Towards Enhanced EEG-based Authentication with Motor Imagery Brain-Computer Interface

Bingkun Wu, Weizhi Meng, and Wei-Yang Chiu
SPTAGE Lab, DTU Compute, Technical University of Denmark, Kgs. Lyngby, Denmark
s210318@student.dtu.dk;{weich,weme}@dtu.dk

ABSTRACT

Electroencephalography (EEG) is the record of electrogram of the electrical activity on the scalp typically using non-invasive electrodes. In recent years, many studies started using EEG as a human characteristic to construct biometric identification or authentication. Being a kind of behavioral characteristics, EEG has its natural advantages whereas some characteristics have not been fully evaluated. For instance, we find that Motor Imagery (MI) brain-computer interface is mainly used for improving neurological motor function, but has not been widely studied in EEG authentication. Currently, there are many mature methods for understanding such signals. In this paper, we propose an enhanced EEG authentication framework with Motor Imagery, by offering a complete EEG signal processing and identity verification. Our framework integrates signal preprocess, channel selection and deep learning classification to provide an end-to-end authentication. In the evaluation, we explore the requirements of a biometric system such as uniqueness, permanency, collectability, and investigate the framework regarding insider and outsider attack performance, cross-session performance, and influence of channel selection. We also provide a large comparison with state-of-the-art methods, and our experimental results indicate that our framework can provide better performance based on two public datasets.

CCS CONCEPTS

• **Security and privacy** → Biometrics.

KEYWORDS

EEG, Biometrics, Time Series Classification, Deep Learning, Authentication

1 INTRODUCTION

With the rapid development of smart cities, biometric authentication receives more attention and opportunities [38]. Biometrics can be generally divided into two categories [45]: a) Physiological characteristics are inherent properties of human body such as fingerprint, palm veins, face recognition and iris recognition. b) Behavioral characteristics are related to the pattern of behavior of a person, including signature, voice and EEG. In real life, there are already many identity recognition or authentication systems constructed using physiological characteristics, such as payment systems based on facial recognition [52]. Behavioral biometrics is designed to complement the former system, such as EEG biometric, which has many advantages.

Physiological characteristics such as fingerprints or faces can be forged [10] and may suffer from spoofing attacks [17]. EEG signal is highly emotional state dependent so anomalies will be detected under coercion situations [24]. Users are unlikely to pass authentication if they are threatened. Similarly, EEG signals cannot be forcibly acquired like body tissues or generated from places other than the subject's brain. Among all the biometrics, EEG can reach 83 bits entropy for shallow classification [41]. The uniqueness, collection, and persistence of EEG biometrics towards authentication needs to be proved [24]. The performance of some models, which have been shown to be more efficient at utilizing EEG information in other domains, has not been systematically studied on this task [3].

Motivation. In cryptography protocols, authentication is a process to prove or disprove a claimed identity while identification aims to determine who the user is. Plenty of studies adopted EEG biometric to construct identification systems, trying to classify signals to all subjects in the system [11]. However, most studies on identification ability of EEG biometric confined the subject number under 50 and this is insufficient to claim the uniqueness of EEG. By increasing 10 subjects, the identification accuracy would even decrease up to 9% [49]. In real life scenario, security system needs to serve a large set of individuals. In order to mitigate this impact of subject amount, an authentication system is more practical compared with identification when managing access to protected properties.

EEG-based authentication has a variety of acquisition protocols. Subjects are designed to perform different mental tasks and produce characteristic EEG signals. The selected task can affect the accuracy of authentication. Rest state signal needs no external stimuli but is sensitive to artifacts and environmental noise. Visual stimuli can meet the permanency requirements of biometric but it requires the support of external equipment and synchronization. Also, individual's familiarity for visual stimulation is easy to be confused [11].

Motor Imagery requires the subject to imagine physical movements [15]. This task allows the subject to be more concentrated without being disturbed by environmental factors. In addition, due to the potential of Motor Imagery in improving exercise and assisting stroke patients, the understanding of such EEG signals has been extensively studied. This not only allows patients who use Motor Imagery-based exercise assistance to be more directly authenticated

ACSAC, December 5–9, 2022, Austin, TX, USA

ACM ISBN 978-1-4503-9759-9/22/12…$15.00
https://doi.org/10.1145/3564625.3564656

by their devices, but also can transplant many of the Motor Imagery classification methods for identity authentication [3].

Contributions. Motivated by the above, in this work, we propose an enhanced EEG authentication framework with Motor Imagery. The EEG processing contains signal preprocessing, channel selection and classification. In the preprocessing stage, the signal is segmented according to the task interval, and artifacts in the signal are removed. The purpose of channel selection is to find the channels the most relevant to event related potential to reduce the number of electrodes that need to be processed [18]. This reduces the requirements for equipment and software. There are many classifiers based on traditional machine learning methods or shallow methods [16]. Although they also have good performance, they mainly rely on manually extracted features. In recent years, more and more deep learning classifiers have been applied in this field. In particular, the classifiers in the Motor Imagery field for brainwave signals to categorize different limb movements can well extract temporal, spatial and spectral characteristics from the motion signal.

Our contributions can be summarized as below.

- Our proposed EEG authentication framework consists of three key components:
  - **ICA Artifacts Removal.** Blind source separation (BSS) is conducted on the raw signal to separate sources according to different statistical features of artifacts and obtain input composed of all brain electrical signals.
  - **Channel Selection.** The channel selection method is based on effective connectivity. When the body movement is imagined, the causality of the signal in different electrodes is analyzed to retain the channel as the cause.
  - **Deep Learning Classification.** The feature extraction and classification can refer to the method of Motor Imagery decoding to fully extract the frequency, space and multi-mode temporal features of EEG. Through the feature extraction of the convolution layer, the input can be directly classified as bona fide presentation or attack presentation.
- In the evaluation, we consider two public and popular datasets (Physionet and BCI dataset) and provide a large comparison with 9 similar studies and methods. In addition, we also investigate insider attack and outsider attack performance, cross-session performance and the influence of channel selection. The results indicate that our proposed EEG authentication framework can perform two-class classification accurately and outperform the other state-of-the-art methods.

The rest of the paper is organized as follows. Section 2 introduces the state-of-the-art EEG-based authentication methods. Section 3 details our proposed EEG authentication framework including signal preprocessing, channel selection and deep learning classification. Experimental configuration and result analysis are given in Section 4 and Section 5, respectively. A discussion is provided in Section 6. Finally, Section 7 concludes our work.

2 RELATED WORK

For the EEG authentication system, the tasks, features, and classification methods used in past research are very extensive. A summary and evaluation of all these systems can be found in the survey [24].

EEG tasks are also known as acquisition protocols. Those protocols greatly affect the quality of data and user experience. Resting state is a very popular acquisition protocol because it requires minimal user and setup requirements [26, 39]. However, such acquisition methods are easily disturbed by environmental factors. Hence some complex protocols introduce more focused tasks on the attention of participants. Visual Evoked Potential (VEP) is the EEG signal caused by visual stimuli. In [21], texts are presented for individuals to read silently. Zeng *et al.* [56] utilized the P300 ERP triggered by Rapid Serial Visual Presentation (RSVP). The familiarity of different individuals with different pictures was also used to generate EEG signals containing discriminative information [11]. There is also a class of protocols that contain mental tasks. For example, Motor Imagery or actual body movements belong to mental tasks [15, 34]. More and more tasks have been introduced for designing EEG biometric systems, such as the N-back tasks [43].

The main purpose of acquisition protocols is to include EEG traits in the data that are easier to separate and optimize the user experience. Appropriate algorithms are expected to make better use of these features for classification. Some traditional machine learning methods require handcrafted features. Kumar *et al.* [27] extracted statistical features from EEG data and feeded into Support Vector Machine (SVM) and Hidden Markov Model (HMM) classifier. Alyasseri *et al.* [4] designed an identification system based on SVM classifier with a Radial Basis Function kernel. Omerhodzic *et al.* [36] and Sharma and Vaish [28] concentrated on the energy distribution feature of EEG signal and selected Neural Network as their classifier. Jayarathne *et al.* [25] adopted Common Spatial Patterns (CSP) values as feature and Linear discriminant analysis (LDA) as classification algorithm. In addition, many research studies also pay attention to the consistency of feature classification in different sessions. Maiorana and Campisi [32] proved that discriminative traits with HMM classifier can conquer aging effect over long-term periods. Similarly, Das *et al.* [14] focused on the longitudinal study, and evaluated the discriminative capabilities of generic visually-evoked potentials (VEPs) and visual event-related potentials (ERPs) associated to specific cognitive tasks. Armstrong *et al.* [7] provided an example of assessing the uniqueness, collectability, and permanence of traits from the Event-Related Potential (ERP).

Deep learning methods have also been introduced for classifying Motor Imagery data for EEG authentication. Most of them are CNN-based with an end-to-end framework using automatic feature extraction. The Motor Imagery CNN (MI-CNN) method [15] is a representative that could achieve a classification accuracy higher than 98%. Sun *et al.* [47] enhanced the CNN with a recurrent structure aiming to handle the time series of Motor Imagery data. Some deep learning methods also tried to solve longitudinal immutability. For instance, Ozdenizci *et al.* [37] proposed an adversarial inference approach to learn session-invariant person-discriminative representations that can provide robustness in terms of longitudinal usability. Table 9 (Appendix) provides a comprehensive summary about the related studies.

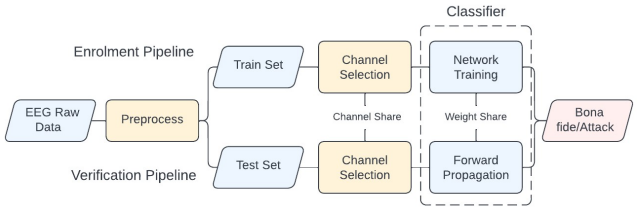

Figure 1: The flowchart of the proposed authentication framework.

Among the BCI systems, Motor Imagery has been widely studied. In recent years, methods based on deep learning have been used more for EEG information analysis related to Motor Imagery. The review of [3] summarized deep learning methods for Motor Imagery content understanding and classification in recent years. The classification method used to understand the meaning of Motor Imagery movements is of great significance for authentication based on the same signal. CP-MixedNet [30] was identified by the mixed-scale convolutional block from temporal aspect. The FBC-Net [33] then combined the concept from [6] to draw attention on the spectral aspect. Tabar and Halici [48] investigated CNN and stacked autoencoders (SAE) to classify EEG Motor Imagery signals. Ingolfsson *et al.* [22] further improved the classification performance. Transformer-based methods [46] were recently introduced for EEG classification.

Channel Selection is also an important aspect for EEG authentication. Varsehi and Firoozabadi [50] first introduced a method of channel selection based on Granger causality (GC) analysis. In addition to this hypothetical approach based on brain connectivity, Alyasseri *et al.* [4] defined the problem as a NP-hard problem and designed a binary version of the Grey Wolf Optimizer (BGWO) to find an optimal solution.

3 OUR PROPOSED FRAMEWORK

3.1 Framework Overview

The flowchart of our proposed authentication framework is depicted in Figure 1. Our proposed framework incorporates an effective preprocessing method and a deep learning classifier. Also, in order to reduce system complexity and extract the most influential electrode channels, a channel selection method is added before classification. This section will introduce these three modules theoretically to help understand how invalid signals are eliminated, the modeling of cortical signals and how deep learning models can extract sufficient features from a limited amount of data.

It is worth noting that the EEG authentication system is trained for each subject, which means a subject owns private selected channels and weights of deep learning classifier. The selected channel for each subject is shared between training data and testing data. A subject's model contains its own selected channels and deep learning weights.[1]

[1]The source code of our framework is available at: https://github.com/BKAUTO/EEG-Biometric.

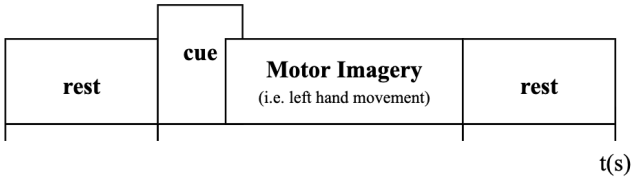

Figure 2: The timing scheme of a trial in Motor Imagery.

3.2 Preprocessing

3.2.1 Segmentation. In the Motor Imagery task, the multi-channel EEG data collected by non-invasive equipment is generally labeled, which means that the data at each moment corresponds to a state, which generally includes rest state, cue state, and imaging state. After seeing the cue, the subject needs to imagine a specific limb movement according to the instructions. In a trial that includes rest, cue, and imagination, we only intercept a fixed-length time series based on the label as our original EEG data. The timing scheme for one trial is illustrated in Figure 2. In one trial, the user performs one imagination, and there is a period for rest before and after the imagination. The cue generally refers to a symbol prompt from, for example, a computer monitor, prompting the user to start the imagination.

Typically, the length of imagination period is around 4s. If considering a sample frequency of 250Hz, then the time series segment would have a length around 1000 samples for each trial.

3.2.2 Artifact Removal. The raw EEG data generally contains noise and artifacts caused by eye blink, cardiac activity and muscle movement [42]. Blind source separation (BSS) technique is proved to be effective in automatic artifact removal. Signals from different sources such as artifacts and EEG signals can be separated by this type of technology. Independent Component Analysis (ICA) is a representative method, assuming that time series recorded on scalp are spatially mixtures of temporally independent neurological and artifactual sources. All the electrodes record a linear summation of potentials from spatial distributed positions on scalp.

It is argued that ocular activity tends to have higher power, and muscle activity contains a higher frequency than EEG [13]. Let E denote the raw EEG signal of shape $(channels \times trails \times samples)$. E is assumed to be a linear mixture of source S and white noise N [23].

$$E = A \times S + N \tag{1}$$

A is the matrix expressing the linear combination of sources, and the inverse $W = A^{-1}$ is therefore the unmixing matrix to separate the sources.

$$S' = W \times E \tag{2}$$

The core problem here is how to identify sources other than EEG signals from all sources and eliminate them to obtain S'_{clean} that removes artifacts. **Algorithm 1** shows the K-means and ICA artifact removal.

This work combines clustering with ICA to distinguish between suspected artifacts and EEG sources [31]. The ICA is applied to each trial to derive ICA components, which are the various sources. Multiple statistical descriptors are considered, such as variance,

Algorithm 1 K-means and ICA artifact removal

1: Raw EEG data of shape $(N_{trial} \times N_{channel} \times N_{sample})$, N_{trial}—number of trials, $N_{channel}$—number of channels, N_{sample}—number of time samples
2: **for** $i = 1, 2, \ldots, N_{trial}$ **do**
3: Z-score normalization of each trial
4: **end for**
5: Reshape EEG data to a matrix of $(N_{channel} \times N_t)$ where $N_t = N_{trial} \times N_{sample}$.
6: Calculate ICA linear combination matrix W, using the Picard ICA algorithm.
7: Calculate ICA components of sources $S' = WK \times E$, K is the whitening matrix.
8: Derive descriptors, including variance, amplitude, range, max derivative, kurtosis, entropy, mean local variance and mean local skewness of each ICA component.
9: Utilize K-means clustering based on above features into two classes. Class with less components is considered as suspected artifacts.
10: Remove two components with highest variance by setting corresponding rows of S', the S'_{clean} is derived.
11: Reconstruct EEG data $E_{clean} = K^{-1}W^{-1}S'_{clean}$

maximum amplitude, range of the signal amplitude, max first derivative, kurtosis, shannon entropy, mean local variance of time intervals of 1s and 15s duration, and mean local skewness of time intervals of 1s and 15s duration [53]. It is followed by a k-means cluster based on these features. ICA components are clustered into two classes, suspected artifacts and original EEG. Two components with the highest variance are removed and the components are unmixed to reconstruct the multi-channel EEG data.

3.3 Channel Selection

3.3.1 Brain Connectivity. The current brainwave acquisition setup uses an average of more than 30 electrodes, and some can reach more than 60 [24]. In order to improve *Collectability*, channel selection is used to choose the most relevant electrodes for a specific task. This assumes that some channels have a more significant impact on the specific functions of EEG than other channels. This technique can make brainwave acquisition equipment more user-friendly in practice.

Our work conducts the channel selection based on brain connectivity. In particular, brain connectivity refers to a pattern of anatomical links (anatomical connectivity), statistical dependencies (functional connectivity) or causal interactions (effective connectivity) between distinct units within a nervous system.

Compared with functional connectivity, less interest is shown on the classification of brain areas as it mainly relies on effective connectivity. Effective connectivity is defined as the influence that a node exerts over another under a network model of causal dynamics. When the subject performs Motor Imagery, some neural nodes are the causes of potentials, and other secondary nodes are stimulated in time sequence, which establishes a causal model. An observed time series $x_j(n)$ Granger-causes another series $x_i(n)$, if knowledge of $x_j(n)'s$ past significantly improves prediction of $x_i(n)$ [20]. Evaluating the extent of Granger causality provides a measure of the strength of causal interaction between nodes in neural structure.

3.3.2 Partial Directed Coherence. Here partial directed coherence (PDC) [9] is applied to describe the direction of information flow based on Granger causality. First it is necessary to construct a multivariate autoregressive model (MVAR). After that, the least square method is adopted to solve the model coefficients and error coefficients. Then the AR model is converted to the frequency domain by Laplace transform to obtain the PDC value.

Autoregressive model (AR) is a linear regression model that uses the linear combination of random variables at several moments in the previous period to describe the random variables at a certain moment in the future. It is a common form of time series. Assuming a MVAR:

$$x_i(n) = \sum_{i=1}^{p} a_{id} x_i(n-i) + e_i(n) \tag{3}$$

a_{id} represents the coefficient of the i-th channel to the d-th channel, e is the deviation. $x_i(n)$ represents the variable state value at time n. p represents the order of building the model that can be selected by Bayesian information criterion (BIC) [51]. The predictive model can be solved by only requiring the coefficient state quantity a_{id} and the error e. The transpose of Equation (3) is shown as below,

$$X^T(n) = \sum_{i=1}^{p} X_i^T(n-i) a_{id}^T + E^T(n) \tag{4}$$

$X^T(n)$ is the discrete samples at time n while $E^T(n)$ is the deviation matrix. Let

$$D = \begin{bmatrix} X_1^T & \ldots & X_{p_{m+1}}^T \\ \ldots & & \ldots \\ X_{N-p_m}^T & \ldots & X_{p_m}^T \end{bmatrix} \tag{5}$$

p_m is the maximum order of predictive model of MVAR. Then Equation (4) can be converted to

$$Y = DA \tag{6}$$

Since $D^T D$ is a symmetric square matrix, the coefficients of MVAR can be solved as

$$\begin{aligned} A &= (D^T D)^{-1} D^T Y \\ E &= X_i - \sum_{i=1}^{N} a_{id} X_i(n-i) \end{aligned} \tag{7}$$

A represents the coefficients of the forecast time series, and E represents the coefficients of the forecast error series.

After fitting the coefficient $A(r)$ of MVAR by the least square method, it is converted to the frequency domain by Laplace transform.

$$A_{ij}(f) = I - \sum_{r=1}^{p} a_{ij} e^{-\pi i r f} \tag{8}$$

Algorithm 2 PDC-based Channel Selection

1: Artifact removed EEG data of subject s of shape ($N_{trial} \times N_{channel} \times N_{sample}$)
2: **for** $i = 1, 2, \ldots, N_{trial}$ **do**
3: To calculate PDC matrix ($N_{channel} \times N_{channel}$) for i-th trial.
4: To derive the mean for each column, which represents the PDC from j-th channel to all the channels.
5: To sort and return the maximum M mean PDC value channels.
6: **end for**
7: To select M most frequent channels in N_{trial} trials.

Then the partial directed coherence (PDC) value from j-th channel to i-th channel is

$$P_{ij}(f) = \frac{A_{ij}(f)}{\sqrt{a_j^H(f)a_j(f)}} \tag{9}$$

H means conjugate transpose, $A_{ij}(f)$ is the coefficient of the i-th row and the j-th column.

$$A_{ij}(f) = \begin{cases} 1 - \sum_{i=1}^{p} a_{ij}(r)e^{-i2\pi fr} & i = j \\ \\ -\sum_{i=1}^{p} a_{ij}(r)e^{-i2\pi fr} & i \neq j \end{cases} \tag{10}$$

Note the normalization properties as below:

$$\begin{aligned} 0 \leq |P_{ij}(f)|^2 \leq 1 \\ \sum_{i=1}^{N} |P_{ij}(f)|^2 = 1 \end{aligned} \tag{11}$$

PDC value describes the intensity of the causal action from the j-th channel to the i-th channel. When $i = j$, PDC represents the influence of the past value of $X(n)$ on the current value.

3.3.3 PDC-based Channel Selection. The idea is based on the influence of some specific EEG channels while measuring the causality of these channels onto others. In addition, these selected channels are different for each subject. This is because the brain function connection network generated by each person during Motor Imagery activity is different. This can also be used as an additional factor to strengthen the authentication ability. For the j-th channel, its PDC values for all other channels are calculated and averaged to measure the possibility of the j-th channel being a cause channel and affecting other channels.

The channel selection is applied to each trial for each subject and the most frequent selected channels are considered as the cause channels of one particular subject, as shown in **Algorithm 2**.

3.4 Deep Learning Classification

The deep learning framework is modified from the Motor Imagery decoding task. This task focuses on classifying Motor Imagery trials as corresponding limb movements, but some of the adopted methods have good generalizability in extracting time series features.

FBCNet [33] extends the deep convolution structure to the classic FBCSP [6] method. Motivated by this, we develop a hybrid temporal feature extraction structure to further enrich the basis of the classifier. The deep learning framework mainly consists of four stages:

(1) *Filter-bank spectral decomposition*: Multiple narrow-band filters are applied to the EEG data to decompose different frequency bands. Different frequency bands are then input into the convolutional network in parallel to obtain multi-band characteristics.
(2) *Spatial convolution*: The convolution kernel slides in the channel dimension to communicate the feature distribution among different electrodes data.
(3) *Mixed temporal feature extraction*: Two kinds of temporal characteristic are concatenated. Temporal feature is inferred from variance layer and standard convolution layer along time axis.
(4) *Classifier*: The feature map is flattened and input into a fully connected layer.

The original data is firstly decomposed into different frequency intervals to obtain spectro-spatial features. These features pass through the parallel conventional & convolutional layer and variance layer to finally obtain spectro-spatial-temporal features. Finally, feature maps are expanded into one-dimensional vectors and mapped into two categories: Bona fide access and Attack access. The architecture of our framework is illustrated in Figure 3.

1) Multi-Frequency Representation by Filter Bank: Considering the input EEG data as $E = \{(X_i, y_i)|i = 1, 2, ..., n\}$. The i-th trial EEG sample is $X_i \in \mathbb{R}^{C \times S}$ and the corresponding label is $y_i \in \{0, 1\}$, where 0 denotes the attack access and 1 denotes the bona fide access. C represents the channel number and S represents time points of one single trial.

There are several significant frequency bands in EEG signal, including δ (1-3Hz), θ (4-7Hz), α (8-13Hz), β (14-30Hz), etc. Below the power line noise - 60Hz, the frequency is divided into 9 non-overlapping frequency intervals from 4Hz to 40Hz, and the bandwidth of each frequency band is 4Hz [33]. Each frequency band is obtained by a narrow-band filter. As a result, the i-th trial high-frequency EEG signal can be deconstructed into 9 different frequency band signals, $X_{FB} \in \mathbb{R}^{B \times T \times S}$. $B = 9$ represents the number of narrow-band filters and frequency bands. The subsequent convolution operation is performed on $B = 9$ signals in order to extract features corresponding to different spectral intervals.

2) Spatial Feature Aggregation: Each frequency band is followed by a spatial convolution block. The spatial convolution is responsible for connecting features from different electrodes across the scalp. The core component is $m = 32$ kernels of size $(C, 1)$ where C represents the number of channels. This is also called a Depth-wise Convolution Layer. Information from all the channels for each frequency band is assigned with different weights and aggregated. The rest configurations of spatial convolution block are identical to FBCNet [33].

The output feature map is $X_{SC} \in \mathbb{R}^{(m \times B) \times 1 \times S}$, where channels are aggregated in multiple filters.

3) Mixed Temporal Feature: Temporal features can be extracted in different manners including pooling, convolution and other operations. In [30], a parallel structure of regular and dilated convolution is applied for generating two groups of feature maps containing different scales of temporal information. Inspired by this, the mixed

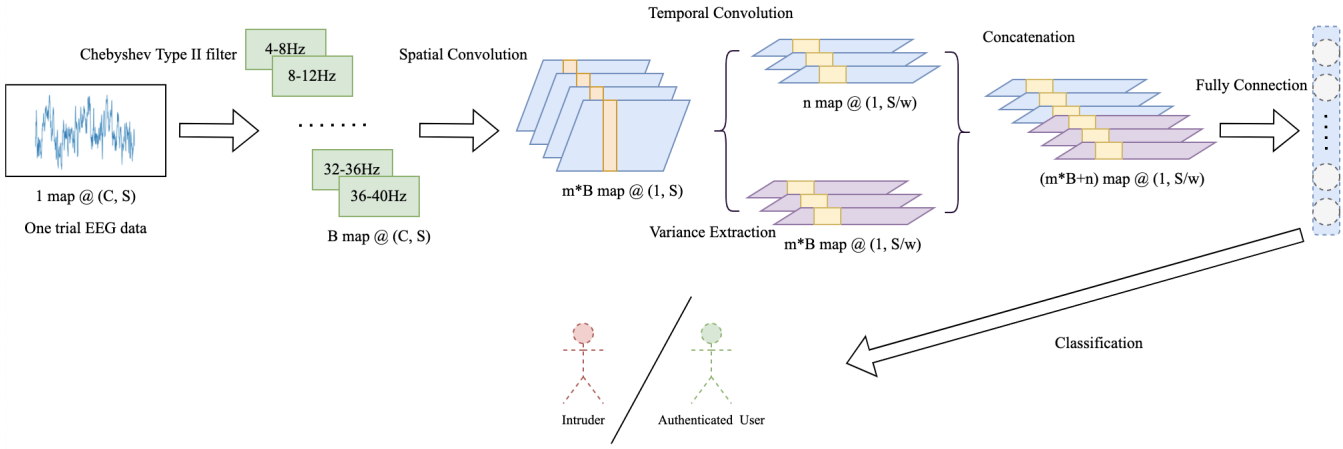

Figure 3: Modified Network architecture. (C: number of channels, S: number of samples, B: number of frequency bands, m: number of spatial kernels per frequency band, n: number of temporal convolution kernels in total, w: length of temporal convolution kernel)

temporal feature block adopts both regular temporal convolution and variance layer in parallel. The strategy is using a medium-sized convolution filter $(1 \times w/p)$ to extract features and a small max pooling window $(1 \times p)$ to select representative features. This means that the kernel extracts features from non-overlapping segments of time points. The output feature map of regular convolution is of size $X_{RC} \in \mathbb{R}^{n \times 1 \times S/w}$ where $n = 28$ is the kernel number for all the frequency bands.

In addition to regular temporal convolution, a variance layer is applied to extract discriminative traits in EEG signal [33]. It is assumed that different individuals generate distinguishable power spectrums. Therefore, local variance is calculated in non-overlapping windows.

$$x_{var}(k) = \frac{1}{w} \sum_{t=w*k}^{(k+1)*w-1} (X_{SC}(t) - \mu(k)) \tag{12}$$

$\mu(k)$ is the mean value of the k-th window. k has a range of $[0, S/w]$. For the power differs among different frequencies, the variance calculation is associated with each frequency band. The output feature map is therefore $X_{var} \in \mathbb{R}^{(m \times B) \times 1 \times S/w}$ and the last two dimensions are identical to X_{RC}.

X_{RC} and X_{var} are concatenated to compress temporal shape characteristic and power characteristic together. The final feature map X_T can be denoted using a concatenating function $\tilde{H}(\cdot)$.

$$X_T = \tilde{H}([X_{RC}, X_{var}]) \tag{13}$$

4) Classification: The concatenated feature map is flattened into a vector. The fully connected layer is applied for connecting all the activations of spectro-spatial-temporal features. The probability of 2 classes are given by softmax layer and the whole network is trained by negative log likelihood loss.

4 EXPERIMENTAL DESIGN

In this section, we aim to verify the actual performance and potential problems of the proposed framework. Our evaluation mainly uses two public datasets, their acquisition methods and data styles have certain commonalities, and they were widely used in many other research studies. This contributes to the standardization of data collection in the EEG authentication system.

The framework is tested with a single factor authentication security model, which means that Biometrics is the only defense. Our threat model partially follows the protocol from some other biometric research like [54] [55]. Attackers are assumed to have the same prior knowledge and behavioral abilities as normal users. Inspired by intra-test and inter-test in other studies, we defined insider attack and outsider attack. For an insider attack, the attacker is one of the system users with template enrolled, while trying to impersonate other users. For an outsider attack, the attackers come from outside the registered users with no template enrolled.

4.1 Dataset

We selected two datasets to conduct the experiment. The Physionet EEG Motor Movement/Imagery Dataset contains a large number of subjects, which can be used to test the robustness of the framework towards a large number of users. The reason for involving BCI competition IV-dataset is that it contains samples from different days, which can be used to evaluate the Longitudinal performance of the framework.

1) Physionet EEG Motor Movement/Imagery Dataset [19]: This dataset is recorded using the BCI2000 system [44]. The subject is required to perform either real movement or imagination of opening and closing fists or feet. The experiment only selects trials for imagination tasks, including:

(1) imagine opening and closing left or right fist.
(2) imagine opening and closing both fists or both feet.

Cues appear on the screen as instructions so that the subject should perform the corresponding tasks. The sampling rate was

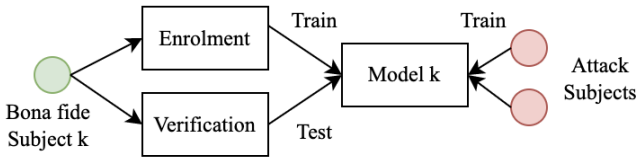

Figure 4: The deep learning model is trained for each subject.

160Hz and the data was acquired in 64 channels. Data of 109 subjects is available and each subject performed 6 runs of 15 trials in one session. Subject 88 and 92 were excluded for data completeness reason. In the experiment, the signal with a duration of 4s in the imagination phase was intercepted as a trial EEG data.

2) BCI competition IV-dataset 2a[2]: The dataset is also recorded using a cue-based BCI paradigm. The subject is required to perform four different motor imagery tasks, including:

(1) imagine movement of the left hand.
(2) imagine movement of the right hand.
(3) imagine movement of both feet.
(4) imagine movement of tongue.

The data is acquired in 22 channels and the sampling rate is 250Hz. This dataset convened a smaller number of volunteers. Up to 9 subjects performed 6 runs of 48 trials for each in one session. Two sessions on different days were recorded. Although the small number of subjects limits the persuasiveness of evaluation on this dataset, using different sessions for enrolment and verification can evaluate the permanency of the authentication system. The duration of 4.5s was used for one trial where the cue was prompted in the first 0.5s.

4.2 Protocol and Measurement

Individuals need to perform motor imagery tasks when registering biometric information and then performing authentication. The EEG data that executes a trial is a sample used for system training or testing. How many trials are executed in the enrolment phase can determine the accuracy, user-friendliness and usage time of the system. In principle, the fewer imaginations the user needs to perform during the enrolment and verification phase, the more it helps to improve the user-friendliness of the system, while at the same time maintaining acceptable accuracy.

Which body part (left hand, right hand, foot) the subject imagines in detail was mixed in the experimental data. The experiment aims to verify that all classes of motor imagery have universal characteristics that can distinguish subjects. As shown in Figure 4. One subject's deep learning model is trained by this subject's EEG data as Bona fide sample and several other subjects' data as attack samples. In the verification phase, the subject or the user also utilizes his corresponding model for verification. Each subject has an independently trained model for authentication, that is, we perform authentication instead of identification. When evaluating the performance of models corresponding to different subjects, we used the same attackers to achieve fairness in the evaluation.

The accuracy of the authentication system is mainly measured by Equal Error Rate (EER), which is a widely accepted metric in the performance measurement of biometric system. The EER is the location on a ROC or DET curve where the false acceptance rate and false rejection rate are equal. Besides, the time used for enrolment and verification, the parameters of deep learning are also recorded aiming to evaluate the user-friendliness of the authentication system.

4.3 Configuration

The ICA computation applies the Picard algorithm [1, 2]. The max iteration was set to 150 and the tolerance is 10^{-6}.

A trial contains a single imagination, which consists of consecutive values in the time domain.

For the Physionet dataset, one trial has 640 time points (4s). The temporal convolution filter has a length of $w/p = 32$ and the max pooling window has a length of $p = 4$. Therefore the time points of the trial data are reduced to $S/w = 5$. The variance layer calculates variance on a window of $w = 128$.

For the BCI dataset, one trial has 1125 time points (4.5s). The temporal convolution filter has a length of $w/p = 45$ and the max pooling window has a length of $p = 5$. Therefore the time points of the trial data are reduced to $S/w = 5$. The variance layer calculates variance on a window of $w = 225$.

The deep learning classifier was realized using Pytorch. Batch normalization and swish nonlinearity were used after each convolution layer. A dropout function of 0.5 probability was applied in temporal convolution aiming to prevent *overfitting*. The training process contains 300 epochs and the final classifier for each subject was selected in the last 50 epochs with the best accuracy. Learning rate is 0.001, and it is reduced to 0.1 times every 40 epochs.

For the Physionet dataset, the first four runs (60 trials) of each subject were used for training, and the last two runs (30 trials) were used for testing. For the BCI IV 2a dataset, two different sessions were used for training and testing, 96 trials per subject were used as bona fide samples, and 48 trials were used for attacks on other subject models.

5 RESULT ANALYSIS

This section discusses in detail the results obtained through experiments and analyzes the characteristics of our proposed authentication framework. Below are the main goals and observations in the evaluation:

- **Insider Attack Performance.** Subjects that provide attack samples during training can still be identified as attackers in the testing phase. The system could achieve an average EER below 1% using 10 channels under two protocols with different attacker numbers.
- **Outsider Attack Performance.** Subjects not present in training can still be classified as outliers (attackers) in the testing phase. The system could achieve an average EER below 1.3% using 10 channels under two protocols with different attacker numbers.
- **Cross-session Performance.** When the enrolment and the verification occur at different times, that is, the data used for training and the data collected in the testing phase are collected at different time periods, the system could still classify accurately. Either the attack comes from an insider

[2]https://www.bbci.de/competition/iv/

Table 1: The result of EER (%) for insider and outsider attack experiment on Physionet dataset.

Protocol		Subject										
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**avg**
Insider	EER-19	1.05	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.19	3.15	0.74
	EER-49	2.04	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.06	0.0	0.51
Outsider	EER-19	1.06	0.0	1.06	0.0	0.0	0.0	0.0	0.0	7.37	3.19	1.27
	EER-47	2.13	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.19	4.26	0.96

Table 2: Configuration of Insider Attack Experiment

Dataset	Trials	Channels
Physionet	60	10
Enrollment Time	**Verification Time**	**Model Parameters**
8-10 mins	4s	450,626

Table 3: Configuration of Outsider Attack Experiment

Dataset	Trials	Channels
Physionet	60	10
Enrollment Time	**Verification Time**	**Model Parameters**
8-10 mins	4s	450,626

Table 4: Configuration of BCI IV 2a Experiment

Dataset	Trials	Channels
BCI IV 2a	96	10
Enrollment Time	**Verification Time**	**Model Parameters**
14-18 mins	4.5s	450,626

or an outsider, the system could achieve an average EER below 0.3%.

- **Performance Comparison.** The proposed system outperformed selected baselines and SOTA methods under both insider and outsider attacks, especially when using a limited number of channels.
- **Influence of Channel Selection.** When reducing the number of used channels, the performance of authentication system could decrease to a certain extent, but it was still within the acceptable range. In particular, when the same channels are used for all subjects in the training phase, the performance of the system could still be maintained at 1%-2%.

5.1 Insider Attack Performance

The insider attack here refers to an attack on the authentication system from the subject (as an attacker) that has appeared in the training. This means that the system recognizes these attackers, and these attackers are other users who use the same system. When training the model of subject k, the data enrolled by these subjects is used as attacks.

For the insider attack experiment, two protocols were leveraged with the Physionet dataset. The bona fide data for training consists of 4 runs of 60 trials and the attack data consists of 19 or 49 subjects. Each attacker performs 5 trials for 19 attackers and 2 trials for 49 attackers. In the test, data from another two runs was used for bona fide and attack presentation.

Table 2 depicts the configuration and statistics under the insider attack experiment. The enrolment time contains the imaginations, 4s rest between two imaginations, and the optional rest between runs. The 60 trials were the bona fide samples of the subject of the model, which needed to be enrolled.

The performance for 10 subjects was recorded in the row of insider, as shown in Table 1. EER-19 represents the test EER for each subject's model with the same 19 attackers in training and testing. EER-49 represents the result of 49 attackers. It can be seen from the results that there are 7 subject models that can completely separate the bona fide presentation from the attack presentation, that is, to correctly classify honest visitors from visitors who falsely claim their identities. Although the EER of subject 9 and subject 10 exceeded 3%, the EER of subject 10 could decrease due to the addition of more attack samples. On average, using more attackers during training (the total training samples remain unchanged) can improve the performance of the system, which is in contrast to the identification system that was affected by the number of users.

5.2 Outsider Attack Performance

An outsider attack refers to an attack towards the system from the subject who has not appeared in the training. The authentication system does not know the attacker, so the characteristics of the attacker's data are completely unknown.

The same protocols for insider attack experiment were used for outsider attack experiment again. For EER-47, 49 subjects were used as attackers in the training and 47 attackers were used in the testing. Except for using different attackers in the testing and training phases, the remaining configurations of the experiment were consistent with the insider attack experiment. Table 3 depicts the configuration and statistics under the outsider attack experiment.

The performance for 10 subjects was recorded in the row of outsider, as shown in Table 1. It is found that subjects' model that performed well in the insider attack experiment could also better resist outsider attacks. However, when facing an unknown subject attack, the performance of the system could decrease to a certain extent compared with classifying known subjects. On average, an EER of no more than 2% is an acceptable performance of unknown attacks. Further, when the number of attackers used for training increases, the performance of the system will also be improved. The performance of EER-47 was better than EER-19, which is consistent with the situation of insider attacks.

5.3 Cross-session Performance

The BCI IV 2a dataset was used to evaluate the cross-session performance of the system. The bona fide data for enrolment consists of 96 trials per subject according to the configuration in Table 4. The testing data and the training data were extracted from two sessions from different days. The performance result is shown in Table 5.

Limited by the size of the dataset, each subject model has only 4 attackers for training or testing. Compared with using more attacker samples, the performance of the system in the face of outsider

Table 5: The result of EER (%) for insider and outsider attack experiment on BCI IV 2a dataset.

Protocol		Subject									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**avg**
Insider	EER-4	0.0	0.0	2.34	0.0	0.0	0.58	0.0	0.0	0.0	0.32
Outsider	EER-4	9.04	0.0	20.45	1.14	0.0	0.0	1.74	12.35	0.0	4.97

Table 6: Performance Comparison with Baseline and SOTA Methods on Physionet Dataset.

Method	Insider			Outsider		
	Mean Accuracy (%)	**Mean EER-19 (%)**	**Lowest Subject/EER-19**	**Mean Accuracy (%)**	**Mean EER-19 (%)**	**Lowest Subject/EER-19**
SVM[27]	90.63	6.73	10 / 13.68	91.44	5.785	3 / 24.21
HMM[27]	76	18.23	3 / 25.85	74	20.57	7 / 27.12
CSP_LDA	98.32	0.84	1 / 5.26	96.96	1.37	1 / 5.26
energyNN	82.6	15.47	5 / 19.17	80.23	17.98	9 / 24.23
MI_CNN[15]	84.96	11.88	6 / 26.08	80.56	15.02	6 / 25.27
CNN_LSTM[47]	78.2	17.89	7 / 24.54	76	19.12	7 / 26.25
EEGNet[29]	82.16	22.04	1 / 32.97	79.6	23.44	1 / 36.17
CP_MixedNet[30]	74.97	9.95	1 / 13.6	67.87	15	1 / 18.22
FBCNet[33]	98.02	1.45	3 / 4.34	96.12	1.98	7 / 6.23
Mixed_FBCNet_10	**99.48**	**0.74**	9 / 3.19	**98.89**	**1.27**	9 / 7.37

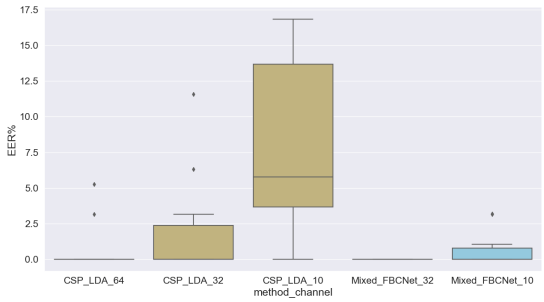

Figure 5: The EER-19(%) of CSP_LDA and Mixed_FBCNet using 64, 32 and 10 channels.

Table 7: Configuration of 32-channel Experiment

Dataset	**Trials**	**Channels**
Physionet	60	32
Enrollment Time	**Verification Time**	**Model Parameters**
8-10 mins	4s	457,622

attacks has dropped significantly, but the system could still give an average result of <1% EER when classifying known people.

5.4 Performance Comparison

We further provided a comparison with several selected representative algorithms in the literature. These methods include baselines for EEG authentication and Motor Imagery classification, as well as state-of-the-art methods. For instance, Kumar *et al.* [27] utilized SVM and HMM classifiers, which are two classic shallow methods. Mahajan *et al.* [32] proved that EERs below 2% could be achieved when comparing samples taken at temporal distances in the order of years. Time domain statistical features were added to such methods as handcrafted features that are similar to [27].

Jayarathne *et al.* [25] provided a representative baseline for the common spatial coherence feature, which was used frequently in spatial-frequency domain. Linear Discriminant Analysis (LDA) is another linear classifier, which is used when there are so many features with possibility of correlation. CSP feature is a good fit of LDA classifier. They particularly proposed an EEG-based biometric authentication system based on this method, which achieved a maximum accuracy rate of 96.97%.

In addition, Wavelet Transform (WT) is widely used as a powerful feature extractor regarding the non-stationary nature of EEG signals [24]. Sharma and Vaish [28] combined Wavelet decomposition with Motor Imagery task. Das *et al.* [15] and Sun *et al.* [47] proposed two novel deep learning based methods for resolving Motor Imagery EEG authentication. They could both achieve an accuracy rate around 99% in certain conditions.

EEGNet [29], CP_MixedNet [30] and FBCNet [33] are convolutional neural network-based BCI methods, which handle movement-related signals. More specifically, EEGNet has been configured as backbone in multiple SOTA methods as it can best encapsulate the well-known EEG feature extraction concept for BCI through convolutional architecture. CP_MixedNet proposed a structure that combines different time dimensions. For FBCNet, the characteristics of different frequency domains and timing characteristics can be considered at the same time. It is also the template method we followed in this work.

For all these methods, we managed to use the preprocessing and feature extraction methods proposed in its original place, and in order to further improve the performance, we also added filters to extract α and β bands [27] or normalization [15] and select the optimal configuration.

As shown in Table 6, it is seen that our proposed method could outperform all the other methods. Some of the shallow methods also achieved promising results such as CSP_LDA [25]. It even surpassed many deep learning based methods. All methods were better at distinguishing insider attacks except for SVM. The energyNN refers to [28], which utilized energy wavelet features. It is worth noting

Table 8: The result of EER (%) for insider and outsider attack experiment on Physionet dataset of 32 channels.

Protocol		Subject									
		1	2	3	4	5	6	7	8	9	avg
Insider	EER-19	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Outsider	EER-19	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.13	0.0	0.21

that we used 17 selected channels in the MI_CNN method. The experimental results of CP_MixedNet were given based on the BCI IV 2a dataset, as it provided better training accuracy on this dataset.

Further, we compared CSP_LDA with our proposed method under different number of channels. The result is plotted in Figure 5. Although the LDA classifier and CSP features can generate an EER less than 2%, its performance decreased intensely when reducing the number of channels. In contrast, the features and classifier in our proposed framework are more robust with a small number of channels.

5.5 Influence of Channel Selection

Physionet provides 64 electrodes signals located on the scalp. The previous experiments only used the 10 selected channels the most relevant to Motor Imagery (see Section 3.3). To verify whether the selected channels are sufficient for EEG biometric extraction, we provided a comparison by using more channels. The configuration is summarized in Table 7.

The result of EER-19 for both insider attack and outsider attack is shown in Table 8. It is found that using 32 channels yielded more valid information to give correct authentication results than using 10 channels. For all subject models, more channels could bring a drop in EER, but 7 out of 10 subjects might already extract enough traits to achieve 100% classification accuracy when using 10 channels.

The most frequently selected 10 electrodes for the 10 subjects are illustrated in Figure 6. When training models for all subjects by using the same 10 channels, we could achieve an average EER-19 of 1.21 for insider attack and 1.74 for outsider attack. This rate is instructive and can completely reduce the complexity of EEG authentication systems by also reducing the number of required channels during the training phase.

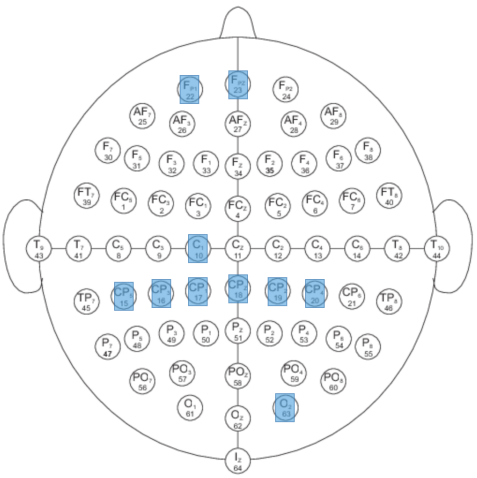

Figure 6: Map of the 10 frequently selected channels among 10 subjects (in the EEG international 10-10 system).

6 DISCUSSION AND LIMITATIONS

From the experimental results, it is found that our proposed EEG authentication system can perform the two-class classification on the visitors well, and evaluate whether the visitors belong to their claimed identities.

Further, the experimental results showed that more EEG channels have no proportional effect on improving the system performance. For our proposed method, the channels that are the most relevant to the Motor Imagery task are screened out. Using only these channels can achieve a similar accuracy rate the same as using more channels. The channel selection can not only simplify the equipment used by the system, but also if the channels corresponding to each subject are kept secret, the channels can be used as a further representation of identity information.

It can be seen from the most frequently selected channels that the scalp area, which is the cause of Motor Imagery, is relatively concentrated. In future studies, uniform channels can be used across all subjects to compress the number of channels required for raw data.

The use of deep learning classifiers can directly extract different representations of EEG data and conduct the classification in an end-to-end manner. Our proposed framework does not require a large amount of data and time for training, which can reduce the requirements for biometric system in the aspects of collectability and user-friendliness.

Our work, at this stage, is not sufficient to study the longitudinal performance of the system, which is mainly limited by the characteristics of public datasets. In future, we plan to focus on the permanency of the authentication system and ensure it to have acceptable performance in a long period of time.

7 CONCLUSION

In this work, we proposed an enhanced EEG authentication framework with Motor Imagery, which is a mental process by which a subject imagines a given action without actually performing the action. It consists of three main components: signal preprocessing, channel selection, and deep learning classification. Our framework does not require a large amount of data and time for training. In the evaluation, we investigated the framework in the aspects of insider and outsider attack performance, cross-session performance, and influence of channel selection. In the large comparison, our framework could outperform the other 9 relevant state-of-the-art methods (i.e., with a mean EER-19 of 0.74% and 1.27% for insider attack and outsider attack respectively).

REFERENCES

[1] Pierre Ablin, Jean Francois Cardoso, and Alexandre Gramfort. 2018. Faster ICA under Orthogonal Constraint. *Icassp, Ieee International Conference on Acoustics, Speech and Signal Processing - Proceedings* 2018- (2018), 4464–4468.

[2] Pierre Ablin, Jean Francois Cardoso, and Alexandre Gramfort. 2018. Faster independent component analysis by preconditioning with hessian approximations. *Ieee Transactions on Signal Processing* 66, 15 (2018), 4040–4049.

[3] Ali Al-Saegh, Shefa A. Dawwd, and Jassim M. Abdul-Jabbar. 2021. Deep learning for motor imagery EEG-based classification: A review. *Biomedical Signal Processing and Control* 63 (2021), 102172.

[4] Zaid Abdi Alkareem Alyasseri, Osama Ahmad Alomari, Sharif Naser Makhadmeh, Seyedali Mirjalili, Mohammed Azmi Al-Betar, Salwani Abdullah, Nabeel Salih Ali, Joao P. Papa, Douglas Rodrigues, and Ammar Kamal Abasi. 2022. EEG Channel Selection for Person Identification Using Binary Grey Wolf Optimizer. *Ieee Access* 10 (2022), 10500–10513.

[5] Zaid Abdi Alkareem Alyasseri, Ahamad Tajudin Khader, Mohammed Azmi Al-Betar, João P. Papa, and Osama Ahmad Alomari. 2018. EEG-based Person Authentication Using Multi-objective Flower Pollination Algorithm. *2018 Ieee Congress on Evolutionary Computation, Cec 2018 - Proceedings* (2018), 8477895.

[6] Kai Keng Ang, Zheng Yang Chin, Haihong Zhang, and Cuntai Guan. 2008. Filter Bank Common Spatial Pattern (FBCSP) in brain-computer interface. *Proceedings of the International Joint Conference on Neural Networks* (2008), 2390–2397.

[7] Blair C. Armstrong, Maria V. Ruiz-Blondet, Negin Khalifian, Kenneth J. Kurtz, Zhanpeng Jin, and Sarah Laszlo. 2015. Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics. *Neurocomputing* 166 (2015), 59–67.

[8] Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. 2011. Low-cost electroencephalogram (EEG) based authentication. *2011 5th International Ieee/embs Conference on Neural Engineering, Ner 2011* (2011), 442–445.

[9] Luiz A. Baccalá and Koichi Sameshima. 2001. Partial directed coherence: A new concept in neural structure determination. *Biological Cybernetics* 84, 6 (2001), 463–474.

[10] D Baldisserra, A Franco, D Maio, and D Maltoni. 2006. Fake fingerprint detection by odor analysis. *Advances in Biometrics, Proceedings* 3832 (2006), 265–272.

[11] Wei-Yang Chiu, Weizhi Meng, and Wenjuan Li. 2021. I Can Think Like You! Towards Reaction Spoofing Attack on Brainwave-Based Authentication. *Lecture Notes in Computer Science* 12382 (2021), 251–265.

[12] John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. 2013. I think, therefore I am: Usability and security of authentication using brainwaves. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7862 (2013), 1–16.

[13] Nguyen T.K. Cuong, Vo Q. Ha, Nguyen T.M. Huong, Truong Quang Dang Khoa, Nguyen Huynh Minh Tam, Huynh Q. Linh, and Vo Van Toi. 2010. Removing noise and artifacts from EEG using adaptive noise cancelator and blind source separation. *Ifmbe Proceedings* 27 (2010), 282–286.

[14] Rig Das, Emanuele Maiorana, and Patrizio Campisi. 2016. EEG Biometrics Using Visual Stimuli: A Longitudinal Study. *Ieee Signal Processing Letters* 23, 3 (2016), 341–345.

[15] Rig Das, Emanuele Maiorana, and Patrizio Campisi. 2018. MOTOR IMAGERY FOR EEG BIOMETRICS USING CONVOLUTIONAL NEURAL NETWORK. *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (icassp)* (2018), 2062–2066.

[16] Yang Di, Xingwei An, Feng He, Shuang Liu, Yufeng Ke, and Dong Ming. 2019. Robustness Analysis of Identification Using Resting-State EEG Signals. *Ieee Access* 7 (2019), 42113–42122.

[17] Nesli Erdogmus and Sebastien Marcel. 2013. Spoofing 2D face recognition systems with 3D masks. *Lecture Notes in Informatics (lni), Proceedings - Series of the Gesellschaft Fur Informatik (gi)* P-212 (2013), 6617158.

[18] David Feess, Mario M. Krell, and Jan H. Metzen. 2013. Comparison of Sensor Selection Mechanisms for an ERP-Based Brain-Computer Interface. *Plos One* 8, 7 (2013), e67543.

[19] A. L. Goldberger, L. A. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C. K. Peng, and H. E. Stanley. 2000. PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. *Circulation* 101, 23 (2000), E215–220.

[20] C. W. J. Granger. 1969. Investigating Causal Relations by Econometric Models and Cross-spectral Methods. *Econometrica* 37, 3 (1969), 424.

[21] Qiong Gui, Zhanpeng Jin, Wenyao Xu, Maria V. Ruiz-Blondet, and Sarah Laszlo. 2015. Multichannel EEG-based biometric using improved RBF neural networks. *2015 Ieee Signal Processing in Medicine and Biology Symposium - Proceedings* (2015), 7405418.

[22] Thorir Mar Ingolfsson, Michael Hersche, Xiaying Wang, Nobuaki Kobayashi, Lukas Cavigelli, and Luca Benini. 2020. EEG-TCNet: An Accurate Temporal Convolutional Network for Embedded Motor-Imagery Brain-Machine Interfaces. *Conference Proceedings - Ieee International Conference on Systems, Man and Cybernetics* 2020- (2020), 2958–2965.

[23] Md Kafiul Islam, Amir Rastegarnia, and Zhi Yang. 2016. Methods for artifact detection and removal from scalp EEG: A review. *Neurophysiologie Clinique* 46, 4-5 (2016), 287–305.

[24] Amir Jalaly Bidgoly, Hamed Jalaly Bidgoly, and Zeynab Arezoumand. 2020. A survey on methods and challenges in EEG based authentication. *Computers and Security* 93 (2020), 101788.

[25] Isuru Jayarathne, Michael Cohen, and Senaka Amarakeerthi. 2016. BrainID: Development of an EEG-based biometric authentication system. *7th Ieee Annual Information Technology, Electronics and Mobile Communication Conference, Ieee Iemcon 2016* (2016), 7746325.

[26] Donghyeon Kim and Kiseon Kim. 2019. Resting State EEG-Based Biometric System Using Concatenation of Quadrantal Functional Networks. *Ieee Access* 7 (2019), 65745–65756.

[27] Pradeep Kumar, Rajkumar Saini, Partha Pratim Roy, and Debi Prosad Dogra. 2017. A bio-signal based framework to secure mobile devices. *Journal of Network and Computer Applications* 89 (2017), 62–71.

[28] Pinki Kumari Sharma and Abhishek Vaish. 2016. Individual identification based on neuro-signal using motor movement and imaginary cognitive process. *Optik* 127, 4 (2016), 2143–2148.

[29] Vernon J. Lawhern, Amelia J. Solon, Nicholas R. Waytowich, Stephen M. Gordon, Chou P. Hung, and Brent J. Lance. 2018. EEGNet: A compact convolutional neural network for EEG-based brain-computer interfaces. *Journal of Neural Engineering* 15, 5 (2018), 056013.

[30] Yang Li, Xian Rui Zhang, Bin Zhang, Meng Ying Lei, Wei Gang Cui, and Yu Zhu Guo. 2019. A Channel-Projection Mixed-Scale Convolutional Neural Network for Motor Imagery EEG Decoding. *Ieee Transactions on Neural Systems and Rehabilitation Engineering* 27, 6 (2019), 1170–1180.

[31] Ruhi Mahajan and Bashir I. Morshed. 2015. Unsupervised eye blink artifact denoising of EEG data with modified multiscale sample entropy, kurtosis, and wavelet-ICA. *Ieee Journal of Biomedical and Health Informatics* 19, 1 (2015), 158–165.

[32] Emanuele Maiorana and Patrizio Campisi. 2018. Longitudinal Evaluation of EEG-Based Biometric Recognition. *Ieee Transactions on Information Forensics and Security* 13, 5 (2018), 1123–1138.

[33] Ravikiran Mane, Effie Chew, Karen Chua, Kai Keng Ang, Neethu Robinson, A. P. Vinod, Seong-Whan Lee, and Cuntai Guan. 2021. FBCNet: A Multi-view Convolutional Neural Network for Brain-Computer Interface. (2021).

[34] Sébatien Marcel and José del R. Millan. 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, 4 (2007), 743–748.

[35] Orlando Nieves and Vidya Manian. 2016. Automatic person authentication using fewer channel EEG motor imagery. *World Automation Congress Proceedings* 2016- (2016), 7582945.

[36] Ibrahim Omerhodzic, Samir Avdakovic, Amir Nuhanovic, and Kemal Dizdarevic. 2013. Energy Distribution of EEG Signals: EEG Signal Wavelet-Neural Network Classifier. (2013).

[37] Ozan Özdenizci, Ye Wang, Toshiaki Koike-Akino, and Deniz Erdoğmuş. 2019. Adversarial deep learning in EEG biometrics. *IEEE signal processing letters* 26, 5 (2019), 710–714.

[38] Katya Pivcevic. 2021. Smart city growth creates biometrics opportunity. https://www.biometricupdate.com/202104/smart-city-growth-creates-biometrics-opportunity. [Online; accessed 30-April-2022].

[39] M. Poulos, M. Rangoussi, and E. Kafetzopoulos. 1998. Person identification via the EEG using computational geometry algorithms. *9th European Signal Processing Conference (eusipco 1998)* (1998), 4 pp.

[40] W Rief. 2006. Getting started with neurofeedback. *Journal of Psychosomatic Research* 60, 3 (2006), 313–313.

[41] Koosha Sadeghi, Ayan Banerjee, Javad Sohankar, and Sandeep K.S. Gupta. 2017. Geometrical analysis of machine learning security in biometric authentication systems. *Proceedings - 16th Ieee International Conference on Machine Learning and Applications, Icmla 2017* 2017- (2017), 309–314. https://doi.org/10.1109/ICMLA.2017.0-142

[42] Chong Yeh Sai, Norrima Mokhtar, Hamzah Arof, Paul Cumming, and Masahiro Iwahashi. 2018. Automated classification and removal of EEG artifacts with SVM and wavelet-ICA. *Ieee Journal of Biomedical and Health Informatics* 22, 3 (2018), 664–670.

[43] Nima Salimi, Michael Barlow, and Erandi Lakshika. 2020. Towards Potential of N-back Task as Protocol and EEGNet for the EEG-based Biometric. *2020 Ieee Symposium Series on Computational Intelligence, Ssci 2020* (2020), 1718–1724.

[44] Gerwin Schalk, Dennis J. McFarland, Thilo Hinterberger, Niels Birbaumer, and Jonathan R. Wolpaw. 2004. BCI2000: A general-purpose brain-computer interface (BCI) system. *Ieee Transactions on Biomedical Engineering* 51, 6 (2004), 1034–1043.

[45] Ioannis Stylios, Spyros Kokolakis, Olga Thanou, and Sotirios Chatzis. 2021. Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Inf. Fusion* 66 (2021), 76–99.

[46] Jiayao Sun, Jin Xie, and Huihui Zhou. 2021. EEG classification with transformer-based models. *Lifetech 2021 - 2021 Ieee 3rd Global Conference on Life Sciences and Technologies* (2021), 92–93.

[47] Yingnan Sun, Frank P.W. Lo, and Benny Lo. 2019. EEG-based user identification system using 1D-convolutional long short-term memory neural networks. *Expert Systems With Applications* 125 (2019), 259–267.
[48] Yousef Rezaei Tabar and Ugur Halici. 2016. A novel deep learning approach for classification of EEG motor imagery signals. *Journal of neural engineering* 14, 1 (2016), 016003.
[49] Preecha Tangkraingkij, Chidchanok Lursinsap, Siripun Sanguansintukul, and Tayard Desudchit. 2010. Personal identification by EEG using ICA and neural network. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 6018, 3 (2010), 419–430.
[50] Hesam Varsehi and S. Mohammad P. Firoozabadi. 2021. An EEG channel selection method for motor imagery based brain computer interface and neurofeedback using Granger causality. *Neural Networks* 133 (2021), 193–206.
[51] Scott I. Vrieze. 2012. Model selection and psychological theory: A discussion of the differences between the Akaike information criterion (AIC) and the Bayesian information criterion (BIC). *Psychological Methods* 17, 2 (2012), 228–243.
[52] Mei Wang and Weihong Deng. 2021. Deep face recognition: A survey. *Neurocomputing* 429 (2021), 215–244.
[53] Irene Winkler, Stefan Haufe, and Michael Tangermann. 2011. Automatic Classification of Artifactual ICA-Components for Artifact Removal in EEG Signals. *Behavioral and Brain Functions* 7, 1 (2011), 30.
[54] Jianwei Yang, Zhen Lei, and Stan Z. Li. 2014. Learn Convolutional Neural Network for Face Anti-Spoofing. (2014), 8.
[55] Zitong Yu, Chenxu Zhao, Zezheng Wang, Yunxiao Qin, Zhuo Su, Xiaobai Li, Feng Zhou, and Guoying Zhao. 2020. Searching Central Difference Convolutional Networks for Face Anti-Spoofing. (2020).
[56] Ying Zeng, Qunjian Wu, Kai Yang, Li Tong, Bin Yan, Jun Shu, and Dezhong Yao. 2019. EEG-Based Identity Authentication Framework Using Face Rapid Serial Visual Presentation with Optimized Channels. *Sensors* 19, 1 (2019).

APPENDIX

EEG Background

EEG is the electrical signal along the scalp surface. These signals are often representatives of physical or mental states of individuals. EEG recordings are diverse in amplitudes and dominant frequencies. Depending on the equipment, the frequency bands, which can be triggered and influenced by most tasks in an EEG authentication system, are introduced as follows:

- **Alpha** (8-12Hz) is the dominant frequency band during relaxed state. Focused attention can reduce the amplitude of this band.
- **Beta** (12-25Hz) is related to thinking and focused attention. Body movements can also increase amplitude of this band.

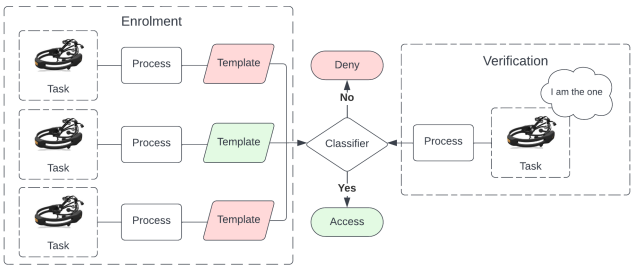

Figure 7: The Stages of EEG Authentication System

These two bands are usually acquired and filtered for usage in EEG authentication as they contain most of the traits [25]. Except for the amplitude and frequency of EEG signals, different electric potentials are captured at different scalp locations through electrodes. Standards have been introduced to regularize the expression of electrode location. For instance, 10-20 standard [40] could place the electrodes at 10% and 20% points along lines of longitude and latitude.

Based on these concepts, EEG authentication systems are constructed using biometric factor(s). The users are required to perform designed tasks under specific settings. These tasks are designed to trigger particular potentials such Visual Evoked Potential (VEP) and Event Related Potential (ERP), which can be captured through EEG headsets. Some of the tasks have even higher demands on the experimental environment. For the authentication system, two stages of usage fall into *registration phase* and *enrolment phase*. During registration phase, an individual records his or her own EEG signal and forms a template, the signal is processed and analyzed together with other people's signals, and finally a classifier is trained. This classifier can exclusively distinguish the individual. Followed by the enrolment phase, an individual claims his/her identity, which calls the corresponding classifier to validate. The user usually has to perform the same task or a task from the same type during the enrolment phase. Figure 7 depicts the stages for an EEG authentication system.

Table 9: Related EEG Authentication/Identification Studies Categorized by Tasks (*auth* in Type stands for authentication and *iden* stands for identification)

Study	Year	Type	Task	Subject	Channel	Feature	Method	Performance
[8]	2011	auth	resting state/ motor imagery/ thinking stimuli	5	14	AR/ PSD/SP/ IHPD/ IHLC	SVM	100%
[12]	2013	auth	resting state/ motor imagery/ visual/ auditive stimuli	15	1	time series	Cosine Similarity	1.1% HTER
[35]	2016	auth	motor imagery	20	2 ~6	STFT	SVM/NN	98%
[28]	2016	iden	motor imagery/ movement	5	1	Wavelet Decomposition	NN	95% TAR 4.44 %FAR
[15]	2018	iden	motor imagery	40	17	time series	CNN	99.3%
[5]	2018	iden	motor imagery/ movement	10/11	64	MOFPA-WT	NN	85.71% TAR 14.28% FAR
[47]	2019	iden	motor imagery	109	16	time series	CNN-LSTM	99.58%
[4]	2022	iden	motor imagery/ movement	109	23	AR	SVM-RBF	94.13%
[7]	2015	iden	text reading (ERPs)	45	3	time series	NN	82% ~97%
[25]	2016	auth	visual stimuli/ thinking stimuli	12	14	CSP	LDA	96.97%
[14]	2016	auth	visual stimuli	50	19	time series	Similarity	95% EER confidence intervals
[27]	2017	auth	gesture patterns	50	14	DFT	SVM/HMM	25% Global HTER 2.01% Local HTER
[32]	2018	auth	resting state/ math computation/ speech imagery	45	19	AR/ MFCC/ Bump	HMM	<2% EER
[37]	2019	iden	RSVP Keyboard (RSVP)	10	16	time series	Adversarial CNN	99% within-session 72% across-sessions

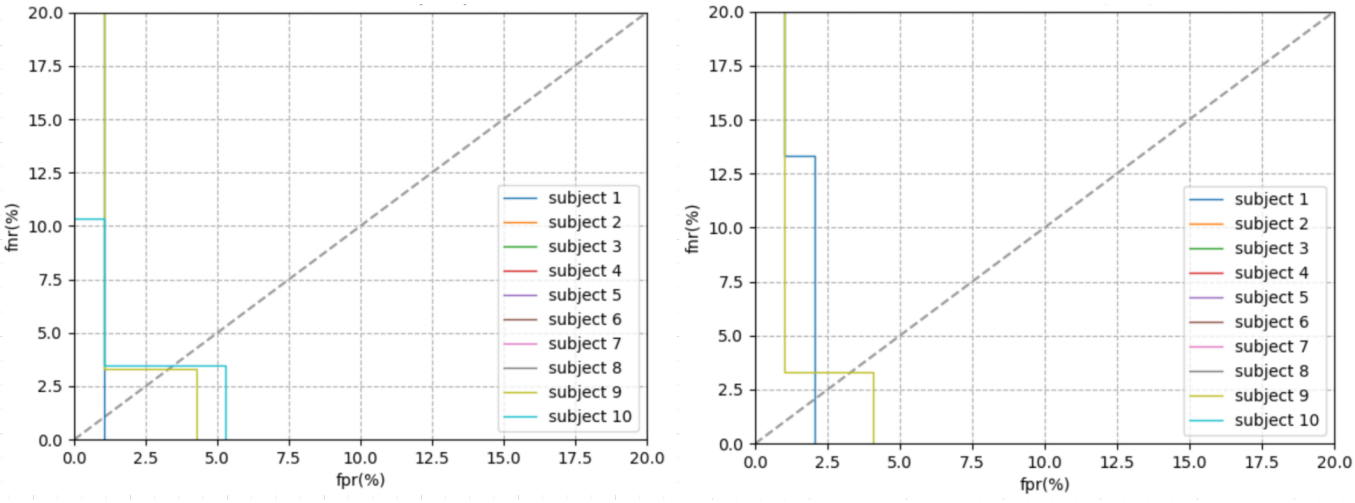

Figure 8: The DET curve of Insider Attack Experiment. (Left: EER-19, 19 attackers in test, Right: EER-49, 49 attackers in test)

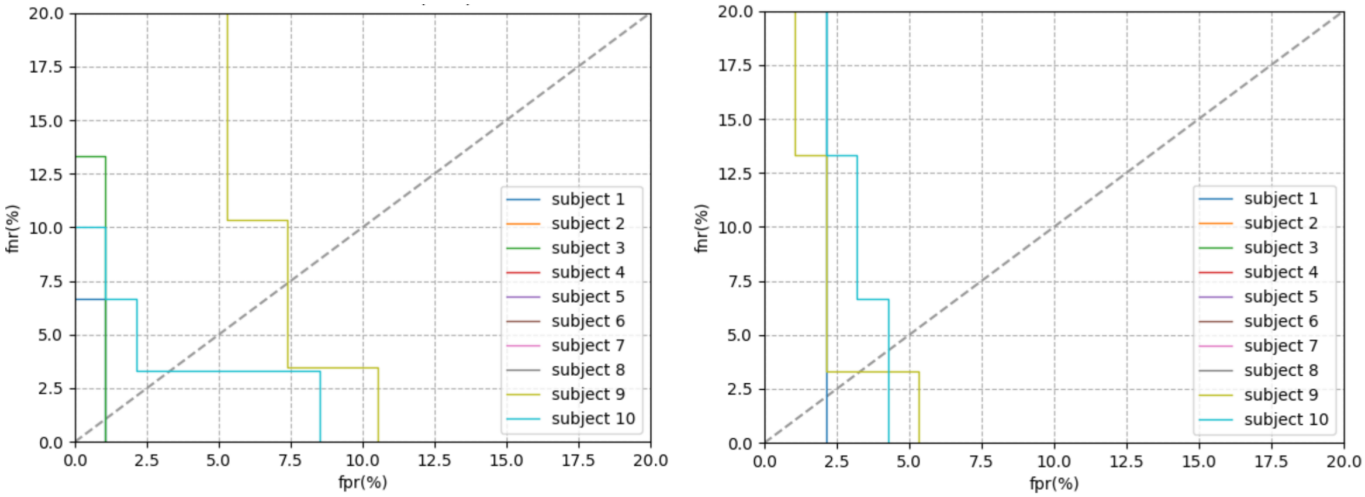

Figure 9: The DET curve of Outsider Attack Experiment. (Left: EER-19, 19 attackers in test, Right: EER-47, 47 attackers in test)