40 types of weak classifier candidates. SVM is a very good algorithm choice for brain wave classification, as demonstrated by prior research. A summary of various MLs used for neural decoding is provided in [26], where comparative analysis of prior studies indicate that SVM delivers better than its traditional counterparts; more specifically, a recent review of existing EEG authentication methods identified SVM as one of the preferred choices [27]. A number of studies focused specifically at the performance of SVM in BCI, such as [28] and [29], where the authors perform EEG signal classification using a more basic approach.

The Radial Basis Function is used for the SVM kernel. The generation of the learning model consists of two processes, weak discriminator candidate generation, and strong discriminator generation.

First, in the weak classifier candidate generation, SVM is applied to features. By doing this, a weak classifier is generated. The second strong classifier generation is ensemble learning. A strong classifier combined with a weak classifier is generated by using AdaBoost; the combination of SVM and AdaBoost was successfully validated by prior BCI work in [30]. The strong classifier is generated in Steps 3 and 4 and becomes a learning model for personal authentication. Since there are only 40 weak classifier candidates, 40 weak classifier candidates are generated. AdaBoost selects and combines the most suitable weak classifiers from these weak classifier candidates. The second strong classifier generation will be explained. First, it is necessary to select the weak classifier to be combined from the weak classifier candidates. For these selections, the error rate of the weak classifier candidates are used. The weak classifier candidate with the lowest error rate is selected. Then, the reliability of the weak classifier is calculated from the error rate. Next, we adjust the data weights to learn the wrong results. This is done repeatedly to the selected weak classifier until its reliability becomes a strong classifier.

AdaBoost is a method to improve identification accuracy by adaptively updating the weights of the training data. Figure 4 shows the flow of weight update for AdaBoost, and it is an example of this learning repeated three times. First, the weak Classifier 1 classifies the class. Incorrect data in weak Classifier 1 updates the weight and then classifies it in weak Classifier 2.

Similarly, erroneous data in Classifier 2 updates the weights and is applied to weak Classifier 3. These processes are repeated, and the final classification result is determined by a weighted majority vote of the weak classifier. The detailed algorithm is shown in the procedure below.

In Step 1, set the weights used in AdaBoost. Initialize to $1/N$ to equalize the weight vector w of each input x. The sum of the elements of the weight vector w is always 1. Here, the weight vectors w of all 40 types of inputs x are initialized. In Step 3, a weak classifier combined with a strong classifier is selected from the weak classifier candidates. This process is learning for AdaBoost. First, in Step 3.1, the error rates E of 40 types of weak classifier candidates are calculated. If the input data is correctly classified as the person, it is set as 0, and if it is incorrectly classified as another person, it is set as 1. The error rate is calculated considering the weight of each input data. When $m = 1$, there is no bias in the weight of the input data. In Step 3.2, the weak classifier candidate with the lowest error rate obtained in Step 3.1 is selected. The weak classifier candidates selected here are the classifiers with the highest classification accuracy among the prepared weak classifier candidates. Let this be the m^{th} weak classifier y that is the output of the weak classifier.

In Step 3.3, the reliability of the weak is calculated from the error rate $E(y)$ of the weak classifier $\boldsymbol{y}$. In Step 3.4, it is judged whether the learning is sufficient. If the error rate exceeds 0.5, it is judged that the classification accuracy will not improve even if more weak classifiers are added, the learning is finished, and the process proceeds to Step 4, and if the error rate is less than 0.5, continue learning. In Step 3.5, the weight vector w of the input x is updated. Since the sum of the elements of the weight vector w is always equivalent to 1. Add the value of m in Step 3.6 and repeat Step 3.1 to 3.6 until the criteria in Step 3.4 are met. In Step 4, the M weak classifiers selected so far to form a strong classifier. The result of weighting and adding each weak classifier by reliability is the strong classifier, the learning model used in this system.

In this article, since the reliability was obtained from the result of AdaBoost as personal authentication, the cumulative reliability of the weak classifiers a_{sum} was corrected to 100% after the strong classifier was configured.

3.5. Evaluation

The certifier measures the EEG and designates the legitimate user. This system is measured by finding the reliability of the legitimate user specified by the certifier. The measurement data is preprocessed, and features extracted every second, as in the case of registration. The extracted features are applied to the learning model generated in the registration phase. The learning model calculates the reliability of the specified legitimate user and certifier. Since the measurement data is divided and processed every second, greater reliability can be obtained if the data length is 2 seconds or longer. The average of these credibility scores, ranging from 0-100%, is then used as the certifier credibility. If the trustworthiness of the certifier is equal to or higher than the preset threshold value, it is considered the person themselves and ac-

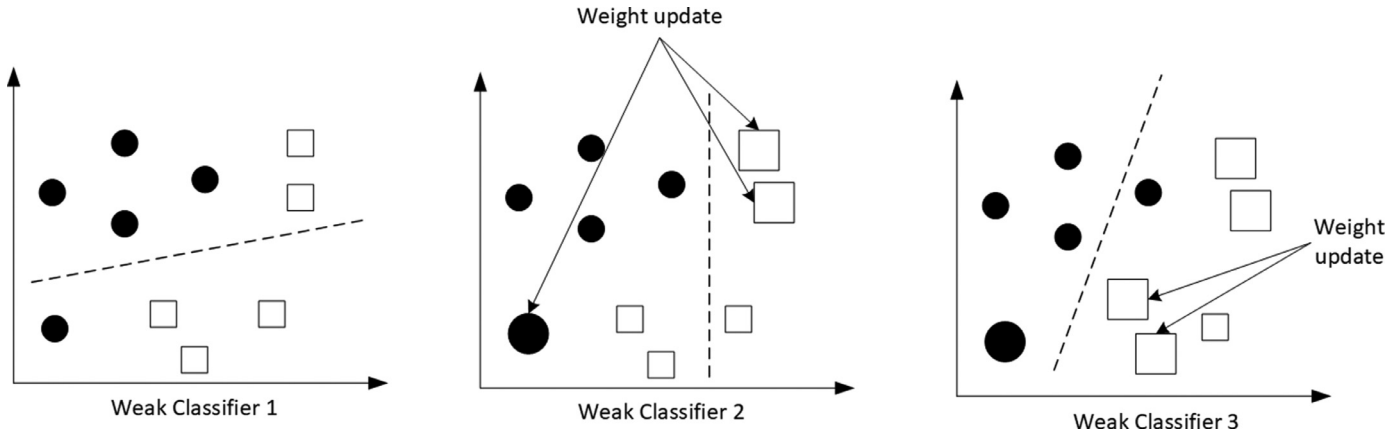


Figure 4. Weight update examples.

cepted. If it is less than the threshold value, it is regarded as another person and rejected.

4. Results and Analysis

4.1. Experiment Setting

The performance of this system is calculated from EER and classification rate. A set of EEGs were carried out on 50 participants aged between 20 and 30. Due to the demographic mix of the audience where the experiment was advertised, all participants to the study were females, students in a higher education institution. Prior to the experiment, the participants were briefed about the full process, and they signed an agreement authorizing the use of all data from the experiment to be used anonymously for research purposes. All recordings were taken using an OpenBCI electroencephalograph with 16 electrodes, and subjects were at rest with closed eyes and in the sitting position. All EEG recordings lasted for 60 seconds and were repeated 50 times per subject, resulting in 2,500 samples.

The dataset was split into two: training and testing. Since this system uses a SVM that is supervised learning at the time of authentication, it is necessary to divide the measurement data of the legitimate users into test data and supervised data. To reduce the error in authentication accuracy due to test data selection, it uses ten cross-validation to calculate the results. In other words, 50 pieces of data of each legitimate user is randomly divided into ten groups. The system uses 45 samples per participant, which corresponds to nine groups, as trained data, and the remaining five samples, which corresponds to one group, as its actual data. Similarly, one of the ten groups is used as test data for intruder data.

The performance value is calculated by the following method. EER is obtained from FAR and FRR calculated by comparing the reliability of the input data and the threshold value. The classification rate is calculated by calculating the reliability of each legitimate user in the input data and the probability that the highest reliability is the legitimate user himself.

The verification items of this proposed system are shown below:

1. Performance evaluation of the proposed system verification:
   a. Performance evaluation of each feature.
   b. Reliability verification of legitimate users and intruders.
   c. Performance comparison between the proposed system and existing research.
   d. Performance evaluation of the proposed system due to changes in the test data length.
2. Generation results of the learning model:
   a. Configuration of the generated learning model.
   b. Proposal of a new learning model verification.

Table 2
Features classification rates.

Feature	EER, %	Classification rate, %
Spectral information	2.83	92.19
Coherence	2.55	93.69
Mutual correlation coefficient	1.75	96.69
Mutual information	1.17	98.25
Proposed method	0.52	99.06

However, since test data is input data and needs to be measured each time it is authenticated, it is desirable to authenticate with short-time data. In this experiment, the first 10 seconds are cut out from each measurement and is used as training data to for learning. The rest of the data is considered measurement data, and the next 6 seconds of this data is matched against the test data and is used for verification. In this study, the data is used at the time of authentication, based on the first 6 seconds of measurement data which is used for verification.

The results of data classification by SVM for all 16 channels and the EER and classification rate are calculated from the results shown in Table 2. We compare the method using four types of features: spectral information, coherence, mutual correlation coefficient, and mutual information, with the proposed method that combines the four types of features with AdaBoost. The values in Table 2 show the average value after ten cross-validations in a percentage. Data measurement, preprocessing, feature extraction, and judgment methods are the same as the proposed method. The lower EER and higher classification rates are obtained from the four types of features in mutual information, mutual correlation coefficient, coherence, and spectral information. The proposed method that combines multiple features by AdaBoost obtained high performance with an EER of 0.52% and a classification rate of 99.06%. This is the best result compared to the four types of features. In particular, the EER was less than 1%, and the error rate was less than half of the mutual information amount that can obtain the lowest EER among single features. Therefore, it is considered that the combination of features by the proposed method is more effective as an authentication method than the one that uses a single feature.

4.2. Authentication Accuracy

The effectiveness of this system is confirmed by verifying the difference in reliability between the legitimate user and the in-

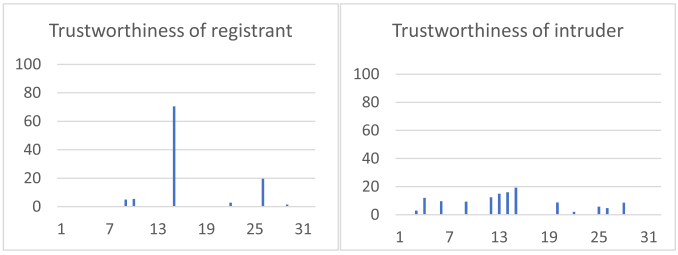


Figure 5. An example of trust between a legitimate user and an intruder.

truder. Verification by the following three types of authentications is required to evaluate the authentication system's performance. Next, to check the authentication accuracy, it is necessary to perform the following three types of verification case studies:

Verification A. Formal Authentication of legitimate users.

Verification B. Authentication by impersonation of the legitimate user.

Verification C. Authentication by impersonation of the intruder.

Verification A verifies when the legitimate user is officially authenticated, and Verification B verifies when the legitimate user impersonates another legitimate user. Verification C verifies when the intruder impersonates the legitimate user.

Figure 5 shows an example of the trustworthiness of authentication using this system with two types of input data: legitimate user and intruder. The left figure shows an example of the trustworthiness of the legitimate user, which corresponds to Verification A and Verification B. The right figure shows an example of the trustworthiness of intruders, which corresponds to Verification C. The horizontal axis is the number of legitimate users, and there are 32 legitimate users in this experiment. The vertical axis is the confidence level of the input data. The left figure in Figure 5 shows the confidence of each legitimate user obtained from the input data of Legitimate User 15. The confidence level of 70.43% is obtained for the Legitimate User 15.

The numbers of the other legitimate users for which a confidence level was obtained are 9, 10, 22, 26, and 29. This indicates that the split data was classified as data other than the original data. However, since the legitimate user with the highest confidence is Legitimate User 15, the classification of the input data is successful. Here, we discuss the results of Verification A. Since authentication is based on the threshold value, if the threshold value is less than 70.43% confidence of the input data, the authentication is accepted as having sufficient confidence. Therefore, it can be said that the legitimate user is officially recognized. However, if the threshold value is higher than the confidence level of the input data, the authentication is rejected.

Next, we consider the case of Verification B, where Legitimate User 15 impersonates Legitimate User 26 and performs authentication. The subsequent highest trustworthiness of Legitimate User 15 is 18.50% for Legitimate User 26, which is lower than the trustworthiness of legitimate user 15. However, if the threshold is less than 18.50%, the authentication is allowed as Legitimate User 26. This is the authentication by impersonating the legitimate user. In this case, setting the threshold value to a value greater than 18.50% and less than 70.43% enables Verification A proper authentication of the legitimate user. It prevents Verification B authentication by the legitimate user's impersonator. Figure 5 shows the trust level of each legitimate user obtained from the input data of intruders. Out of the 32 legitimate users, 13 legitimate users have a confidence level. The highest confidence level is 15.45% for Legitimate User 15, which is exceptionally low compared to the result of Verification A. Also, as in the result of Verification B, if the threshold is less than 15.45%, the authentication is accepted as Legitimate User

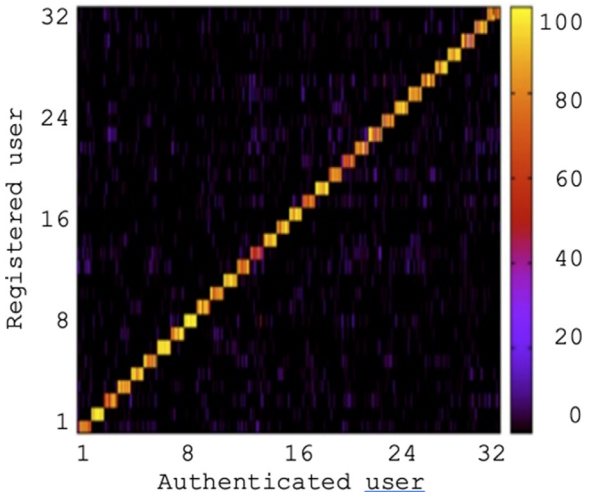


Figure 6. Reliability of Verification A and B.

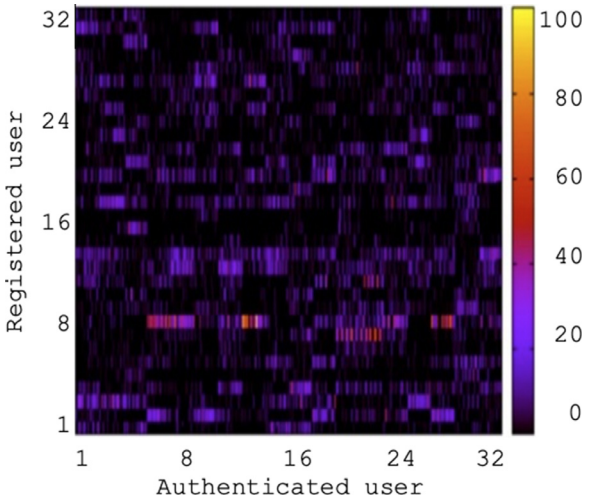


Figure 7. Reliability of Verification C.

15. By setting the threshold higher than 15.45%, it is possible to prevent authentication by intruder spoofing (Verification C).

Figures 6 and 7 show the reliability of all the data obtained by the proposed method. The horizontal axis is the certifier's number, and the vertical axis is the legitimate user's number.

Figure 6 shows the reliability of Verifications A and B. Suppose the certifier number and the legitimate user number are matched. In that case, it is the result of authentication of Verification A, and if they did not match, it is the result of authentication by spoofing Verification B. In other words, the diagonal component is the result of Verification A, and the non-diagonal component is the result of Verification B.

From Figure 6, it is clear that if the certifier and the legitimate user matched, the reliability is high, and if they did not match, the reliability is low. The average reliability of each component is 80.54% for Verification A and 0.63% for Verification B. Therefore, it is possible to prevent spoofing of the legitimate user.

Figure 7 shows the reliability of Verification C. All components show the results of Verification C. Since Verification C is the data of an intruder not registered in the system, the legitimate user number and the certifier number do not match. The reliability of Verification C is lower than that of Verification A. The average value of the reliability of all components in Verification C is 3.12%. Although the reliability is higher than that of Verification B, the difference

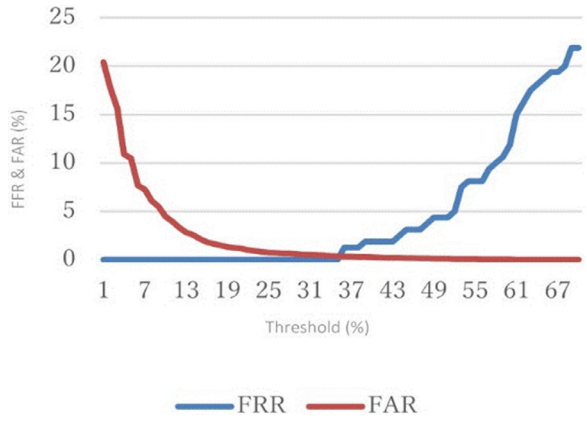


Figure 8. False acceptance and recognition rates.

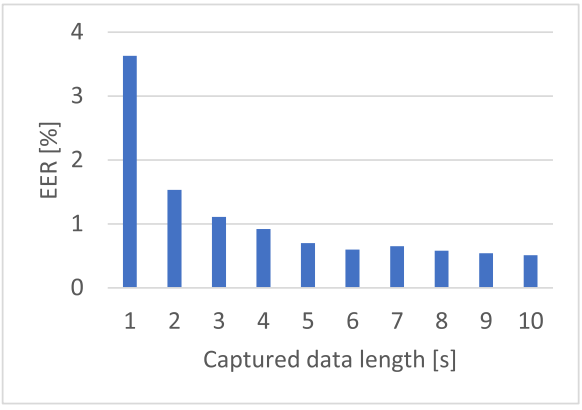


Figure 9. Equivalent error rate: case of changing data length.

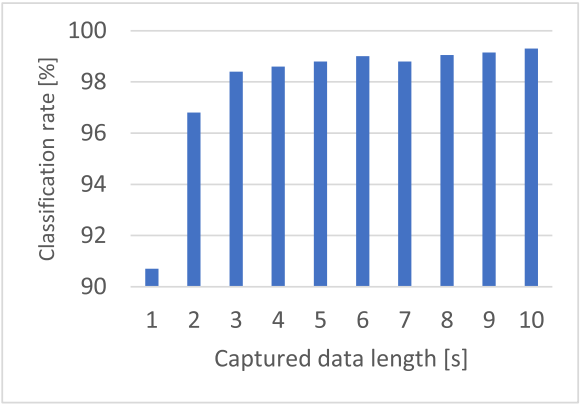


Figure 10. Classification rate: case of changing data length.

Figures 9 and 10 showed the EER and classification rate when the data length used during authentication was changed. The horizontal axis is the data length changed in 1–10 seconds, and the vertical axis is the EER at that time.

These figures show that the longer the data length was used, the better the accuracy of both EER and classification rate will show. When the data length is one second, the EER and the classification rate are 3.61 and 90.50%, respectively, which cannot be sufficient authentication accuracy. Since the data is not divided, it cannot be averaged, and the accuracy is considered low. Since the average number of EERs less than 1% is four or more, the shortest data length needs to be four seconds or more. In addition, since the average number with a classification rate of 99% or more is six or more, the shortest data length must be 6 seconds or more. When using the data length for ten seconds, the EER and classification rate are 0.43% and 99.19%, respectively. And both have good results.

from Verification A is unambiguous. Therefore, it is considered that a highly accurate authentication system can be constructed by setting a threshold value between the reliability of Verifications A and C.

The FRR and FAR of the proposed system are shown in Figure 6. This is an example of the 10-fold cross-validation result. The horizontal axis is the reliability threshold, and the vertical axis is the FAR and FRR values. The solid line shows its graph of FRR, and the dotted line shows its graph of FAR. Focusing on the FRR graph, the false-negative rate has an FRR of always 0% for those with a threshold of 35% or less, and the FRR value gradually increases as the threshold rises from 35%. In other words, it can be said that there was no input data which reliability was 35% or less.

On the other hand, in its FAR graph, which is a false-positive rate, the value of FAR decreases as the threshold increases, and when the threshold is 64%, it has FAR of 0% and does not change after that. Since EER is the intersection of FAR and FRR, it can be obtained from the graph in Figure 6. When the threshold is 35%, FRR is 0% and FAR is 0.35%, and the EER is determined to be 0.18% from the average value. EER considers both FRR and FAR values and shows the best performance value of the system to be verified. However, since the FAR and FRR required by the system are different, it is necessary to set an appropriate threshold. If it requires FAR less than 0.1% in this system, the threshold needs to be 52% or more, and FRR is 5% or more. If the FAR is set to 0% and no one else is accepted, the threshold value must be 64% or higher, and the FRR is 18% or higher. In this way, it can be seen from Figure 8 that FRR and FAR are in a trade-off relationship and that if one decreases the other increases.

4.3. Comparison with Other Studies

The comparison of the proposed method with existing studies [11–17] is shown in Table 3. These studies include studies that use only legitimate users as subjects for verification and studies that use legitimate users and intruders. During verification of intruders, it indicates the number of intruders after the number of legitimate users. Additionally, the state at the time of authentication is different from the existing studies. It describes resting at rest, mental at the time of the mental task, VEP when the visual evoked potential was used, and ERP when the self-proclaimed related potential was used. This shows the features used for authentication and the classification method. The proposed method results are the average values of EER and classification rate after ten cross-validations, which are 0.52% and 99.06%, respectively. This result is for a data length of 6 seconds, the same length as Safant 2016 [11] published, which authenticates using the shortest data length in his research. Other existing studies [6–10,12–17] use 24 seconds' period. The data length was used for several minutes.

The authentication accuracy of the proposed method of EER is higher than that of all mentioned studies. In the proposed system, Safant 2016 [11], which has the lowest EER in the existing research, is 2.4% or less, which is less than 1/4 of the EER. As for the classification rate, 100% was obtained according to the reports of Mohammadi et al. [9], La Rocca et al. [12], and Blondet et al. [17]. Among mentioned studies [9] and [12], who used resting EEG as in the proposed method, had data lengths of 24 seconds and 60 seconds, respectively, corresponding to 4 and 10 times of the data lengths used in this experiment. It requires more than double. Therefore,

Table 3
Studies and methods of comparison.

Research case	Subject	State	Method	ERR, %	Classification rate, %
Poulos, 1999 [6]	4, 75	Resting	Spectral information, AR/LVQ	21.0	72.0..82.0
Poulos, 1999 [7]	4, 75	Resting	Spectral information, AR / computational geometry algorithm	9.2	95.0
Paranjanpe, 2001 [8]	40	Resting	AR/DA	–	79.0..85.0
Mohammadi, 2006 [9]	10	Resting	AR/NN	–	80.0..100
Riera, 2008 [10]	51, 36	Resting	Spectral information, intercorrelation coefficient, coherence / DA	3.5..5.5	97.5..98.1
Safont, 2012 [11]	50, 20	Resting	AR, spectral information, independent component analysis, time reversibility, DA, classification tree	2.4	93.8
La Rocca, 2014 [12]	108	Resting	Coherence	–	97.5..100
Safont, 2012 [11]	32, 18	Resting	S-information, SVM	0.5	99.1
Mercel, 2007 [13]	9	Mental	Gaussian mixed model	6.6..7.1	–
Hema, 2008 [14]	6	Mental	Spectral information / NN	–	91.6..97.5
Ravi, 2005 [15]	20	VEP	Simplified fuzzy ARTMAP	–	92.0..95.3
Palaniappan, 2007 [16]	40	VEP	Spectral information / NN	–	92.9..98.1
Blondet, 2016 [17]	50	ERP	Normalized cross-correlation	–	100
Present study	50	Resting	SVN/AdaBoost	0.52	99.06

Table 4
Single feature analysis for each pattern (1..10).

	Reliability									
Feature	1	2	3	4	5	6	7	8	9	10
Spectral information, %	0	0	0.03	0	0	0	0	0	0	15.58
Coherence, %	0	0	0.05	0	0	0	0	0	0	20.03
Interrelationship, %	0	0	0	0	0	0	0	0	0	21.61
Mutual information, %	0	0	6.39	0	0	0	0	0	0	36.31

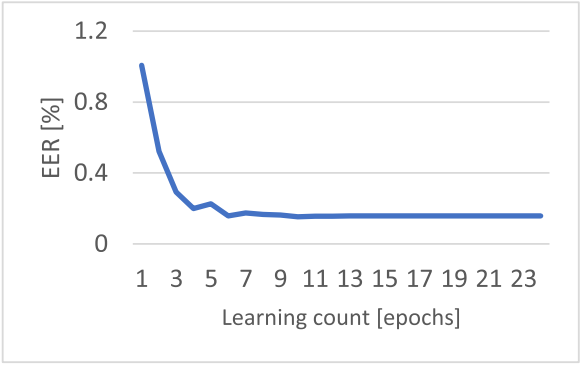


Figure 11. Error rate by learning epochs.

Table 5
Reliability and accuracy of combined features.

Feature extracted	Pattern	Reliability, %	EER, %	Classification rate, %
Mutual information	10	36.31	1.17	98.25
Cross-correlation coefficient	10	57.92	0.76	98.69
Coherence	10	77.96	0.57	98.87
Spectral information	10	93.54	0.56	98.94
Mutual information	3	99.92	0.52	99.06
Coherence	3	99.97	0.52	99.06
Spectral information	3	100	0.52	99.06

the classification rate of the proposed method is considered higher when short-time data is used in our study.

4.4. Combining Results of Multiple Features

We will consider the combination of results of the features at the proposed method. First of all, Figure 11 shows an example of the learnings number of AdaBoost and the transition of EER used in the proposed method. The horizontal axis is the value of the number of learnings repeated in AdaBoost, and the vertical axis is the value of EER at the same time. The first few learnings can confirm a depression in EER. In this example, the learning ends with its 24 lessons, and after 14 lessons, it has no change in EER and stays constant.

Table 4 shows the reliability of each feature after learning. Ten is the average value after cross-validation, and it is displayed in a percentage. The total reliability of spectral information, coherence, mutual correlation coefficient, and mutual information amount are 15.61, 20.08, 21.61, and 42.70%, respectively. Mutual information accounts for nearly half of the total, and spectral information is the least. The reason the spectral information's reliability was low is that in the proposed method, the features are extracted from the data every second so that individual differences from the spectral information are not sufficiently obtained in one second. By extending the data length for feature extraction, sufficient reliability can be obtained even with spectral information. Pattern 10 accounts for 93.53% of the total, focusing on the electrode arrangement pattern. Just Pattern 3 is different. Pattern 3 uses 11 electrodes, which is the second largest number after Pattern 10, so it is considered that the number of used electrodes has a significant effect on the results. In addition, the occipital region has less noise, such as eye movements, than the frontal region. In this way, high reliability is obtained. Out of the 40 combinations, 33 combinations have never been used. Therefore, it can be said that the feature quantities used are limited to the few top ones.

By doing so, for a combination of features suitable for authentication, it is necessary to select the top few with high reliability. Table 5 shows the results of accumulating 40 combinations in descending order of reliability. The selected features and electrode arrangement pattern, cumulative reliability, EER, and classification rate are displayed when the number of used features is increased

to 1–7. From the mentioned table, it is evident that EER decreases while the number of used features increases.

However, it is shown that the classification rate is increasing. Therefore, it is considered that the combination of features leads to the improvement of authentication accuracy. Further, when the number of features is five, the cumulative reliability exceeds 99% and remains constant after that. The EER and classification rates are 0.52 and 99.06%, respectively, equivalent to the results that use all the features selected by AdaBoost. It is worth noting that these figures position the proposed method at the top of the state of the art biometric classification methods, as shown in Table 4. The results are surpassed only by the authors of [17], who did benefit though from a more controlled stimuli environment (specific images shown to the subjects in a controlled environment).

Due to this, it is considered that sufficient learning can be performed with five features. The selected combinations are {mutual information, pattern 10}, {mutual correlation coefficient, pattern 10}, {coherence, pattern 10}, {spectral information, pattern 10}, {mutual information, pattern 3}. This combination is valid for authentication because the results are the same for all ten cross-validations.

5. Conclusions

This article proposes biometric authentication by combining multiple features using EEG. We used four types of spectral information for the features: coherence, mutual correlation coefficient, and mutual information. There were 40 combinations of ten patterns in which the electrodes in the electroencephalograph were changed. We succeeded in improving the authentication accuracy from these combinations by selecting the optimum features using AdaBoost. As a result, the EER showed 0.52% when the data length for authentication was 6 seconds after applying the proposed method. This is undoubtedly a good result even in comparison to existing studies.

It is considered that the selected features vary influenced by the used data length for authentication, but by adopting the combination of features by AdaBoost, which is the proposed method, the suitable features for the data length were selected.

In the future, we aim to identify effective electrode arrangements for authentication by considering the combination of all electrodes. This article evaluated the performance by comparing the current research results and the proposed method. Henceforward, we put a task to show the effectiveness by comparing the existing method using the same experimental data. To establish biometric authentication using EEG, developing a large-scale EEG database will be necessary.

Funding

This research received no external funding.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Mahyar TajDini: Conceptualization, Methodology, Software, Investigation, Writing – original draft. **Volodymyr Sokolov:** Conceptualization, Validation, Writing – original draft, Resources. **Ievgeniia Kuzminykh:** Visualization, Formal analysis, Writing – review & editing. **Bogdan Ghita:** Visualization, Formal analysis, Resources, Writing – review & editing.

Data availability

The data that has been used is confidential.

References

Neurowear Projects/nekomimi. Available online: https://neurowear.com/necomimi/ (accessed on 5 October 2021).
MindRDR. Available online: http://mindrdr.thisplace.com/static/index.html (accessed on 5 October 2021).
Marasco, E., Ross, A., 2015. A survey on antispoofing schemes for fingerprint recognition systems. ACM Comput. Surv. 47 (2), 1–36. https://dl.acm.org/doi/10.1145/2617756.
Cao, K., Jain, A.K., 2016. Technical Report MSU-CSE-16-2, pp. 1–3.
Gupta, P., Behera, S., Vatsa, M., Singh, R., 2014. On iris spoofing using print attack. In: 22nd International Conference on Pattern Recognition, pp. 1681–1686. doi:10.1109/ICPR.2014.296.
Poulos, M., Rangoussi, M., Chrissikopoulos, V., Evangelou, A., 1999. Person identification based on parametric processing of the EEG. In: IEEE International Conference on Electronics, Circuits and Systems, 1, pp. 283–286. doi:10.1109/icecs.1999.812278.
Poulos, M., Rangoussi, M., Chrissikopoulos, V., Evangelou, A., 1999. Parametric person identification from the EEG using computational geometry. In: IEEE International Conference on Electronics, Circuits and Systems, 2, pp. 1005–1008. doi:10.1109/ICECS.1999.813403.
Paranjape, R.B., Mahovsky, J., Benedicenti, L., Koles, Z., 2001. The electroencephalogram as a biometric. Canadian Conference on Electrical and Computer Engineering 2, 1363–1366. doi:10.1109/CCECE.2001.933649.
Mohammadi, G., Shoushtari, P., Molaee Ardekani, B., Shamsollahi, M.B., 2006. Person identification by using AR model for EEG signals. World Academy of Science, Engineering and Technology (11) 281–285 no.EPFL-CONF153223.
Riera, A., Soria-Frisch, A., Caparrini, M., Grau, C., Ruffini, G., 2008. Unobtrusive biometric system based on electroencephalogram analysis. EURASIP J. Adv. Signal Process. 1, 1–8. doi:10.1155/2008/143728.
Safont, G., Salazar, A., Soriano, A., Vergara, L., 2012. Combination of multiple detectors for EEG based biometric identification/authentication. In: IEEE International Carnahan Conference on Security Technology, pp. 230–236. doi:10.1109/CCST.2012.6393564.
La Rocca, D., Campisi, P., Vegso, B., Cserti, P., Kozmann, G., Babiloni, F., Fallani, F.D.V, 2014. Human brain distinctiveness based on EEG spectral coherence connectivity. IEEE Trans. Biomed. Eng. 61 (9), 2406–2412. doi:10.1109/TBME.2014.2317881.
Marcel, S., Milla'n, J.D.R., 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Trans. Pattern Anal. Mach. Intell. 29 (4), 743–752. doi:10.1109/TPAMI.2007.1012.
Hema, C.R., Paulraj, M.P., Kaur, H., 2008. Brain signatures: A modality for biometric authentication. In: International Conference on Electronic Design, pp. 1–4. doi:10.1109/ICED.2008.4786753.
Ravi, K.V.R., Palaniappan, R., 2005. Leave-one-out authentication of persons using 40Hz EEG oscillations. In: International Conference on Computer as a Tool, 2, pp. 1386–1389.
Palaniappan, R., Mandic, D.P., 2007. Biometrics from brain electrical activity: A machine learning approach. IEEE Trans. Pattern Anal. Mach. Intell. 29 (4), 738–742. doi:10.1109/TPAMI.2007.1013.
Ruiz-Blondet, M.V., Jin, Z., Laszlo, S., 2016. CEREBRE: A novel method for very high accuracy event-related potential biometric identification. IEEE Trans. Inf. Forensics Secur. 11 (7), 1618–1629. doi:10.1109/TIFS.2016.2543524.
Nakanishi, I., Fukuda, H., Li, S., 2013. Biometric verification using brain waves toward on-demand user management systems: Performance differences between divided regions in α–β wave band. In: 6th International Conference on Security of Information and Networks, pp. 131–135. doi:10.1145/2523514.2523536.
Karayama, H., 2014. Outdoor EEG personal authentication. Intell. Inf. Wearable BMI Oper. 26 (2), 606–616.
Ishikawa, Y., Yoshida, C., Takata, M., Joe, K., 2014. Validation of EEG personal authentication with multichannels and multi-tasks. In: International Conference on Parallel and Distributed Processing Techniques and Applications, 2, pp. 182–188.
Ishikawa, Y., Yoshida, C., Takata, M., Kamo, H., Joe, K., 2015. A personal classification method using spatial information of multi-channel EEG. In: International Conference on Parallel and Distributed Processing Techniques and Applications, 1, pp. 229–235.
Ishikawa, Y., Nishibata, K., Takata, M., Kamo, H., Joe, K., 2017. Validation of EEG Authentication Accuracy with Electrode Slippage. In: International Conference on Parallel and Distributed Processing Techniques and Applications, pp. 302–308.
TajDini, M., Sokolov, V., Kuzminykh, I., Shiaeles, S., Ghita, B., 2020. Wireless sensors for brain activity—A survey. Electronics 9 (12), 1–26. doi:10.3390/electronics9122092.
Jasper, H.H., 1958. The ten twenty electrode system of the international federation. Electroencephalogr. Clin. Neurophysiol. 10, 371–375.
Klem, G.H., Lüders, H.O., Jasper, H.H., Elger, C., 1961. The ten twenty electrode system: International federation of societies for electroencephalography and clinical neurophysiology. Am. J. EEG Technol. 1 (1), 13–19.
Saeidi, M., Karwowski, W., Farahani, F.V., Fiok, K, Taiar, R, Hancock, PA, Al-Juaid, A., 2021. Neural Decoding of EEG Signals with Machine Learning: A Systematic Review. Brain Sci 11 (11), 1525. doi:10.3390/brainsci11111525.
Shams, T.B., Hossain, M.S., Mahmud, M.F., Tehjib, M.S., Hossain, Z., Pramanik, M.I., 2022. EEG-based Biometric Authentication Using Machine Learning: A Com-

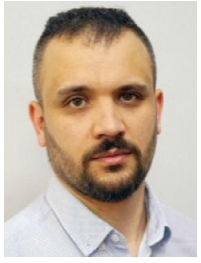
prehensive Survey. ECTI Transactions on Electrical Engineering, Electronics, and Communications 20 (2), 225–241. doi:10.37936/ecti-eec.2022202.246906.

Costantini, G., Todisco, M., Casali, D., Carota, M., Saggio, G., Bianchi, L., Abbafati, M., Quitadamo, L., 2009. SVM Classification of EEG Signals for Brain Computer Interface. Frontiers in Artificial Intelligence and Applications 204, 229–233. doi:10.3233/978-1-60750-072-8-229.

Costantini, G., Casali, D., Carota, M., Saggio, G., Bianchi, L., Abbafati, M., Quitadamo, L., 2009. Mental task recognition based on SVM classification. In: 3rd International Workshop on Advances in Sensors and Interfaces. IWASI, pp. 197–200. doi:10.1109/IWASI.2009.5184795.

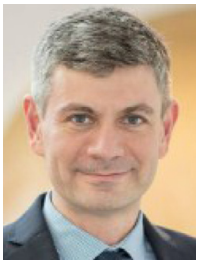
Wang, J.; Gao, L.; Zhang, H.; Xu, J. Adaboost with SVM-Based Classifier for the Classification of Brain Motor Imagery Tasks. In: Stephanidis, C. (eds) *Universal Access in Human-Computer Interaction. Users Diversity. UAHCI 2011. Lecture Notes in Computer Science,* 2011, vol. 6766. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21663-3_68.

Mahyar TajDini Ph.D. Candidate at The National Academy of Sciences of Ukraine and received the B.S. degree in Cyber security from State university of Telecommunication in Kyiv, Ukraine Microsoft Certified Professional (MCP) Since 2007 MCSA, MCSE, MCTS, MCITP, Azure Security Engineer Associate, Hacking Forensic Investigator (CHFI v10), EC-Council Certified Incident Handler (ECIH v2), CCNP R&S, CCNP Security and ISO 27001 Lead Auditor



Volodymyr Sokolov received Ph.D. degree in IT in 2019 at the Institute of Telecommunications and Global Information Space, Ukraine. He acquired his first research and teaching experience from 2005 to 2018 at the State University of Telecommunications, Ukraine. Since the end of 2018, he has been teaching security and information security courses at the Borys Grinchenko Kyiv University, Ukraine. Together with his Ph.D. students, he researches the issues of wireless security, speech recognition, and brain waves. Dr. Sokolov is the editor of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, is on the editorial board of the journal "Cybersecurity: Education, Science, Technique" (ISSN: 2663-4023), and also is the reviewer of the IEEE Problems of Infocommunications Science and Technology conference.

Ievgeniia Kuzminykh received the Ph.D. degree in telecommunications in 2013 from the Kharkov National University of Radio Electronics where she is currently a Visiting Associate Professor with the department of infocommunication. From 2017 to 2020, she was a Senior Lecturer with the computer science department in Blekinge Institute of Technology, Sweden. She was holding joint appointment as postdoc researcher with the Technical University of Denmark in 2019-2020. From July 2020 she is Lecturer in Cybersecurity Education with King's College London. She has coauthored over 40 publications. Her research interests include cybersecurity, IoT, security aspects of cloud and networks. Dr. Kuzminykh has served for various conferences and journals as a reviewer (IEEE Trans. on Cloud Computing, Hindawi Journal of Security and Communication Networks, MDPI Journal of Applied Sciences, Acta Innovation Journal, IEEE conference Problems of Infocommunications Science and Technology).



Bogdan Ghita received his PhD in 2005 from University of Plymouth, UK. He is Associate Professor at University of Plymouth and leads the networking area within the Centre for Security, Communications, and Network research. His research interests include computer networking and security, focusing on the areas of network security, performance modelling and optimization, and wireless networking, published over 150 papers, graduated 20 PhD students, and having been principal investigator in a number of industry-led, national, and EU research projects in these areas. He was a TPC member for over 100 international conference events as well as a reviewer for IEEE communications letters, computer communications, and future generation computer systems journals.