

Toward Secure and Intelligent Subject Authentication Using Brainprints and Enhanced AMEEGNet

Adnan Elahi Khan Khalil, Jesus Arturo Perez-Daz(✉), Jos Antonio Cantoral-Ceballos, and Javier M. Antelis

School of Engineering and Sciences, Tecnológico de Monterrey, Monterrey, NL 64700, Mexico
jesus.arturo.perez@tec.mx

Abstract. Neural based subject authentication has emerged as a promising paradigm in biometric security, with the P300 event related potential (ERP) gaining particular attention due to its reliability and individual specificity. The proposed scheme introduces a personalized brainprint recognition framework that utilizes an enhanced AMEEGNet architecture to accurately classify symbol evoked P300 responses. A visual oddball paradigm featuring directional arrows and a stop sign was employed to elicit P300 activity with minimal cognitive demand. 16 subjects (participants) completed the task across three separate sessions conducted on different days. EEG data from the session 1 and 2 were used to train the deep learning model, while the third session was utilized for cross-session validation and testing. The proposed framework achieved strong performance, with an average classification accuracy of 89.25% and average Cohen's kappa score of 0.88. These findings demonstrate that symbol-evoked P300 responses carry consistent, individual-specific features, underscoring their potential for use in practical EEG-based subject authentication systems.

Keywords: Brainprint biometrics · Cognitive biometric authentication · Neural signature recognition · Privacy-preserving EEG user authentication

1 Introduction

In current period of knowledge and advanced technology, the importance of safe user authentication schemes are growing with fast pace. The lack of typical conventional approaches such as, passwords and physical tokens have illustrated considerable issues due to their vulnerability to be forgotten, spoofed, or bypassed, that leads to a considerable security breaches and financial losses [1]. Even though facial recognition and fingerprint based user authentication systems have illustrated a very high accuracy, yet they are not immune to security breaches, including spoofing attacks, data breaches, and identity fraud [2]. Subsequently,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2027
O. Gervasi et al. (Eds.): ICCSA 2026 Workshops, LNCS 16759, pp. 624–640, 2027.
https://doi.org/10.1007/978-3-032-30518-3_39

scholars have pursued way more secure and tamper-resistant user authentication schemes and methods. In this context, electroencephalogram (EEG) signals have been getting attention as a viable source due to its unique, user specific patterns that are difficult to replicate [3]. Experimental research have shown that EEG-based biometrics exhibit important key properties, including universality, ease of acquisition, and the ability to be revoked or reissued [4]. As a result, EEG based user authentication has emerged a useful approach for future generation biometric system [5]. For example, an EEG based experiment was conducted [6] that involves 30 subjects which involves resting state EEG signals with closed and open eyes for user identification. By employing a similarity based classification approach, the system achieved an average identification accuracy of 85%. However, since the system relies on resting state activity, there was a lack of active mental activity, increasing the surrounding noise, single session experiment leading to potential spoofing attacks. In a given study [7] an EEG authentication framework was developed utilizing rapid serial visual presentation (RSVP) to capture neural responses during login attempts. The given framework employed shrinkage discriminant analysis to classify EEG signals from 16 subjects, which yields a mean validation accuracy of 87%. Although, RSVP based approaches often depend on repetitive passive visual stimulation, that leads to a lower inter session robustness with limited user interaction, which affects a long term stability and user experience for real time applications. In a another investigation, researchers developed an user authentication system using steady state auditory evoked potentials collected from 40 subjects. A canonical correlation analysis was implemented to match the EEG template, they obtained competitive recognition performance [8]. Despite these good results, SSVEP-based methods typically require a long periods for stimulation with deep electrode arrays implementation, which may restrict it for real time practice with fast, and user friendly user authentication scenarios.

Some of the current studies have investigated symbol evoked P300 responses as a robust biometric markers for user authentication systems [9]. Unlike traditional visual evoked potentials, these event related potentials are elicited by different meaningful symbol stimuli that produces a distinctive waveforms which exhibits a strong inter individual variability [10]. The P300 component, particularly when evoked by different symbolic patterns demonstrates an enhanced signal-to-noise characteristics as compared to the conventional flash producing stimuli [11]. Most recent studies indicate that symbol evoked P300 paradigms achieve high classification accuracy in EEG based biometric applications, reporting user authentication in controlled experiments [12]. These studies have established symbol evoked P300 responses as a robust EEG based biometric verifier. Rathi [13] proposed a P300 based brain signal user authentication scheme using picture based visual stimuli instead of conventional alphanumeric characters. The recorded P300 responses from users were tested with three different classifiers by presenting object images that achieved a an accuracy of 97%, highlighting the method's robustness and usability for secure user authentication. However, this work primarily focused using compact EEG setups, no evaluation of temporal

generalization. A recent study by Akram [14] presented a smart home control with symbol based P300 BCI paradigm that achieved an improved flexible command and control classification accuracy of 92.25%. The system helped users to manage various appliances and even to make phone calls, demonstrating the real time use of symbol evoked P300 responses in assistive technologies demonstrating robustness of the EEG based authentication. But, the study was based on control applications rather than universal biometric user authentication, and also did not address the longitudinal stability or security specific evaluations of the biometric system.

Neural cognitive tasks has improved EEG based authentication by utilizing unique neural patterns like P300 ERPs [15]. This method is widely employed for capturing individual active neural responses. For instance, [16] utilized SSVEPs for user identification from a character recognition task. A causal connectivity analysis to EEG data from 15 subjects was applied achieving a high user identification accuracy of 95.5%. Despite of having high performance, this approach is based on large number electrode configurations and extended stimulation, which limited to employ this system in a compact and efficient user authentication environments. Similarly, [17] proposed a user authentication method using rapid serial visual presentation (RSVP) with similar and non similar faces (face RSVP). To support the effectiveness of cognitive task for enhanced EEG biometrics, these stimuli achieved an average verification accuracy of 88.88%. However, but this paradigm is based on controlled laboratory settings and large number electrodes, and cross session robustness with lack of model interpretability exploration which is crucial for scalable user authentication frameworks.

EEG data processing for user authentication employs several key methods and techniques. Like, temporal averaging of EEG epochs enhances the signal to noise ratio of event related potentials (ERPs), improving user biometric performance [18]. Many studies have demonstrated effectiveness of this approach [19]. Deep learning methods have emerged as a prominent classification method in EEG based biometrics, with novel convolutional neural networks (CNNs) being particularly valuable in these approches. In [20] the authors employed CNNs for EEG template matching, while Roy et al. [21] applied CNN based feature extraction to motor imagery data. The specialized CNN architecture knowns as EEGNet [22] has been widely adopted in various user authentication systems demonstrating its effectiveness for EEG signal processing.

EEG based user authentication systems faces four major limitations: (1) reliance on large numbers of electrodes placement, (2) large duration for user authentication process, (3) lacking of standardized naturalistic neural cognitive paradigms, and (4) unverified longitudinal stability. To address these limitations, a novel framework that combines a symbol evoked P300 responses with an enhanced AMEEGNet-CAM architecture is proposed [23]. The system employs (1) a low burden on neural cognitive activity using familiar symbols to elicit distinct P300 ERPs responses, and (2) AMEEGNet-CAM, a convolutional network with channel attention mechanisms using key input electrodes, less EEG data processing and improved interpretability. While active participation is required,

this approach enhances resistance to spoofing attacks and increases user biometric specificity, making it ideal for future critical security applications. The key contribution of the proposed study is as follows:

1. The introduction of a novel symbol evoked P300 paradigm designed to elicit robust and user friendly event related responses for EEG based user authentication.
2. This study proposes AMEEGNet-CAM, an enhanced deep learning architecture with channel attention mechanisms, enabling efficient less EEG data processing and use of key electrode inputs.
3. The proposed study conducts a comprehensive evaluation across performance metrics, temporal robustness a cross session generalization (EEG data across different sessions), and an efficient system with key electrode setup, demonstrating the framework's practicality, stability, and spoof resistance for real time applications.

This scheme was evaluated and tested across three dimensions: (i) performance metrics such as accuracy, ROC, FAR, and FRR; (ii) robustness through test and retest reliability across sessions (training on session 1 and session 2, testing on session 3); and (iii) the efficiency of the scheme using discriminative feature extraction from a compact EEG setup. The adaptive feature learning along with explainable attention mechanisms was integrated which advances EEG based user authentication for more practical and scalable real world scenarios. To highlight the distinctions between the proposed framework and existing EEG based user authentication approaches, a comprehensive comparison of representative studies is provided in Table 1 with detail explanation.

Table 1. Summary of previous EEG based user authentication studies and the proposed approach highlighting methodology, paradigms, classifiers, and performance

Author	Year	Subjects	Channels	Methodology	Protocol	Classifier
Maiorana et al. [6]	2015	50	32	Resting-state EEG	Eyes-open/closed	SVM
Chen et al. [7]	2016	29	31	RSVP features	RSVP	Shrinkage LDA
Seha et al. [8]	2020	40	32	SSVEP analysis	Auditory evoked	CCA
Rathi et al. [13]	2021	10	10	PCA	Picture-based P300	QDA
Akram et al. [14]	2022	10	32	Signal Processing	P300	RF
Santamaria et al. [16]	2019	20	8	ORSD	P300 speller	CCA
Zeng et al. [17]	2018	45	16	HDCA spatiotemporal	RSVP paradigm	HDCA + GA
Proposed Work	**2026**	**16**	**8**	**Processed Raw EEG**	**Symbol-based P300**	**AMEEGNet**

2 Methodology

2.1 Schematic Overview of the Proposed Approach

The proposed study investigates subject authentication through symbol evoked P300 ERP responses, implemented with two discrete stages: subject identification and authentication. During the subject identification stage, the

AMEEGNet-CAM architecture processes EEG signals that are elicited by symbol based stimuli to generate individual active neural profiles. These active neural profiles captures a discriminative P300 features using the model's integrated channel attention mechanisms (CAM) and explainable feature extraction method. In the subject authentication stage, the system verifies subjects comparing the EEG responses to the stored subject profiles, combing the high inter subject variability of symbol evoked P300 neural waveforms. As illustrated in Fig. 1, this framework ensures robust and efficient subject authentication, combining task specific cognitive neural signatures with AMEEGNet-CAM's adaptive data processing.

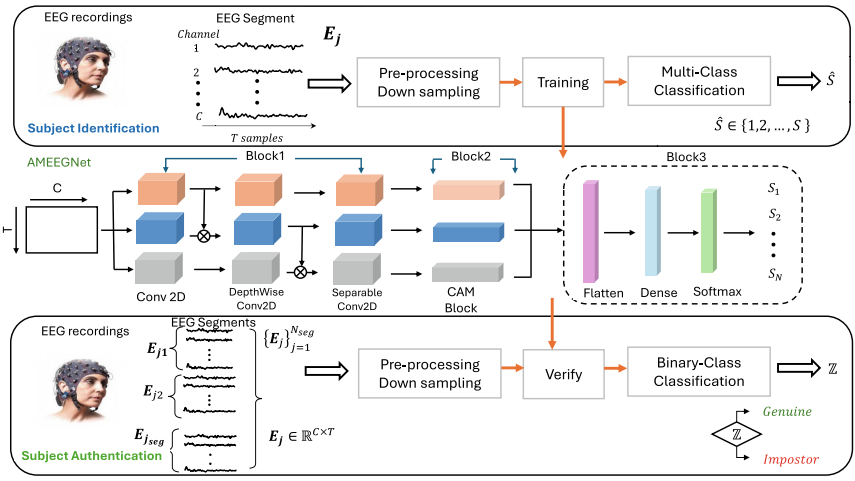

Fig. 1. The proposed EEG-based authentication framework uses symbol-evoked P300 responses in two stages: **(a)** subject identification, where AMEEGNet-CAM employs channel attention to extract unique neural subject profiles emphasizing on key P300 ERP features; and **(b)** subject authentication, where new EEG data is matched against these neural profiles for verification. This scheme integrates the deep learning features with ERP based cognitive neural signatures for robust and efficient subject authentication.

2.2 Problem Statement and Objectives

The given dataset consists of various EEG trials represented as $\mathcal{E} = \{(\mathbf{E}_j, c_j, s_j)\}_{j=1}^{J}$, where each trial $\mathbf{E}_j \in \mathbf{R}^{C\times T}$ corresponds to a segment of the signal recorded from C electrodes over T time points. The variable c_j demonstrates the experimental condition, and $s_j \in \{1, \ldots, S\}$ denotes the subject identity associated with EEG trial j. The proposed method addresses both subject identification and authentication by transforming input EEG signals into discriminative features that capture subject and task related neural signatures.

While the dataset includes condition specific information of the EEG data, the primary focus is to obtain a stable, subject specific EEG patterns for subject related biometric recognition.

The objective of the subject identification task is to determine the true identity s_j from a set of S enrolled subjects with EEG trial $\mathbf{E}_j$. This task is defined, mapping $\mathcal{I} = \mathcal{C} \circ \mathcal{H}$, where $\mathcal{H}$ denotes the feature extraction function which maps EEG epoch into a space representation, and $\mathcal{C}$ is a classifier that allocates identity label.

The objective of the subject authentication task is to verify whether a given EEG trial $\mathbf{E}_j$ relates to a claimed subject identity $s_c \in \{1, \ldots, S\}$. This process is implemented using a binary classifier $\mathcal{A} = \mathcal{V} \circ \Phi$: $\mathbf{R}^{C \times T} \rightarrow \{0, 1\}$, where 1 denotes a trial related to genuine and 0 to impostor. A reliable subject authentication requires robust extraction of subject specific features that minimize false acceptance rates (FAR) and false rejection rates (FRR), thereby ensuring strong EEG biometric environment.

2.3 EEG Data Preprocessing

Filtering and Baseline Correction. To remove non-cognitive relevant brain activity, the EEG data were filtered between (418 Hz) using FIR filter in MNE-Python [24]. This removal of low frequency shifts and noise with high frequency in order to preserve neural EEG signals. This procedure is expressed as:

$$\mathbf{Y}_{i,\mathrm{f}}(t) = \mathcal{B}_{[min,max]} \{\mathbf{X}_i(t)\} \tag{1}$$

where $\mathbf{X}_i(t)$ is the raw epoch, $\mathbf{Y}_i(t)$ is the filtered signal, and $\mathcal{B}_{[4,18]}$ denotes band-pass filtering.

The inherence of EEG signals is low amplitude (μV range) which requires complete preprocessing proedure to reduce interference from both physiological sources (such as eye or muscle movement) and non-physiological artifacts. These EEG recordings were windowed into stimulus locked EEG epochs $\mathbf{E}_j \in \mathbf{R}^{C \times T}$ (200ms pre-stimulus to 800ms post stimulus) which was followed by baseline correction using the prestimulus interval $t \in [-200, 0]$ ms. The baseline corrected epoched signal was computed as:

$$\bar{\mathbf{E}}_j(t) = \mathbf{E}_j(t) - \frac{1}{\Delta\tau} \int_{\tau_b}^{0} \mathbf{E}_j(\tau)\, d\tau \tag{2}$$

where τ_b = -200 ms marks the baseline start, and $\Delta\tau$ = 200 ms is the baseline duration. Here C represents the number of EEG channels, and T denotes the temporal samples per epoch.

EEG Epoch Rejection, Cropping and Downsampling. In order to have EEG data reliability, epochs that contained artifacts of high amplitudes (e.g., from motion or transient noise) were removed. Specifically, those trials where the absolute voltage exceeded from$50\mu V$ on any channel was discarded as well:

$$\max_{t \in [\tau_1, \tau_2]} |\mathbf{E}_j(t)| > 50, \mu\mathrm{V} \tag{3}$$

This strong rejection policy preserved only artifact free EEG segments thus, enhancing the integrity of subsequent neurophysiological analysis of the EEG data.

To remove those EEG trials affected by artifacts such as electromyographic interference or surrounding noise, all EEG segments exceeding that predefined amplitude were excluded. The remaining epochs were cropped to focus on the relevant time window spanning EEG epochs $t \in [0, 800]$ ms are defined by:

$$\bar{\mathbf{X}}_j(t) = \mathbf{X}_j(t) \quad \forall t \in [0, 800] \text{ ms}. \tag{4}$$

Subsequent to this temporal selection, the EEG data was resampled in order to standardize the temporal resolution. These EEG signals were reduced from their normal sampling rate f_s to a resonated rate of $f_t = 64Hz$. This reduction in dimensionality reduced the sample count by a factor of $\frac{f_s}{f_t}$ while it maintained all physiologically relevant frequency components below the $\frac{f_t}{2} = 32Hz$ cutoff.

EEG Vectorization. Each preprocessed EEG epoch $\mathbf{E}_j \in \mathbf{R}^{C \times T}$ was vectorized into a one dimensional feature vector $\mathbf{x}_j \in \mathbf{R}^{C \cdot T}$ using flattening process across channels and time samples. This operation ensures compatibility with conventional machine learning pipelines and is formally expressed as:

$$\mathbf{x}_j = \text{vec}(\mathbf{E}_j) \in \mathbf{R}^{C \cdot T} \tag{5}$$

The data of all the subjects were aggregated into one unified dataset, with each one observated data labeled according to its corresponding subject identity. This standardization of the data supports consistent analysis across classification and evaluation procedures.

2.4 Classification Model

To enhance the feature extraction procedure and improve the ability of the model to focus on the features that are discriminative in symbol evoked based EEG signals, an attention-enhanced multiscale EEGNet architecture, represented as the AMEEGNet-CAM model is proposed. This framework accommodates the classification and subject authentication capabilities. This framework consists of three main components. Block 1, known as multiscale feature extractor which employs three parallel branches inspired by EEGNet with temporal kernel sizes of 32, 64, and 128, dropout rate of 0.5, and L2 regularization ($\lambda = 0.001$) that helps to extract rich temporal spatial patterns from raw EEG data. Block 2 consists of an attention mechanism having a channel attention module (CAM) and a spatial attention module that arbitrarily increase weights and refine the feature learned based on channel and spatial temporal features. Block 3 is the classification stage, includes a global average pooling layer and a dense layer with 256 units and *Swish* activation. This classifier is trained using the adamW optimizer with a learning rate of 5×10^{-5}. The overall AMEEGNet-CAM framework is illustrated in Fig. 1, along with the associated subject identification and authentication scheme.

This classifier employes three parallel EEGNet inspired branches to extract temporal and spatial features from EEG signals containing P300 ERPs for subject identification and authentication scheme. Each branch processes the same 2D input (channels × time samples) and includes: (1) a temporal convolutional layer to capture P300 specific time features using size of various filters (32, 64, and 128), (2) a depthwise convolutional layer to learn spatial patterns across channels, and (3) a separable convolutional layer that combine features efficiently. The depthwise layer uses twice as many filters as the temporal layer, and the separable layer applies filters of size (1, 16). Batch normalization and ELU activation follow both convolutional layers to stabilize learning. Features from all branches are concatenated and passed to a spatial attention module that highlights informative EEG channels. This multi-scale, attention based design accelerates the model ability to decode subject specific ERP patterns for robust subject recognition.

In order to enhance the feature representation for subject identification and authentication based P300 ERPs, the model accomodates a Channel Attention Module (CAM) after the depthwise convolutional layers. CAM adaptively recalibrates channel-wise features by intergrating both average and max. pooled descriptors and move them via a shared MLP that is followed by sigmoid activation to generate attention weights. Following the parallel EEGNet blocks, the resulting feature map X is passed to CAM block which then applies global average pooling (GAP) and global max. pooling (GMP) throughout the spatial dimensions to generate to extract meaningful channel wise information as illustrated in equation:

$$s = \sigma\left(\mathrm{MLP}(\mathrm{GAP}(X)) + \mathrm{MLP}(\mathrm{GMP}(X))\right) \tag{6}$$

where X denotes the input feature map, σ is the sigmoid activation function, and $s \in \mathbf{R}^C$ represents the channel attention weights. These weights are then applied to each channel of the input feature map using element-wise multiplication to recalibrate the features as shown in equation:

$$\tilde{X}_c = s_c \cdot X_c, \quad \text{for } c \in 1, \ldots, C \tag{7}$$

This mechanism allows the model to concentrate on EEG channels most relevant to subject specific P300 ERP responses, hence improving both its discriminative power and robustness while maintaining computational efficiency.

2.5 Implementation of the Subject Authentication Framework

In this research, EEG based subject recognition framework is implemented employing the Enhanced AMEEGNet model to perform subject identification and authentication. The objective of this framework is to validate the effectiveness of the proposed work by recording EEG data from 16 subjects, sessions 1 and 2 was used for training and session 3 for testing. EEG data epochs from all subjects were preprocessed and then analyzed to perform classification based on the learned features.

The EEG based subject identification framework employs a raw EEG segment $\mathbf{E}_j \in \mathbf{R}^{C \times T}$ as input. This undergoes preprocessing steps which includes bandpass filtering, baseline correction, epoch rejection, cropping, and downsampling in order to standardize and clean the EEG signal. The resulted preprocessed EEG segment is then passed through the AMEEGNet-CAM model to integrates channel attention module in order to enhance feature interpretability of the EEG data. EEG data from sessions 1 and 2, the model is trained to learn EEG patterns with specific subject identities. During testing stage the unseen EEG data from session 3 is utilized so the model predicts the subject identity, and labels are evaluated to compare the performance.

The EEG based subject authentication framework is employed to verify either an input EEG segment that originates from a claimed identity is part of the dataset or not. Number of EEG segments $\mathbf{E}_j \in \mathbf{R}^{C \times T}$ undergoes a list of preprocessing stages, including bandpass filtering, baseline correction, artifact rejection, and downsampling, to improve EEG signal quality and reduce artifacts. The preprocessed EEG signal is then fed into the AMEEGNet-CAM model that incorporates channel attention module to improve the interpretability of the features that are extracted. The model work as a binary decider $\mathbf{Z} \in (0, 1)$ where 1 represents a genuine subject and 0 represents an imposter. To assess the generalization ability of the subject authentication system, a leave-one-subject-out (LOSO) cross-validation strategy was implemented, meaning that in each fold the model is trained on all subjects except one and tested on the left-out subject.

2.6 Validation Procedure

Dataset Overview. The proposed scheme analyzes an EEG dataset [25] containing recordings from 16 visually normal, BCI-inexperienced individuals. EEG Neural activity was performed during visual oddball paradigms eliciting P300 potentials. Neural Signals were obtained from 8 optimized electrode sites (Fz, Cz, P3, Pz, P4, PO7, PO8, Oz) according to the 10–20 placement system, with a 256 Hz sampling rate. Sixteen subjects (10 males, 6 females; age 1933, mean 25) completed three sessions with distinct visual paradigms. Facial stimuli elicited stronger P300 responses and higher classification accuracy, while target set size had little effect. These results highlight the value of stimulus optimization and establish the dataset as a benchmark for ERP based subject authentication system.

2.7 Quantitative Metrics

The performance of the proposed methodology was evaluated using accuracy, cohen's kappa, FAR, FRR, and ROC curves. Accuracy measures the overall correctness of predictions, while Kappa accounts for chance agreement between predicted and actual labels:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

$$\kappa = \frac{p_o - p_e}{1 - p_e} \tag{9}$$

Here, p_o denotes the observed agreement (accuracy), and p_e represents the expected agreement by chance.

A confusion matrix was employed to provide insights into classification outcomes. Additionally, system security and usability were analyzed using flse acceptance rate (FAR) and false rejection rate (FRR), defined as follows:

$$\text{FAR} = \frac{\text{Accepted Imposters}}{\text{Unauthorized Attempts}} \tag{10}$$

$$\text{FRR} = \frac{\text{Rejected Genuine Users}}{\text{Authorized Attempts}} \tag{11}$$

Finally, ROC curves were used to visualize the trade-off between the true positive rate (TPR) and false positive rate (FPR) under varying decision thresholds.

3 Results and Performance Analysis

This section outlines the evaluation approach used to assess the effectiveness of the proposed framework and explores the impact of EEG channel utilization on subject identification and authentication performance. Results from experiments conducted across multiple subjects are reported, with various performance metrics analyzed to validate the method's capability.

3.1 Implementation

The proposed classifier was trained using the adamW optimizer with default parameters with 100 epochs and a batch size of 64. EEG data were normalized, shuffled, and preprocessed using MNE-Python. Implemented in Python 3.8 with Keras 3.8.0 and TensorFlow 2.18.0, the model features three parallel EEGNet inspired branches with varying kernel sizes to extract multi-scale temporal spatial features. Residual connections and a channel attention module, integrating spatial and channel attention, refine feature representations. This enhances performance for P300-based EEG subject identification and authentication.

3.2 Results and Outcomes of the Subject Recognition Scheme (Identification and Authentication)

This section outlines the evaluation procedure of the proposed approach and examines the impact of EEG channels on recognition performance. A P300 ERP-based authentication test was conducted on EEG data collected from 16 subjects using the enhanced AMEEGNet model. The framework's performance was assessed for both subject identification and authentication tasks. Results

demonstrate the effectiveness of AMEEGNet in accurately capturing discriminative EEG patterns.

Subject identification is approached as a multi-class classification task, assigning a unique class label to each individual to distinguish them within the system. Table 2 presents the individual classification results for each subject following the application of the multi-class identification method. The performance of the model for subject identification was assessed using 5-fold stratified cross-validation, with precision-recall AUC and cohen's kappa as metrics to evaluate its ability to differentiate between various classes. The model obtained an average precision-recall AUC of 0.90- $SD = 0.0125$, p-value $= 0.0076$, demonstrating the ability to distinguish between various classes. The effectiveness of AMEEGNet was evaluated using the multi-class AUC-ROC metric. The AUC values, presented in Fig. 2 highlight the model's strong capability in distinguishing between subjects. The model's performance was assessed for each individual subject, as shown in Fig. 3, to identify areas of strength and challenge. Although the model achieved almost of 90% accuracy for most subjects, subjects 2 and 14 had accuracies below 80%. Nevertheless, with an overall accuracy of 89.25%, the model effectively captures P300 EPRs from EEG signals.

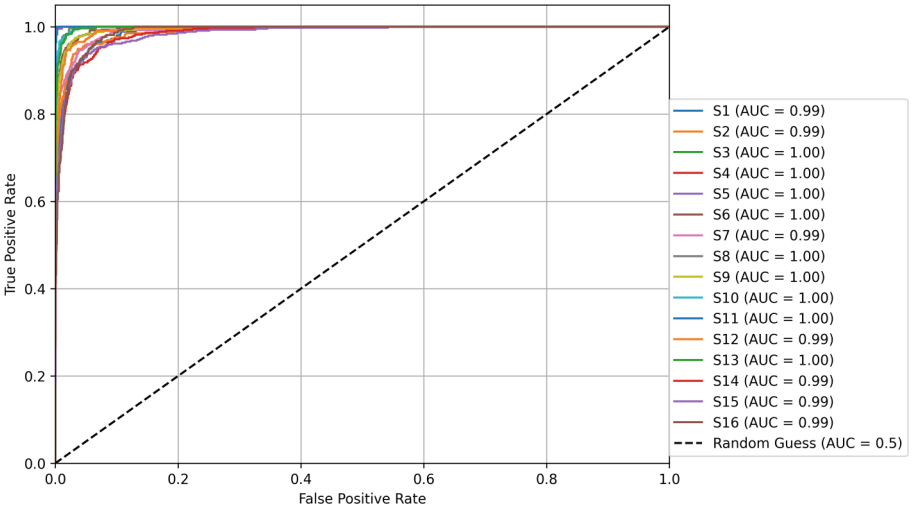

Fig. 2. ROC curves for the AMEEGNet-CAM model across multiple subjects, showing the true positive rate (TPR) versus false positive rate (FPR). AUC values indicate the model's classification performance, with the dashed line representing random guessing (AUC = 0.5).

Subject authentication was assessed using AMEEGNet-CAM by analyzing P300 ERPs from 16 subjects, making the task as a binary classification in which one subject represented the genuine user (1) and the other 15 were grouped as impostors (0). Mean accuracy of 89.25% was obtained for all subjects. The

Table 2. Subject identification performance of AMEEGNet-CAM on 16 subjects

Subject	Precision	Recall	F1-score	k-value
S01	0.72	0.93	0.81	0.80
S02	0.92	0.78	0.85	0.84
S03	1.00	0.99	0.99	0.99
S04	1.00	0.98	0.99	0.99
S05	0.98	0.95	0.97	0.96
S06	0.89	0.95	0.92	0.91
S07	0.81	0.94	0.87	0.86
S08	0.96	0.97	0.96	0.96
S09	0.95	0.89	0.92	0.92
S10	0.96	0.95	0.96	0.95
S11	0.93	0.98	0.95	0.95
S12	0.93	0.91	0.92	0.91
S13	0.94	0.96	0.95	0.95
S14	0.96	0.72	0.83	0.81
S15	0.85	0.87	0.86	0.85
S16	0.85	0.84	0.84	0.83

highest accuracy was obtained for the subject S03 and S04 (100%), while the lowest levels of accuracy were observed for the subject S01 (80%), which seems to be an outlier. The performance of the model for each user was evaluated using the proposed method, as outlined in Table 3. Figure 4 illustrates the classification performance of the proposed model, AMEEGNet-CAM, across 16 subjects using accuracy, precision, and f1 Score. The model achieved an average accuracy of 89.25%, demonstrating strong performance in EEG-based subject authentication. Individual accuracies ranged from 0.81 to 1.00, with precision values mostly above 0.90, indicating effectiveness in reducing false positives. Subjects S03 and S04 showed perfect classification, while S05 and S14 had slightly lower recall values, impacting their f1 scores. Overall, the model maintained high precision and stable performance across all subjects, showcasing its robustness and generalization capability. To further evaluate AMEEGNet's performance, sensitivity and specificity across 16 subjects were analyzed as shown in Fig. 5. Sensitivity ranged from 0.80 to 0.99, indicating consistent true positive. Specificity values were tightly clustered between 0.93 and 0.96, showing robustness in minimizing false positives. The compact distribution in the plot highlights model's reliability and stability, with minimal subject-specific variance. The high and balanced sensitivity and specificity underscore model's effectiveness for EEG-based subject authentication, ensuring accurate detection and minimal false alarms. The proposed scheme exhibited a minimal false acceptance rate (FAR), averaging 3.5% ($\pm$ 2.73%), and a false rejection rate (FRR) of 10.81% ($\pm$ 6.24%) across all

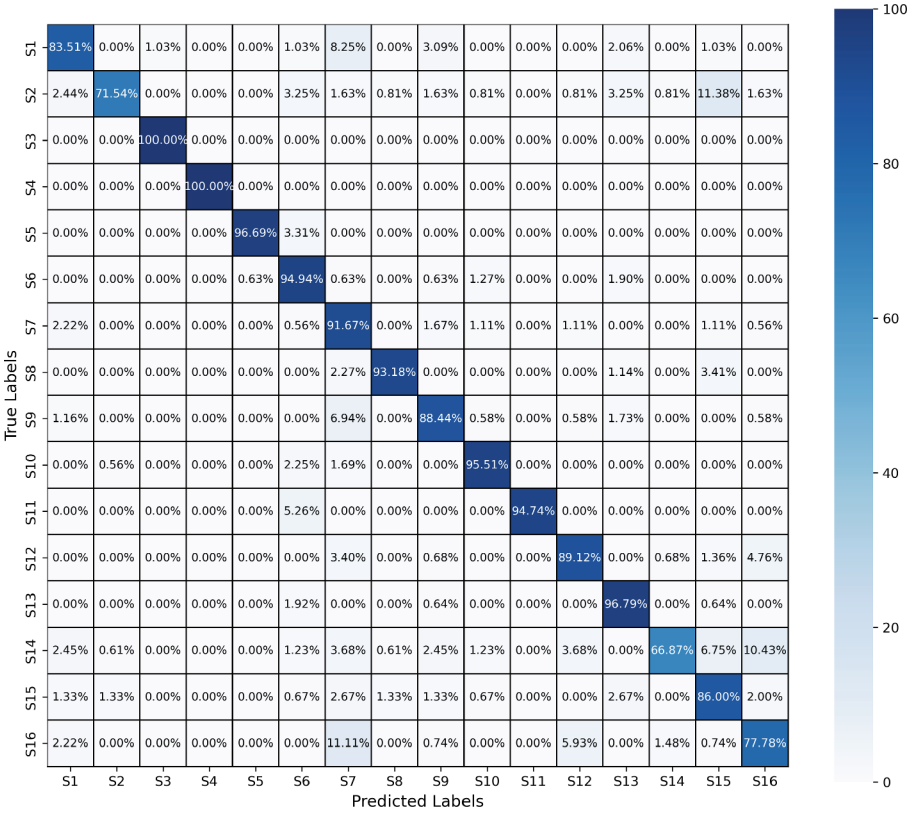

Fig. 3. Identification Accuracy of subjects. Confusion matrix illustrating the classification performance of the AMEEGNet-CAM model for subject identification, highlighting the accuracy and distribution of correct and incorrect predictions across subject classes.

subjects. This indicates its robust capability to accurately differentiate between genuine and impostors.

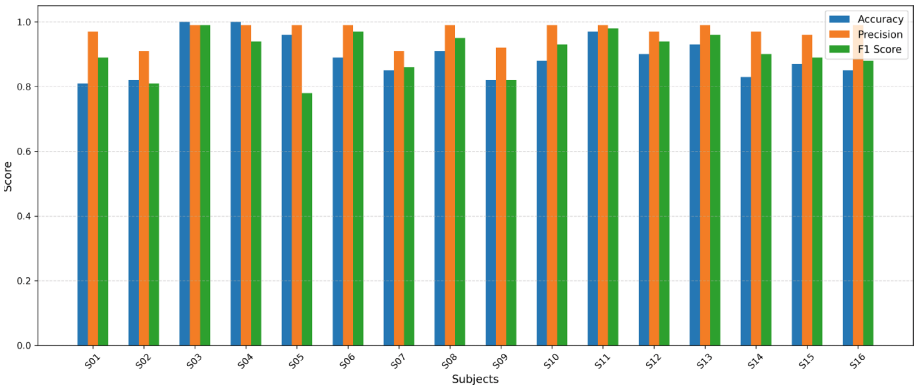

Fig. 4. Performance evaluation of the proposed model across all 16 subjects, illustrating key classification metrics including accuracy, precision, and f1 Score. The results indicate consistent and reliable performance.

Table 3. Subject authentication performance metrics (k-value, FRR, FAR, and accuracy) across 16 subjects for the 2021 samples using the AMEEGNet-CAM model

Subject	k-value	FRR	FAR	Accuracy
S01	0.18	0.03	0.03	81%
S02	0.54	0.20	0.02	82%
S03	0.99	0.01	0.01	100%
S04	0.99	0.03	0.01	100%
S05	0.76	0.06	0.01	96%
S06	0.28	0.04	0.01	89%
S07	0.23	0.16	0.09	85%
S08	0.47	0.08	0.01	91%
S09	0.17	0.19	0.08	82%
S10	0.54	0.12	0.01	88%
S11	0.42	0.03	0.01	97%
S12	0.47	0.08	0.03	90%
S13	0.65	0.07	0.07	93%
S14	0.30	0.16	0.01	83%
S15	0.33	0.16	0.03	87%
S16	0.23	0.20	0.04	85%

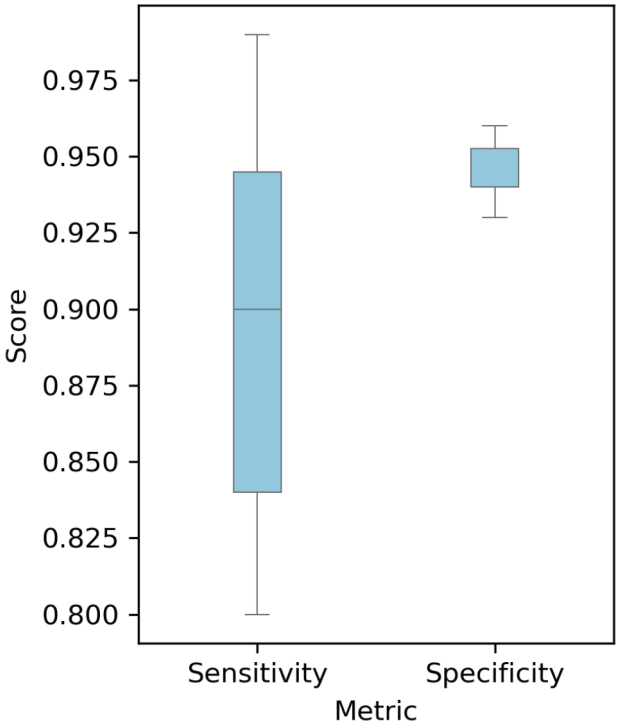

Fig. 5. Comparison of Sensitivity and Specificity values across all 16 subjects, highlighting the distribution and consistency of the model's performance.

4 Discussion and Conclusion

This study explored the use of an Enhanced AMEEGNet model for subject identification and authentication using P300 event related potentials (ERPs), achieving an overall accuracy of 89.25% and Cohen's kappa score of 0.88. As the first work to apply Enhanced AMEEGNet specifically to P300-based biometric authentication, it marks a novel contribution to EEG-based biometric research. The model showed strong generalization across users, with most individuals achieving high classification accuracy. Although some subjects were more challenging, the model remained effective, supporting its suitability for real-world application.

The proposed model demonstrates promising real-time potential for EEG-based authentication systems, thanks to its ability to capture spatiotemporal EEG dynamics efficiently. Its use of P300 ERPs as a biometric trait offers a secure and non-invasive approach for identity verification. Future research should focus on improving performance for low-performing users and exploring other ERP components, such as visual evoked potentials, to enhance biometric robustness. This work establishes a solid foundation for using Enhanced AMEEGNet in next-generation cognitive biometrics.

References

1. Wash, R., Rader, E.: Prioritizing security over usability: strategies for how people choose passwords. J. Cybersec. **7**(1), tyab012 (2021)
2. Galbally, J., Marcel, S., Fierrez, J.: Biometric antispoofing methods: a survey in face recognition. IEEE Access **2**, 1530–1552 (2014)
3. Armstrong, B.C., Ruiz-Blondet, M.V., Khalifian, N., Kurtz, K.J., Jin, Z., Laszlo, S.: BrainPrint: assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics. Neurocomputing **166**, 59–67 (2015)
4. Khalil, A.E.K., Perez-Diaz, J.A., Cantoral-Ceballos, J.A., Antelis, J.M.: Unlocking security for comprehensive electroencephalogram-based user authentication systems. Sensors **24**(24), 7919 (2024)
5. Kumari, P., Vaish, A.: Brainwave based user identification system: a pilot study in robotics environment. Robot. Auton. Syst. **65**, 15–23 (2015)
6. Maiorana, E., La Rocca, D., Campisi, P.: On the permanence of EEG signals for biometric recognition. IEEE Trans. Inf. Forensics Secur. **11**(1), 163–175 (2015)
7. Chen, Y., et al.: A high-security EEG-based login system with RSVP stimuli and dry electrodes. IEEE Trans. Inf. Forensics Secur. **11**(12), 2635–2647 (2016)
8. Seha, S.N.A., Hatzinakos, D.: EEG-based human recognition using steady-state AEPs and subject-unique spatial filters. IEEE Trans. Inf. Forensics Secur. **15**, 3901–3910 (2020)
9. Jin, J., et al.: Optimized stimulus presentation patterns for an event-related potential EEG-based brain–computer interface. Med. Biol. Eng. Comput. **49**, 181–191 (2011)
10. Combaz, A., Van Hulle, M.M.: Simultaneous detection of P300 and steady-state visually evoked potentials for hybrid brain-computer interface. PLoS ONE **10**(3), e0121481 (2015). https://doi.org/10.3886/ICPSR30122.v2
11. Combaz, A., Van Hulle, M.M.: Simultaneous detection of P300 and steady-state visually evoked potentials for hybrid brain-computer interface. PLoS ONE **10**(3), e0121481 (2015)
12. Khalil, A.E.K., Pérez-Díaz, J.A., Cantoral-Ceballos, J.A., Antelis, J.M.: Enhancing user authentication through EEG based P300 speller response. In: In: Martínez-Villaseñor, L., Ochoa-Ruiz, G. (eds) Advances in Soft Computing. MICAI 2024. LNCS, vol. 15247, pp. 124–141. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-75543-9_10
13. Rathi, N., Singla, R., Tiwari, S.: A novel approach for designing authentication system using a picture based P300 speller. Cogn. Neurodyn., 1–20 (2021)
14. Akram, F., Alwakeel, A., Alwakeel, M., Hijji, M., Masud, U.: A symbols based BCI paradigm for intelligent home control using P300 event-related potentials. Sensors **22**(24), 10000 (2022)
15. Zhang, S., Sun, L., Mao, X., Hu, C., Liu, P.: Review on EEG-based authentication technology. Comput. Intell. Neurosci. **2021**(1), 5229576 (2021)
16. Santamaría-Vázquez, E., Martínez-Cagigal, V., Gomez-Pilar, J., Hornero, R.: Asynchronous control of ERP-based BCI spellers using steady-state visual evoked potentials elicited by peripheral stimuli. IEEE Trans. Neural Syst. Rehabil. Eng. **27**(9), 1883–1892 (2019)
17. Zeng, Y., et al.: EEG-based identity authentication framework using face rapid serial visual presentation with optimized channels. Sensors **19**(1), 6 (2018)
18. Chan, H.L., Kuo, P.C., Cheng, C.Y., Chen, Y.S.: Challenges and future perspectives on electroencephalogram-based biometrics in person recognition. Front. Neuroinform. **12**, 66 (2018)

19. Maiorana, E., Solé-Casals, J., Campisi, P.: EEG signal preprocessing for biometric recognition. Mach. Vis. Appl. **27**, 1351–1360 (2016)
20. Mao, Z., Yao, W.X., Huang, Y.: EEG-based biometric identification with deep learning. In: 2017 8th International IEEE/EMBS Conference on Neural Engineering (NER), pp. 609–612. IEEE (2017)
21. Roy, A.M.: An efficient multi-scale CNN model with intrinsic feature integration for motor imagery EEG subject classification in brain-machine interfaces. Biomed. Signal Process. Control **74**, 103496 (2022)
22. Lawhern, V.J., Solon, A.J., Waytowich, N.R., Gordon, S.M., Hung, C.P., Lance, B.J.: EEGNet: a compact convolutional neural network for EEG-based brain–computer interfaces. J. Neural Eng. **15**(5), 056013 (2018)
23. Wu, X., Chu, Y., Li, Q., Luo, Y., Zhao, Y., Zhao, X.: AMEEGNet: attention-based multiscale EEGNet for effective motor imagery EEG decoding. Front. Neurorobot. **19**, 1540033 (2025)
24. Gramfort, A., et al.: MEG and EEG data analysis with MNE-Python. Front. Neuroinform. **7**, 267 (2013)
25. Chailloux Peguero, J.D., Mendoza-Montoya, O., Antelis, J.M.: Single-option P300-BCI performance is affected by visual stimulation conditions. Sensors **20**(24), 7198 (2020)