

Article

Brainwave Biometrics: A Secure and Scalable Brain–Computer Interface-Based Authentication System

Mashaël Aldayel ^{1,*} , Nouf Alsedairy ² and Abeer Al-Nafjan ³ 

¹ Information Technology Department, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

² National Center for Communication Systems and Command and Control Technology, King Abdulaziz City for Science and Technology (KACST), Riyadh 11442, Saudi Arabia; nalsedairy@kacst.edu.sa

³ Computer Science Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia; annafjan@imamu.edu.sa

* Correspondence: maldayel@ksu.edu.sa

Abstract

This study introduces a promising authentication framework utilizing brain–computer interface (BCI) technology to enhance both security protocols and user experience. A key strength of this approach lies in its reliance on objective, physiological signals—specifically, brainwave patterns—which are inherently difficult to replicate or forge, thereby providing a robust foundation for secure authentication. The authentication system was developed and implemented in four sequential stages: signal acquisition, preprocessing, feature extraction, and classification. Objective feature extraction methods, including Fisher’s Linear Discriminant (FLD) and Discrete Wavelet Transform (DWT), were employed to isolate meaningful brainwave features. These features were then classified using advanced machine learning techniques, with Quadratic Discriminant Analysis (QDA) and Convolutional Neural Networks (CNN) achieving accuracy rates exceeding 99%. These results highlight the effectiveness of the proposed BCI-based system and underscore the value of objective, data-driven methodologies in developing secure and user-friendly authentication solutions. To further address usability and efficiency, the number of BCI channels was systematically reduced from 64 to 32, and then to 16, resulting in accuracy rates of 92.64% and 80.18%, respectively. This reduction streamlined the authentication process, demonstrating that objective methods can maintain high performance even with simplified hardware and pointing to future directions for practical, real-world implementation. Additionally, we developed a real-time application using our custom dataset, reaching 99.75% accuracy with a CNN model.

Keywords: biometrics; authentication; brain–computer interface; EEG; signal processing; usability and security



Academic Editor: Mohammed Abdulhakim Al-Absi

Received: 16 July 2025

Revised: 19 August 2025

Accepted: 20 August 2025

Published: 28 August 2025

Citation: Aldayel, M.; Alsedairy, N.; Al-Nafjan, A. Brainwave Biometrics: A Secure and Scalable Brain–Computer Interface-Based Authentication System. *AI* **2025**, *6*, 205. <https://doi.org/10.3390/ai6090205>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Authentication—the process of verifying a user’s identity before granting system access—is a fundamental component of information security. Traditionally, authentication methods have relied on three primary factors: something the user knows (e.g., passwords or PINs), something the user has (e.g., security tokens or smart cards), and something the user is (e.g., biometric traits). However, knowledge-based and possession-based methods are susceptible to various attacks, including interception, theft, and social engineering.

Even biometric authentication, which leverages inherent physiological or behavioral characteristics such as fingerprints or facial features, can be vulnerable to sophisticated spoofing and presentation attacks [1–3].

Recent advances in biometric technologies have expanded the landscape of authentication methods. Some authentication approaches, such as voice recognition, iris scanning, and behavioral biometrics, offer enhanced security, yet each comes with its own limitations regarding accuracy, user acceptance, and vulnerability to forgery. Among these, brain–computer interface (BCI) technology has attracted significant attention as an emerging approach to authentication. BCIs enable direct communication between the human brain and external devices, capturing unique neural activity patterns that are difficult to replicate [1,4–6].

Electroencephalography (EEG), a non-invasive technique for recording electrical brain activity, is particularly promising in this context. EEG signals exhibit individual-specific temporal and spectral characteristics, making them highly distinctive and resilient to forgery. Moreover, EEG is sensitive to cognitive and emotional states, further complicating attempts at impersonation [4,6]. These properties position EEG-based authentication as a compelling alternative to traditional biometrics [7,8].

Despite its potential, EEG-based authentication faces several practical challenges. High-density EEG devices can be costly and cumbersome, potentially impacting user comfort and system usability. Furthermore, the non-stationary nature of EEG signals—affected by factors such as user fatigue, mood, or environmental conditions—necessitates advanced signal processing and machine learning techniques to ensure robust and reliable authentication [1,3,9].

BCI technology, by facilitating direct interaction between users and digital systems without muscular input, provides a promising platform for secure authentication. The inherent complexity and uniqueness of brain signals make them an attractive biometric trait for robust identity verification [3]. In this study, we propose and evaluate a comprehensive BCI-based authentication system using publicly available EEG dataset, named the PhysioNet EEG Motor Movement/Imagery Dataset, to assess its generalizability and practical viability. The proposed system operates in two primary phases: registration and authentication. During registration, a user's EEG signals are recorded, preprocessed, and transformed into feature vectors stored in a secure database. In the authentication phase, new EEG data from the user are similarly processed and compared against the stored templates to verify identity. Access is granted only when a sufficient match is established between the real-time features and the stored data.

The authentication framework comprises four main components: signal acquisition, preprocessing, feature extraction, and classification. Signal acquisition involves recording brainwave activity from users. Preprocessing steps such as noise reduction and artifact removal are applied to enhance data quality. Feature extraction identifies distinctive patterns in the EEG data, which serve as the basis for user differentiation. Finally, a classification model is trained to recognize individual users based on these features, and the resulting models are stored for future authentication attempts.

The main objectives of this study are twofold: (1) to achieve high authentication accuracy and reliability through robust feature extraction and classification techniques and (2) to enhance user experience by reducing the number of EEG channels required, thereby improving practicality without compromising security. These objectives are demonstrated through two experimental setups, focusing on system performance and usability, respectively.

The remainder of this research is structured as follows: Section 2 reviews the relevant literature, Section 3 details the methodology, Section 4 presents the results and discussion, and Section 5 provides the conclusion and future directions.

2. Literature Review

EEG-based authentication is attracting more interest due to its potential to provide secure, user-specific biometric verification. Several experimental designs have been examined, each utilizing a variety of preprocessing techniques, feature extraction strategies, and classification models to optimize identification performance.

Yu et al. [2] implemented an authentication system based on the P300 BCI paradigm, applying feature extraction through filtering and decimation, and classification using Fisher's Linear Discriminant (FLD). Using images of individuals as external stimuli, the system achieved an accuracy of 83.1%. Similarly, Nakamura et al. [1] applied average reference preprocessing and extracted power spectral density (PSD) features, which were subsequently classified using a Support Vector Machine (SVM), achieving an accuracy of 94.5%.

Meanwhile, other researchers have employed multiple feature extraction algorithms to enhance recognition accuracy. Kang et al. [5] developed a multimodal feature extraction pipeline incorporating bandpass filtering, Hilbert transform, and notch filtering, achieving 98.93% accuracy using Euclidean distance. Similarly, Zeynali and Seyedarabi [4] conducted a comparative study of three feature extraction techniques: Discrete Fourier Transform, Discrete Wavelet Transform (DWT), and Autoregressive modeling. These features were evaluated with various classifiers, including SVM, Bayesian Networks, and neural networks, achieving accuracies ranging from 84.49% to 92.89%.

Some research has utilized a hybrid authentication, such as that of Wu et al. [6], who combined EEG signals with eye-blinking data. EEG features were extracted using Event-Related Potentials and classified with Convolutional Neural Networks (CNNs), while blink data were analyzed using a backpropagation neural network. This multimodal system achieved 97.6% accuracy. Additionally, Zeng et al. [10] explored a bimodal system that integrated facial recognition with EEG signals. They extracted features using FLD and employed Hierarchical Discriminant Component Analysis for classification. Utilizing 195 face images as stimuli, the system achieved an average accuracy of 88.88%.

In addition to visual stimuli, auditory stimuli have also been explored in EEG-based biometric systems. For example, Seha and Hatzinakos [3] examined the use of steady-state Auditory Evoked Potentials, applying Canonical Correlation Analysis for feature extraction and Linear Discriminant Analysis for classification. Their system achieved a classification accuracy of 96.46%, highlighting the potential of auditory stimuli in EEG-based biometrics. Thomas et al. [11] emphasized the significance of high-frequency EEG oscillations, particularly in the gamma band, for user identification. They extracted PSD features and classified them using Mahalanobis distance, achieving an accuracy of 90%.

Several studies have emphasized usability by reducing the number of EEG channels necessary for authentication. Ortega et al. [7] proposed an EEG authentication system using a minimal number of channels. With Principal Component Analysis and Wilcoxon ranking for feature extraction and SVM for classification, the system achieved 100% accuracy on a 13-subject dataset. TajDini et al. [12] proposed an EEG-based authentication system using mental tasks recorded from a reduced number of channels. The study utilized PSD for feature extraction and applied an SVM for classification. Their method achieved an accuracy of 91.6%, demonstrating the feasibility of effective biometric authentication with fewer electrodes.

Waili et al. [13] developed a low-complexity, EEG-based biometric authentication system aimed at enhancing usability in real-world applications. They utilized basic statistical features extracted from raw EEG signals and classified them using a decision tree classifier. The system achieved a reported accuracy of 90.1%, emphasizing feasibility in constrained environments with minimal hardware requirements. Suppiah and Vinod [14] proposed a

single-channel EEG biometric system for user identification during relaxed resting states. This system uses PSD and a k-nearest neighbors (k-NN) classifier with majority voting, demonstrating a high identification accuracy of 96.67% across all channels and 97% based on single channel.

Overall, this body of research highlights a wide variety of effective methodologies. While FLD, PSD, and used average reference were among the most-used feature extraction techniques, neural networks and SVM emerged as the most frequently employed classifiers. The consistent use of multimodal inputs and deep learning architectures reflects a broader trend toward hybrid and adaptive EEG-based authentication systems capable of delivering high performance and robustness. Despite these advancements, existing approaches lack a balanced approach to optimizing the trade-off between security robustness and practical usability in authentication frameworks. Our study aims to bridge this gap, underlining the need for a systematic framework that jointly maximizes security and usability constraints.

3. Methodology

In this section, we describe the methodology and design aspects of the proposed BCI-based system, which ensures the accurate identification and verification of users based on their unique brainwave patterns. The following subsections section explains the system architecture and its components, description of the public benchmark dataset used in this study, and system usability.

3.1. System Architecture

The proposed BCI-based system architecture (Figure 1) consists of two primary phases: (1) registration and (2) authentication. The proposed system involves a registration process to gather and record a user's unique brain signals. During this phase, users typically wear a BCI headset equipped with sensors to monitor their brain's electrical activity. During the authentication phase, brainwave signals (EEG) are recorded while the user performs predefined mental tasks or responds to specific stimuli. Distinctive features are then extracted from these signals (e.g., power spectral density, entropy measures, or connectivity patterns) and compared against a stored template using machine learning classifiers to verify the user's identity. For the matching process, the BCI-based authentication system will compare a user's brainwaves with predefined templates (gathered during the registration phase). Authentication will be successful if a match is found, after which the system will accept the user's access. Otherwise, if the brainwave patterns do not closely match the predefined templates, authentication fails, and access is rejected.

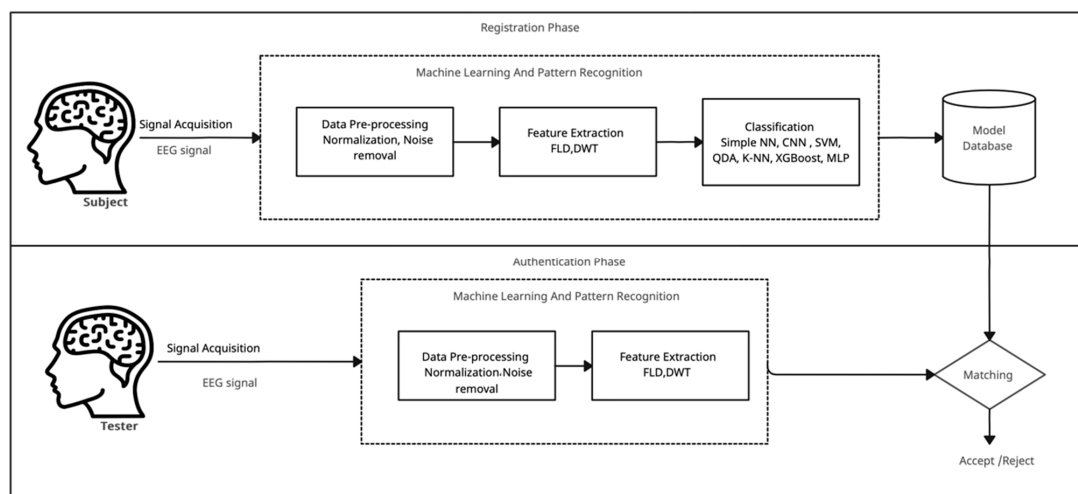


Figure 1. System architecture: registration and authentication phases.

The registration phase encompasses several crucial components, including signal acquisition and preprocessing, feature extraction, classification, and database modeling. The first three components follow the same methodology as in the authentication phase. A detailed explanation of each component is provided in the next subsections.

3.1.1. Signal Acquisition and Preprocessing

We implemented normalization techniques to standardize the EEG signals. Normalization is essential for ensuring uniformity and comparability across disparate scales in the dataset, thereby enhancing the efficacy and performance of machine learning algorithms. Then, we added a new column named “user” as a target label to assign user identity. We removed rows with zero values from the dataset. Before cleaning, the dataset contained 1,063,200 entries. Following the cleaning process, 13,688 rows were removed, resulting in 1,049,512 entries.

3.1.2. Feature Extraction

We transformed the preprocessed signals to extract the essential information needed to produce a simplified representation that preserved the most vital aspects. Fisher’s Linear Discriminant (FLD) and Discrete Wavelet Transform (DWT) were used for feature extraction, as they have been extensively used in previous research [2,15–17]. FLD effectively reduces dimensionality and discriminates between classes, whereas DWT provides a means of decomposing signals into frequency components for analysis.

FLD can project high-direction dimensional data onto a lower-dimensional subspace while concurrently preserving discriminatory information across distinct classes, i.e., maximize class separation while minimizing variance within classes. The objective of FLD is to ascertain a linear transformation that optimizes the ratio between the scatter attributed to inter-class variations and that ascribed to intra-class variations, thereby augmenting the discernibility of disparate classes within the feature space [2,10,16,18]. DWT is a signal-processing technique that decomposes signals into different frequency bands, thereby providing a time-frequency representation of the signals. When used in EEG analysis, DWT captures localized features and thus facilitates multi-resolution analysis, while also aiding in the identification of patterns associated with cognitive states.

3.1.3. Classification

Different classification methodologies were applied, including traditional classifiers, such as SVM, QDA, k-NN, XGBoost, and MLP and deep learning models, such as simple NN and CNN. In the next paragraphs, we provided a description of each algorithm used.

SVM with RBF kernels are particularly effective and can accurately work well with non-linear complex patterns in user data, such as brainwave signals, from EEG measurements. Additionally, SVM with RBF kernels is well known for its generalization capabilities, making it a reliable choice for secure and efficient authentication systems [19].

QDA can model complex decision boundaries captures class-specific variance. It is possible to identify and verify users using QDA precisely due to its flexibility in accounting for different covariance structures between classes. Moreover, QDA’s probabilistic approach enhances the robustness of the system by providing confidence in its predictions [15].

K-NN identifies the k closest data points to a given input and classifies each point based on proximity. The algorithm can be fine-tuned to achieve optimal performance by adjusting the number of neighbors (k) [19].

XGBoost: By using an ensemble of decision trees, it learns complex patterns in large data. Fast training and prediction times make XGBoost suitable for real-time authentication. As a result of its capability to handle large datasets and prevent overfitting through regularization, it ensures the robust and reliable identification and verification of users [20].

MLP consists of multiple layers of neurons capable of learning intricate features from data. Its flexibility in designing its architecture, such as the number of layers and neurons, makes it suitable for a variety of authentication scenarios [8].

Tensorflow and Keras were used to implement a NN model for classifying user data. Initially, user identifiers were encoded using LabelEncoder to transform categorical labels into numerical values. The NN architecture was constructed with a sequential model comprising three dense layers: an input layer with 64 units, a hidden layer with 32 units, both employing the ReLU activation function, and an output layer with a softmax activation function tailored to the number of unique classes in the target variable. The model was compiled with the Adam optimizer, was set to a learning rate of 0.001, and used sparse categorical cross-entropy as the loss function to handle multi-class classification. To prevent overfitting, a callback was included to monitor the validation loss to stop the process early.

CNN was designed to efficiently extract and learn features from the input data for the classification task. Figure 2 illustrates the architectural design of the CNN model. The model was initiated with a Conv1D layer with 64 filters and a kernel size of 3. The ReLU activation function introduces nonlinearity and facilitates feature learning. Batch normalization normalizes the activations of the previous layer, which then stabilizes and accelerates the training process. Sub-sampling is performed using a max pooling layer with a pool size of 2 to reduce the spatial dimensions of the feature maps. After the first Conv1D layer, dropout regularization is employed at a rate of 0.3 to prevent overfitting by randomly removing 30% of the input units during training. Reducing neuronal interdependence improves the model's generalization performance. An additional Conv1D layer with 32 filters and a kernel size of 3 was added to the second convolutional block. As with the first block, ReLU activation and batch normalization were applied to introduce nonlinearity and normalize activations.

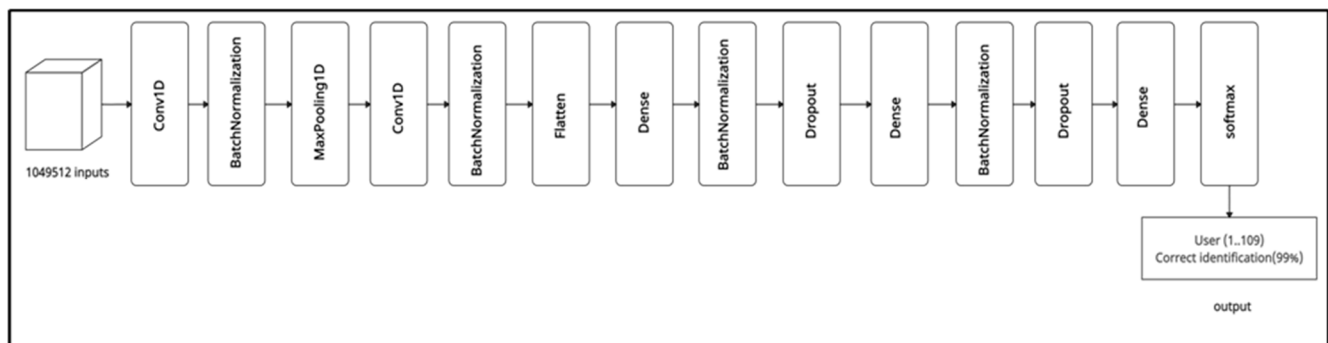


Figure 2. Schematic representation of the CNN architecture.

The flatten layer transforms the multidimensional feature maps into one-dimensional vectors, thereby preparing them for input to the fully connected layers. Following the convolutional layers, fully connected dense layers were added to further process the extracted features. The first dense layer consisted of 512 units with ReLU activation and batch normalization. After the first dense layer, dropout regularization was applied at a rate of 0.3. A second dense layer with 256 units, ReLU activation, and batch normalization was then applied. After the second dense layer, dropout regularization at a rate of 0.3 was again employed. A dense layer of 64 units with ReLU activation was added as a final step. The output layer, which is suitable for tasks involving multi-class classification, is completed by a dense layer feeding a softmax activation function. In this layer, the number of units is determined by the number of unique classes in the target variable.

3.2. Dataset Description

The EEG Motor Movement/Imagery Dataset (EEGMMIDB) record brain activity during motor imagery tasks for BCI research. EEGMMIDB dataset developed by Goldberger et al. In 2000 and made publicly available by PhysioNet [21]. The dataset was recorded using the BCI2000 system, a widely used platform for BCI research, and it provides valuable information regarding neural responses during motor imagery. Several studies related to BCI and EEG-based authentication have used this dataset [5,11,13,14,22–25]. A description of the dataset can be found in Table 1.

Table 1. Summary of characteristics of EEG dataset.

Participants	109 volunteers
Stimuli type	Different motor/imagery tasks such as open eyes, closed eyes, moves left/right hand, imagine moves left/right hand, open fists, imagine fists, open feet, and imagine feet.
Stimuli duration	Recordings of the EEG for one minute and two minutes.
Stimuli arrangement	During the experiment, the subjects were asked to perform 14 experimental runs: two one-minute baseline runs (one with the eyes open and one with the eyes closed) and three two-minute runs with other tasks.
Experiment protocol	A total of 14 experimental runs were conducted using the BCI2000 system, which involved a variety of tasks. First, there were two one-minute baseline runs, with eyes open and closed. Four tasks involved motor/imagery actions in response to visual cues displayed on the screen. The tasks included mimicking and imagining fist or foot movements based on screen targets.
Electrodes	An electrode system of 64 electrodes was used in accordance with the international 10-10 system (excluding electrodes Nz, F9, F10, FT9, FT10, A1, A2, TP9, TP10, P9, and P10).

This dataset consists of EEG recordings from 109 healthy volunteers engaged in various motor and imagery tasks. EEG signals were recorded at 160 Hz using 64 channels. Participants completed 14 experimental runs, including two baseline runs (one with eyes open and one with eyes closed) and three two-minute runs for each of the four different tasks. The participants were required to physically open and close their left or right fists or visualize such movements. Furthermore, participants were required to open and close their feet and imagine doing so. For authentication purpose, we used EEG signals collected during rest state tasks with eyes opened and eyes closed, processed to remove noise, and fed into classification algorithms to verify identity based on brainwave patterns [26,27].

3.3. System Usability

Channel selection was utilized to improve the practical usability of the authentication system by minimizing the number of EEG channels, thus reducing system complexity and making the process more convenient for end-users. We focused on channel selection to enhance usability within the authentication process based on related research that highlights the most related channels used in authentication. Using correlation analysis and insights from previous studies, we took a systematic approach to selecting the most relevant channels for the analysis.

3.3.1. Based on Correlation Analysis

We measured the relationship between EEG recordings obtained using the open eyes task and the target label using correlation analysis in the EEGMMIDB dataset. The following channels were ranked according to their effectiveness based on the same dataset as shown in the left side of Figure 3. The right side of Figure 3 presents these numbers that reflect channels FP1, FPZ, AF7, FP2, T10, AF4, FC5, PO8, T7, AF8, AFZ, and FC4 as well.

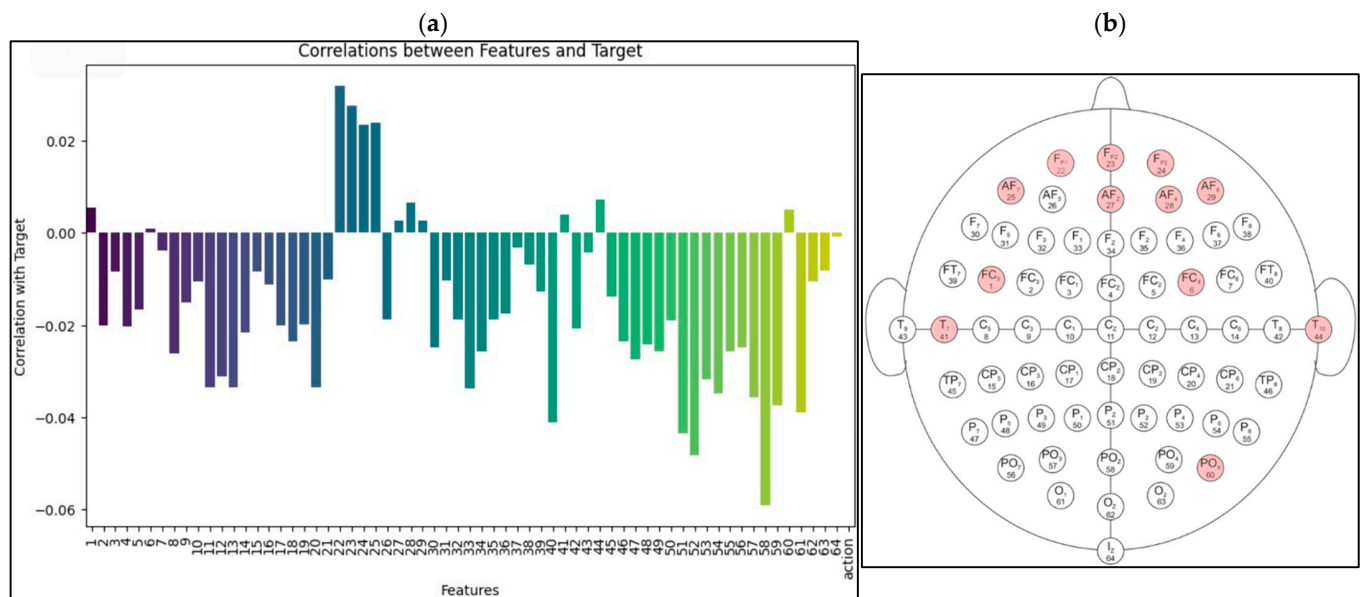


Figure 3. Most effective channels based on correlation analysis in (a) with corresponding reflected channels in (b).

3.3.2. Based on Related Research

Based on our literature review of studies utilizing the same dataset, we observed a consistent choice of channels. Table 2 presents the channels employed in these studies. The common channels used were FP1, FP2, F3, FZ, F4, and F7. Based on the analysis of the most effective channels from the correlation analysis, FP1 and FP2 had already been selected. As a result, we can say that the selected channels were as follows: FP1, FPZ, AF7, FP2, T10, AF4, FC5, PO8, F3, FZ, F4, and F7.

Table 2. Channels utilized in studies employing the same dataset.

Reference	Channels
Thomas and Vinod 2018 [11]	FP1, FP2, F3, F4, FZ, F7, F8, T7, T8, C3, CZ, C4, P3, PZ, P4, P7, P8, O1, O2
Ortega-Rodríguez et al., 2023 [7]	F7, F5, F3, F1, FZ, AF7, AF3, AFZ, FP1, FPZ, FT7, FC5, FC3, FC1, C5, C3
Bidgoly et al., 2022 [23]	FP1, AF3, F7, F3, FZ, FC5, FC1, FP2, AF4, F4, FC2, FC6, F8, T7, C3, CZ, C4, T8, CP5, CP1, CP2, CP6, P7, P3, PZ, P4, P8, PO3, PO4, O1, OZ, O2

4. Results and Discussion

Traditional classification and deep learning methodologies were applied using different methods of feature extraction (FLD and DWT). The classifiers were SVM with an RBF kernel, QDA, k-NN, XGboost, and MLP. We designed two experiments: Experiment-1 to evaluate accuracy and performance of classification models and Experiment-2 to evaluate the system usability based on number of selected channels. Experiment-2 aimed to enhance the user experience in BCI authentication by minimizing the number of channels or electrodes required to acquire signals. Specifically, we examined the transition from 64 channels to 32 channels and then to 16 channels. The goal was to simplify the BCI authentication process by systematically reducing the number of channels and making it more user-friendly and efficient. Additionally, we compared the results of our model with those of other related studies utilizing the same dataset using machine learning evaluation metrics.

4.1. Evaluation Metrics

To maintain consistency and relevance in the system evaluation, we conducted a quantitative assessment based on well-established machine learning evaluation metrics for comparison with similar prior studies [5,7,11,14]. This comprehensive analysis aimed to evaluate the performance, accuracy, and efficacy of our algorithm against established benchmarks in the literature. For evaluation of machine learning, we partition the available data into training and testing sets to evaluate the performance of a model. This study involved splitting the data with a ratio of 80% for training data and 20% for testing data. During the training phase, the model was exposed to training data, which allowed it to learn patterns and relationships within that dataset. Following this, the model's performance was assessed using the testing data, which the model had not encountered during training. This approach helped determine how well the model could be generalized to new, unseen data. The performance of each method was evaluated based on machine learning metrics, such as accuracy, false acceptance rate (FAR), false rejection rate (FRR), equal error rate (EER), precision, recall, and F1 measure.

Accuracy was measured in terms of the percentage of correctly predicted instances among the total number of instances. FAR is the rate at which an unauthorized person is accepted or has access to the system, as shown in Equation (1), where NFR is the number of false rejections, and NAA is the number of authenticated attempts.

$$FAR = \frac{NFR}{NAA} \times 100 \quad (1)$$

FRR is the rate at which an authorized person is rejected, as shown in Equation (2), where NFA is the number of false acceptances, and NIA is the number of impostor attempts. Equal error rate (EER) is shown in Equation (3).

$$FRR = \frac{NFA}{NIA} \times 100 \quad (2)$$

$$EER = \frac{FAR + FRR}{2} \quad (3)$$

Precision is a critical metric in biometric authentication that measures the system's ability to identify actual positive instances among the total predicted positive instances. Equation (4) shows the precision calculation, where true positives (TP) are the model that correctly predicts the positive outcome, and FP is the model that incorrectly predicts the positive outcome.

$$\text{Precision} = \frac{TP}{TP + FP} \quad (4)$$

Recall is defined as the ratio of true positive predictions to the total number of positive instances. Equation (5) present recall, where false negative (FN) means that the model incorrectly predicts the negative outcome.

$$\text{Recall} = \frac{TP}{TP + FN} \quad (5)$$

F1 score is computed as the harmonic mean of precision and recall, which then provides a single value for model performance (Equation (6)).

$$F1 \text{ score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (6)$$

4.2. Experiment-1: System Performance

In Experiment-1, we evaluated classification models to achieve high accuracy and reliability. Our study includes a comparison of the results using the DWT and FLD feature extraction methods to assess the performance of machine learning and deep learning classifiers. Each classifier was examined in terms of accuracy, F1 score, recall, and precision, as well as security metrics, such as FAR, FRR, and EER. Tables 3 and 4 present the results of various classification methodologies using FLD and the DWT feature extraction method. A comparison of the performances with DWT and FLD is illustrated in Figure 4.

Table 3. Results of FLD feature extraction with machine learning and deep learning models.

Classifier	Accuracy	F1 Score	Recall	Precision	FAR	FRR	EER
SVM	89.11%	89%	89%	90%	0.1030	0.1091	0.1060
QDA	99.64%	100%	10%	100%	0.0035	0.0036	0.0035
K-NN	95.79%	96%	96%	96%	0.0365	0.0422	0.0393
Xgboost	85.12%	85%	85%	85%	0.1464	0.1490	0.1477
MLP	92.03%	92%	92%	92%	0.0793	0.0799	0.0796
Simple NN	89.13%	89%	89%	89%	0.1074	0.1090	0.1082
CNN	99.41%	99%	99%	99%	0.0058	0.0059	0.0059

Table 4. Results of DWT feature extraction with machine learning and deep learning models.

Classifier	Accuracy	F1 Score	Recall	Precision	FAR	FRR	EER
SVM	65.72%	66%	66%	68%	0.3203	0.3429	0.3316
QDA	99.64%	100%	100%	100%	0.0035	0.0036	0.0035
K-NN	83.78%	84%	84%	88%	0.1221	0.1625	0.1423
Xgboost	80.12%	80%	80%	81%	0.1945	0.1988	0.1966
MLP	89.58%	90%	90%	90%	0.1027	0.1042	0.1034
NN	87.59%	88%	88%	88%	0.1211	0.1244	0.1228
CNN	99.38%	99%	99%	99%	0.0061	0.0062	0.0061

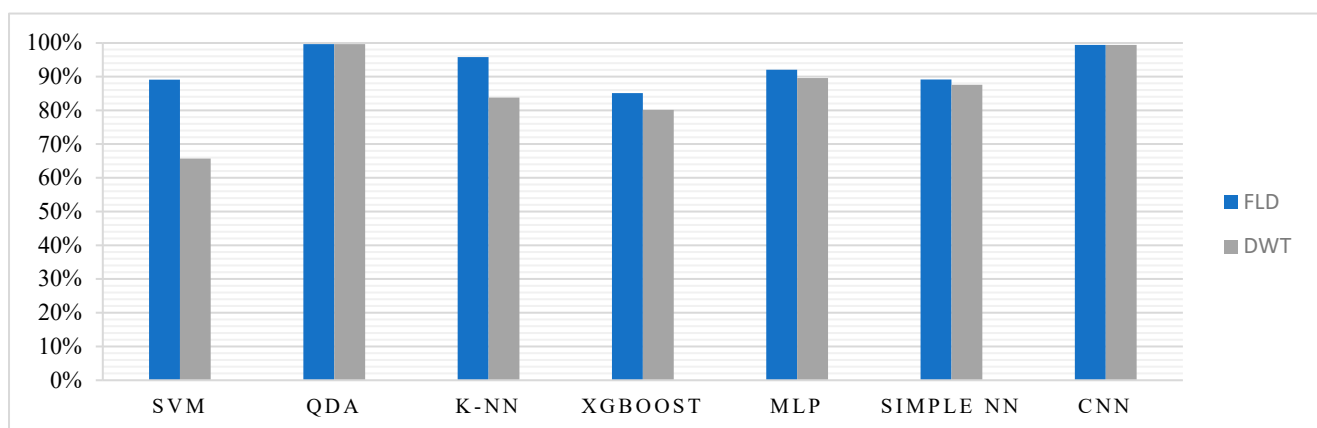


Figure 4. Comparison between DWT and FLD based on the accuracy performance of classifiers.

QDA: Both the FLD and DWT feature extraction methods yielded notable similarities in the performance of the QDA classifier. Both configurations exhibited exceptional accuracy, with a combined accuracy score of 99.64%. Both classifiers achieved or were very close to achieving 100% precision, recall, and F1 scores. In both configurations, the FAR and FRR were extremely low, with values of 0.0035, indicating a minimal risk of misidentification. Regardless of the feature extraction method used, the QDA classifier maintained high reliability, making it an ideal model for sensitive systems. Although both

methods exhibited a comparable performance, the choice between FLD and DWT may depend on specific application requirements or the nature of the dataset.

K-NN: Robust performance in identity classification has been demonstrated by the integration of FLD with the k-NN classifier. With FLD, k-NN achieved an excellent accuracy of 95.79%, allowing for the precise identification of individuals with a balanced precision, recall, and F1 score. The FAR of 0.0365 and FRR of 0.0422 indicate moderate error rates; however, further optimization can refine the balance between false acceptances and rejections. Conversely, DWT combined with k-NN yielded a good accuracy of 83.78% and a good precision of 88%. While k-NN had slightly higher error rates, its balanced EER of 0.0393 underscores its suitability for authentication systems. Overall, the collaborative integration of FLD and k-NN offers promising avenues for effective identification, thereby enabling adaptable solutions for various security environments.

XGBoost: As a result of DWT, XGBoost achieved an accuracy of 80.12% and an F1 score of 80%, while maintaining a precision of 81%. The classifier's error rates, FARs, and FRRs remained acceptable for XGBoost with DWT. A coefficient of 0.1966 indicates a balanced trade-off between accuracy and error. However, in the case of FLD, XGBoost exhibited an accuracy of 95.79%, indicating excellent performance in identity classification, with balanced precision, recall, and F1 scores of 96%. The FAR of 0.0365 and the FRR of 0.0422 indicate a moderate risk of error, but further optimization could balance false acceptances and rejections. In general, XGBoost with FLD provides superior accuracy and performance for sensitive systems.

MLP: With FLD, MLP achieved a higher accuracy of 92.03%, with balanced precision, recall, and an F1 score of 92% and minimal error rates. MLP with DWT achieved a slightly lower accuracy of 89.58% but still maintained strong performance, with both precision and recall at 90%, indicating robust capabilities and incorrect identification. Despite the higher error rates observed in MLP with DWT, the model still presented a low risk of misidentification. These results suggest that, while MLP with FLD offers slightly superior accuracy and lower error rates, MLP with DWT remains a viable option for security-sensitive systems, particularly in contexts where the specific features extracted by DWT prove advantageous.

Simple NN: The performance of simple NN was similar across the FLD and DWT features. With FLD, the simple NN achieved an accuracy of 89.13% and an F1 score of 89%, whereas with DWT, it attained an accuracy of 87.59% and an F1 score of 88%. The simple NN achieved 89% recall and precision with FLD, while 88% recall and precision were obtained with DWT. FAR and FRR, however, exhibited slight variations, with FLD showing lower values than DWT (FLD: FAR = 0.11074, FRR = 0.11090; DWT: FAR = 0.1211, FRR = 0.1244). As evidenced by their EER values, both configurations maintained relatively low risks of individual misidentification (FLD: EER = 0.1082; DWT: EER = 0.1228). In general, both the FLD and DWT configurations of the simple NN are suitable for authentication systems.

CNN: The performance of CNN across the FLD and DWT features was also quite similar. With FLD, CNN achieved an accuracy of 99.41% and an F1 score of 99%, while with DWT, it attained an accuracy of 99.38% and an F1 score of 99%. Both configurations achieved a recall and precision of 99%. In terms of error rates, both the FLD and DWT configurations exhibited minimal risks of individual misidentification, with FLD slightly outperforming DWT in terms of FAR and FRR values (FLD: FAR = 0.0058, FRR = 0.0059; DWT: FAR = 0.0061, FRR = 0.0062). Both configurations demonstrated an optimal balance between false acceptances and false rejections, as evidenced by their EER values (FLD: EER = 0.0059; DWT: EER = 0.0061). Overall, both the FLD and DWT configurations of CNN are considered highly suitable for authentication systems, as they provide exceptional performance and minimal error rates.

To summarize, models employing DWT and FLD feature extraction techniques performed differently across various biometric authentication models. It should be noted that models using the FLD feature extraction generally displayed competitive accuracy, with k-NN achieving the highest accuracy of 80.18%, closely followed by CNN with 78.25%. In contrast, the DWT feature extraction models demonstrated slightly lower accuracy, with CNN leading at 77.85%. Although the QDA models achieved consistent performance across both feature extraction methods, exhibiting accuracies of 75.53%, other models displayed notable variability. Furthermore, the FLD models generally displayed lower FARs, FRRs, and EERs than the DWT models. FLD demonstrated promising performance across multiple biometric authentication models, which underscores the importance of selecting appropriate feature extraction techniques tailored to specific biometric authentication tasks.

4.3. Experiment-2: System Usability and Channel Selection

BCI systems utilize many channels, up to 64 electrodes, to capture brain signals with sufficient spatial resolution. However, this approach presents challenges in terms of system complexity and setup time, as well as user discomfort, thereby affecting the overall user experience. As a result, Experiment-2 was designed to reduce the number of channels while simultaneously maintaining sufficient performance.

All 64 channels were utilized during the implementation while working with the public dataset in Experiment 1. However, to enhance usability, the number of channels used was reduced to 32 and then to 16 to improve the user experience while preserving robust authentication performance. We measured the effect of channel reduction to 16 and 32 using evaluation metrics. Two experimental phases were conducted, each utilizing a different subset of channels. In the first phase, 32 channels were used, while in the second phase, 16 channels were used. These channels were carefully selected based on their demonstrated significance and impact in prior research. The 32-channel approach was initially selected based on its use in another study [26], which explored the implications of halving the number of channels.

According to correlation analysis (Section 3.3), the 16-channel selection included FP1, FP2, and FPZ, all of which were found to be redundant in several studies [7,11,26]. Additionally, the positive impact of selecting these channels was observed in another study [7].

In the set of 32 channels, the following were included: AF3, AF4, AF7, C3, C4, CP1, CP2, CP5, CP6, CZ, F3, F4, F7, F8, FC1, FC2, FC5, FC6, FP1, FP2, FP1, FZ, O1, O2, OZ, P3, P4, P7, P8, PO3, PO4, T7, and T8. For the set of 16 channels, the following were selected: AF3, AF7, AFZ, C3, C5, FC1, FC3, FC5, F1, F3, F5, F7, FP1, FPZ, FT7, and FZ.

- 32-Channel Selection:

We conducted training sessions for identical models employing FLD and DWT feature extractions by utilizing the 32 selected channels. Table 5 provides a comprehensive summary of the results obtained from these training sessions.

The results demonstrated the performance of various evaluation models with different feature extraction techniques for biometric authentication. The CNN model with FLD achieved the highest accuracy and F1 score of 92.64% and 93%, respectively, indicating superior performance. However, considerable variability in performance across models highlights the importance of model selection. Specifically, models utilizing FLD generally exhibited lower FAR, FRR, and EER values than those using DWT for feature extraction.

Table 5. Performance comparison of machine learning and deep learning models with 32 channels.

Classifier	Feature Extraction	Accuracy	F1 Score	Recall	Precision	FAR	FRR	EER
SVM	DWT	36.93%	36%	37%	39%	0.6069	0.6301	0.6185
QDA		55.37%	55%	55%	56%	0.4436	0.4464	0.4450
K-NN		58.92%	59%	59%	64%	0.3623	0.4106	0.3865
XGBoost		42.22%	42%	42%	42%	0.5763	0.5774	0.5769
MLP		52.87%	52%	52%	53%	0.4730	0.4710	0.4720
Simple NN		49.56%	49%	50%	49%	0.5082	0.5041	0.5062
CNN		64.62%	64%	65%	64%	0.3566	0.3536	0.3551
SVM	FLD	76.26%	77%	76%	78%	0.2210	0.2375	0.2293
QDA		92.22%	92%	92%	92%	0.0773	0.0780	0.0776
K-NN		90.28%	90%	90%	91%	0.0862	0.0974	0.0918
XGBoost		73.12%	73%	73%	74%	0.2616	0.2686	0.2651
MLP		80.14%	80%	80%	80%	0.1974	0.1985	0.1979
Simple NN		74.40%	74%	74%	75%	0.2513	0.2560	0.2537
CNN		92.64%	93%	93%	93%	0.07393	0.0736	0.0737

- 16-Channel Selection:

We organized training sessions for identical models utilizing both FLD and DWT feature extraction techniques with the 16 selected channels. Table 6 offers a detailed overview of the results derived from these training sessions.

Table 6. Performance comparison of machine learning and deep learning models with 16 channels.

Classifier	Feature Extraction	Accuracy	F1 Score	Recall	Precision	FAR	FRR	EER
SVM	DWT	39.55%	39%	40%	42%	0.5790	0.6041	0.5916
QDA		75.53%	75%	75%	75%	0.2458	0.2452	0.2455
K-NN		66.86%	66%	67%	70%	0.1221	0.1625	0.1423
XGBoost		53.24%	53%	53%	53%	0.4685	0.4676	0.4681
MLP		69%	68%	69%	69%	0.3134	0.3104	0.3119
Simple NN		65.05%	64%	65%	65%	0.3527	0.3500	0.3514
CNN		77.85%	77%	78%	78%	0.2241	0.2217	0.2229
SVM	FLD	60.58%	61%	61%	63%	0.3727	0.3941	0.3834
QDA		75.53%	75%	75%	75%	0.2458	0.2452	0.2455
K-NN		80.18%	79%	80%	81%	0.1889	0.1981	0.1935
XGBoost		59.36%	59%	59%	60%	0.4034	0.4063	0.4049
MLP		70.36%	70%	70%	71%	0.2949	0.2969	0.2959
Simple NN		65.57%	65%	66%	65%	0.3484	0.3448	0.3466
CNN		78.25%	78%	78%	78%	0.2201	0.2177	0.2189

To summarize, this section addressed the issue of increasing usability by systematically reducing the number of channels from 64 to 32 and then to 16 to identify those most relevant for authentication. It was determined that with 32 channels, an accuracy of 92.64% could be achieved, while with 16 channels, an accuracy of 80.18% could be obtained. By reducing the number of channels, the authentication process was streamlined, and the key channels for authentication were highlighted, thereby allowing for the performance and usability of the system to be improved.

4.4. Comparison with Previous Studies

The EEGMMIDB dataset, established in 2000, has maintained a consistent presence throughout research endeavors across a wide range of areas, resulting in positive results. Recent applications of this dataset have extended to the field of authentication, with studies showcasing commendable results, as detailed in Table 7. EEG authentication framework

has been assessed using the dataset since 2018. For classification, we used machine learning models on EEG signals from motor imagery tasks performed by subjects and the rest state (REC and ROC) in the dataset. Using EEG data from the motor imagery tasks, the dataset demonstrated the robustness and accuracy of the proposed framework in distinguishing between genuine users and potential attackers. This dataset is thus essential for researchers interested in BCIS and EEG-based authentication, since it provides specific EEG signals linked to distinct mental tasks to develop and evaluate authentication frameworks based on brainwave signals. Table 7 summarizes the results from previous studies that used the same dataset.

Table 7. Results comparison with the previous study.

Ref	Feature Extraction	Classifier	Channel	Result
Thomas and Vinod, 2018 [11]	PSD	Based on correlation coefficients	19	EER = 0.0196
Kang et al., 2018 [5]	PSD	Mahalanobis distance-based classifier	56	Accuracy = 98.93% EER = 0.0073 FAR = 0.001 FRR = 0.0011
Suppiah and Vinod 2018 [14]	PSD	FLD	64	Accuracy = 98.9%
Ortega-Rodríguez et al., 2023 [7]	Power spectrum (PS), asymmetry index, and PLV	Wilcoxon signed rank	16 64	Accuracy = 97.67% Precision = 97.38% Recall = 97.18% Accuracy = 99.39% Precision = 99.27% Recall = 99.31
Waili et al., 2019 [13]	Wavelet decomposition, PSD	MLPNN	64	Accuracy = 98.31%
Kim and Kim 2019 [22]	Functional networks	-	64	Accuracy = 98%
Bidgoly et al., 2022 [23]	CNN	DNN	17	Accuracy = 98% EER = 0.0121
Cui et al., 2022 [24]	-	1DCNN-ALSTM	64	Accuracy = 99.97%
Panzino et al., 2022 [25]	CNN	Single threshold classification	64	Accuracy = 98.25%

Our machine learning models are competitive when compared to prior studies utilizing the same datasets. Notably, our QDA classifier attained an accuracy of 99.64%, exceeding previous benchmarks, wherein the highest accuracy achieved through traditional machine learning was 99.39% [7]. Compared to studies reporting accuracies ranging from 75% to 98%, our CNN model achieved an accuracy of 99.41% in the domain of DL. Furthermore, our results are very close to those of a study that achieved an accuracy of 99.97% with 1DCNN-ALSTM [26]. This illustrates the effectiveness and robustness of our deep learning approach in achieving near-optimal accuracy levels.

Although BCI-based authentication systems exhibit high reliability and accuracy, their practical adoption depends heavily on usability and user-friendliness. A critical factor in improving user experience is minimizing the number of signal acquisition channels or electrodes, thereby reducing complexity while maintaining reliable performance.

4.5. Application Interface and Acceptance Test

In this section, we present the BCI-based authentication application with the use of our own data to detect participants' identities during the REST state. We obtained approval from the Institutional Review Board (IRB) under reference number 24-1295 at the College of Medicine Research Center (CMRC) at King Saud University (KSU) to ensure compliance with ethical standards regarding human subjects. The data reported for this experiment were collected between the 5th and the 10th of May 2023 from 20 participants. Twenty female students from KSU participated in the experiment. Participants were asked if they

had any neurological or psychiatric disorders and if their visual and auditory acuities were normal. Furthermore, none of the participants had experience with EEG or BCI devices. All subjects were over the age of 18 and could make decisions on their own. There were 16 subjects between the ages of 18 and 25, three between the ages of 26 and 35, and one between the ages of 36 and 45.

As part of the experiment, the participants were instructed to focus on a specific point to avoid any eye movement or distractions. During the data acquisition process, participants were asked to maintain calmness, relax, and refrain from thinking about anything while placing their hands in a relaxed and comfortable position to prevent muscle movements, which could adversely affect the quality of the data. They were then instructed to abide by the following procedures during the experiment:

1. Sit comfortably, with hands placed in a relaxed manner.
2. Focus on a specific point to avoid eye movements or distractions.
3. Avoid thinking about any matters during the experiment.
4. Avoid moving hands, feet, or any voluntary muscles during the experiment.
5. Refrain from swallowing or any other movements that could affect the quality of the signals captured during the experiment.

We built a graphical user interface (GUI) that allowed users to record brain signals and use them seamlessly and efficiently for authentication processes during both the registration and authentication phases of the process. A Python script presents a graphical wizard interface using a Tkinter to streamline the BCI user authentication setup process. The wizard comprises multiple steps, guiding users through essential procedures, such as headset preparation and behavioral protocols, to ensure optimal data acquisition quality. Users can seamlessly navigate between steps using intuitive buttons, including “Next” and “Back.” The wizard also facilitates user registration and login functionalities, with simulated progress indicators that provide real-time feedback on the registration and login processes.

Overall, this wizard aims to enhance the user experience by simplifying the setup procedure and promoting efficient interaction with the BCI system for authentication purposes. Figure 5 shows the experimental environment with the Emotiv EPOC X EEG device to capture the participants’ brain signals. The Emotiv EPOC X samples EEG signals at a frequency of 128 Hz. This device features 14 channels corresponding to standard international 10–20 system locations, including AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, and AF4. Figure 6 illustrates a sample recording of a participant’s signal using emotivpro software (version 3.0).



Figure 5. Experiment lab environment (a) and Emotiv EPOC X EEG headset (b).

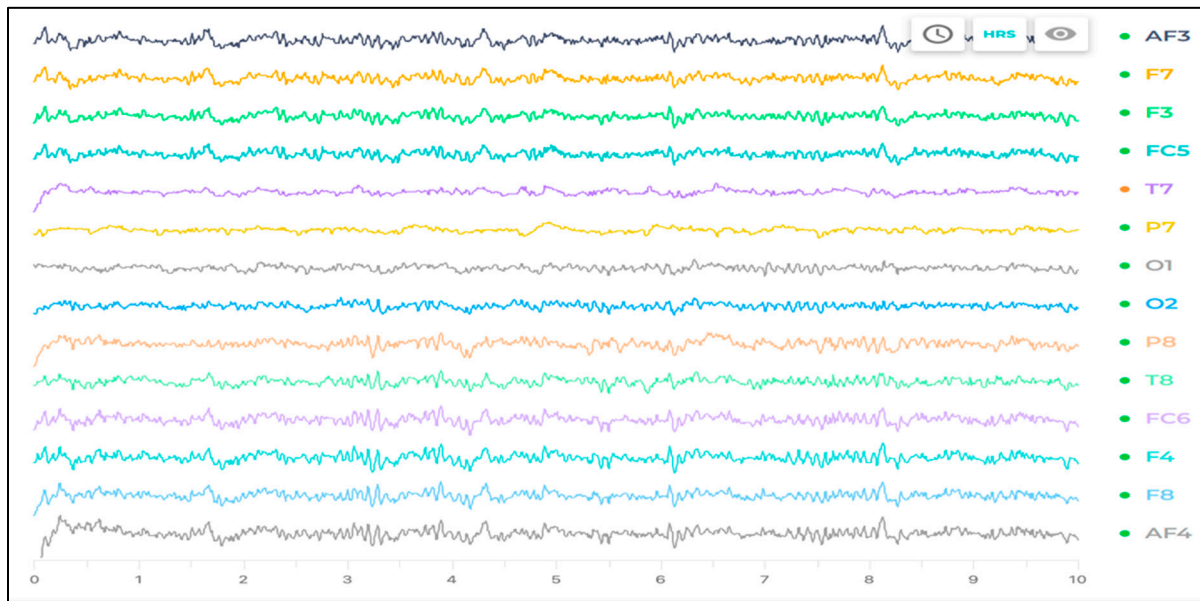


Figure 6. Sample of recorded signals in Emotiv pro software (version 3.0).

Our prototype application was designed based on [28], which investigated EEG acquisition during the rest state for both open and closed eyes. The recording process was divided into two stages. In the first stage, the participants underwent a one-minute session, which was utilized to train the model. In the second stage, recordings were made for a duration of 10 s to test the model's performance. A one-minute rest period was allocated between recordings for each participant to prevent the gel on the electrodes from drying out. This methodology aimed to ensure optimal conditions for data collection and minimize any potential sources of interference during the recording process.

The experiments were conducted in the university's laboratory infrastructure free of noise to ensure optimal conditions for its success. Participants were instructed to open their eyes intermittently during the experiment in a serene setting with the aim of inducing them into a state of rest. To minimize muscle tension, the participants were seated comfortably on chairs with their arms at their sides throughout the study. During the login process, EEG data acquisition took 10 s, as visually represented in the toolbar illustrated in Figure 7. Figure 8 showed the confirmation of granted access.

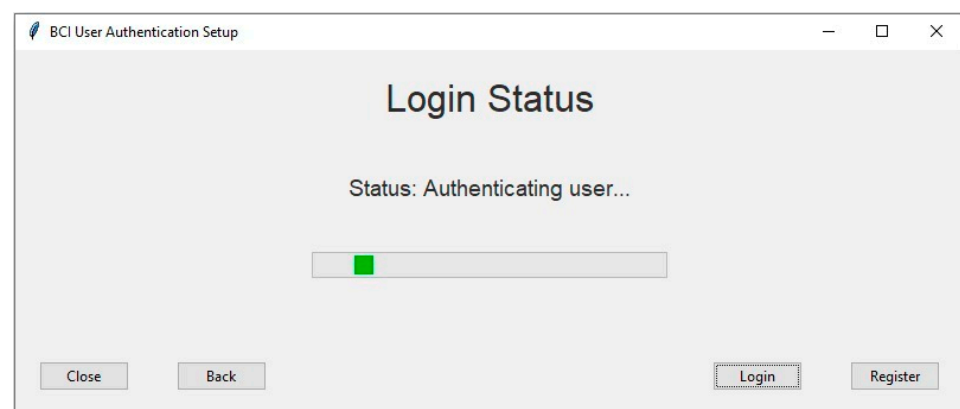


Figure 7. Authentication stage interface during recording of participant brainwave.

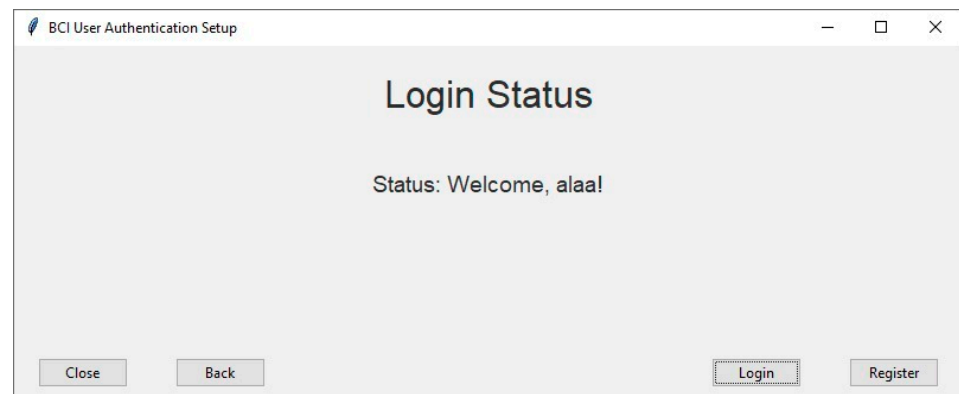


Figure 8. Authentication result interface: Alaa is the participant who granted access.

4.5.1. Application Performance Analyses

EEGMMIDB dataset demonstrated superior accuracy (illustrated in Experiment 1 and Experiment 2) during the CNN model, which led us to attempt to incorporate the CNN model into our own dataset. In the beginning, we used the data acquired from the participants for the one-minute period, separating it into training (80%) and validation (20%) data and following a methodology like that used with the EEGMMIDB dataset. A 99.75% accuracy rate was achieved, accompanied by 100% precision, recall, and F1 scores. A FAR of 0.0025, an FRR of 0.0026, and an EER of 0.0025 represent minimal values, respectively. It is evident from these results that the authentication system is highly accurate and reliable.

Another 10-second recording was taken following the launch of the application for the purpose of evaluating the prediction model. A 99.73% accuracy was achieved, accompanied by 100% precision, recall, and F1 scores. From this performance, it is evident that the model is reliable and effective in accurately predicting authentication systems within a short period of time.

We have conducted latency profiling on our system (Intel Xeon, 2 vCPUs, 13 GB RAM) using the EEGMMIDB dataset (109 users). Table 8 presents a detailed breakdown of offline processing times, FLD feature extraction, and real-time inference. The key metric for real-time application, per-sample classification latency, is low. In 32-channel model, the total processing latency per sample is under 30 s (29.18 s for CNN inference). This efficiency is consistent across configurations, with 16-channel and 64-channel inference times at 41.21 s and 11.77 s (for the NN classifier), respectively. While the initial feature extraction and model training phases are computationally intensive and performed offline, the optimized inference pipeline demonstrates that our system can operate as a real-time application.

Table 8. Offline processing times and real-time inference in EEGMMIDB dataset (109 Users).

Channel Count	Pre-Processing	Feature Extraction	Inference Latency
64-channel	65.10 s	18.30 s	11.77 (simple NN) 41.21 (CNN)
32-channel	75.20 s	9.49 s	29.18 (CNN)
16-channel	69.66 s	2.93 s	41.21 (CNN)

4.5.2. Acceptance Test

After the experiment was completed, the participants were directed to submit user acceptance survey submission. The results of this survey show that out of the twenty subjects, seven reported feeling rather stressed out during the last week. None of the participants reported feeling tired on the day of the experiment. Regarding usability of the rest state (open eyes), participants rated the task as somewhat boring, with four participants

rating it as 3, and three participants rating it as 4 on a scale from 1 (Strongly Agree) to 5 (Strongly Disagree). Regarding the attention requirement, one participant found it minimal (rating of 1), while the majority rated it as somewhat attention-demanding (ratings of 3 to 5). Most participants (11 out of 20) could imagine performing the task repeatedly for authentication purposes.

Regarding the usability of the device, after a brief description, most participants (10 out of 20) could imagine putting the headset on themselves without difficulty. Additionally, the majority (16 out of 20) had a very positive experience with the headset, finding it comfortable to wear for extended periods. All participants expressed no security concerns regarding the use of brainwave authentication.

When asked if they would be willing to use brainwave authentication as their primary authentication method, 11 out of 20 participants responded affirmatively, while 9 were unsure without providing specific reasons. Additionally, all participants did not foresee any potential problems with these techniques in an authentication system.

5. Conclusions

Our experimental evaluation of multiple machine learning models (SVM, k-NN, XGBoost, MLP, and NN) revealed that QDA and CNN delivered better performance when combined with FLD and DWT feature extraction. QDA achieved a notable accuracy of 99.64% with both methods, while CNN attained 99.38% (DWT) and 99.41% (FLD) accuracy. To optimize usability, we systematically reduced the EEG channels from 64 to 32 and finally 16, identifying the most discriminative channels for authentication. This channel reduction yielded accuracies of 92.64% (32 channels) and 80.18% (16 channels), demonstrating an effective balance between performance and practicality while highlighting the most critical channels for reliable authentication. This reduction in channel count streamlined the authentication process and highlighted the key channels crucial for authentication, thereby improving the system's performance and usability. Finally, we implemented a real-time application solution using our own collected dataset, achieving a 99.75% accuracy with CNN model.

Building on these findings, we recommend several promising research directions: investigating multimodal approaches that integrate EEG with complementary physiological or behavioral biomarkers and exploring advanced feature extraction methods and machine learning architectures to further enhance both security and usability. These extensions could lead to more robust and practical authentication systems.

Author Contributions: N.A. conceived and performed the experiment, analyzed and interpreted the data, and drafted the manuscript. M.A. designed, analyzed, validated, reviewed, and edited the manuscript. M.A. and A.A.-N. supervised, reviewed, and edited the manuscript and contributed to the discussion. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by a grant (No. CRPG-25-3009) under the Cybersecurity Research and Innovation Pioneers Initiative, provided by the National Cybersecurity Authority (NCA) in the Kingdom of Saudi Arabia.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of King Saud University (KSU), and approved by the Ethics Committee in the College of Medicine Research Center (CMRC) under reference number 24-1295 to ensure compliance with ethical standards regarding human subjects.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: EEG Motor Movement/Imagery Dataset (EEGMMIDB) used in this study is available at <https://physionet.org/content/eegmmidb/1.0.0/> (accessed on 1 Septem-

ber 2024). Thank you for your comment. The custom dataset used in the real-time application is available upon request.

Acknowledgments: This research is supported by a grant (No. CRPG-25-3009) under the Cybersecurity Research and Innovation Pioneers Initiative, provided by the National Cybersecurity Authority (NCA) in the Kingdom of Saudi Arabia.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nakamura, T.; Goverdovsky, V.; Mandic, D.P. In-Ear EEG Biometrics for Feasible and Readily Collectable Real-World Person Authentication. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 648–661. [\[CrossRef\]](#)
2. Yu, M.; Kaongoen, N.; Jo, S. P300-BCI-Based Authentication System. In Proceedings of the 2016 4th International Winter Conference on Brain-Computer Interface (BCI), Yongpyeong Resort, Republic of Korea, 22–24 February 2016; pp. 1–4.
3. Seha, S.N.A.; Hatzinakos, D. EEG-Based Human Recognition Using Steady-State AEPs and Subject-Unique Spatial Filters. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3901–3910. [\[CrossRef\]](#)
4. Zeynali, M.; Seyedarabi, H. EEG-Based Single-Channel Authentication Systems with Optimum Electrode Placement for Different Mental Activities. *Biomed. J.* **2019**, *42*, 261–267. [\[CrossRef\]](#)
5. Kang, J.-H.; Jo, Y.C.; Kim, S.-P. Electroencephalographic Feature Evaluation for Improving Personal Authentication Performance. *Neurocomputing* **2018**, *287*, 93–101. [\[CrossRef\]](#)
6. Wu, Q.; Yan, B.; Zeng, Y.; Zhang, C.; Tong, L. Anti-Deception: Reliable EEG-Based Biometrics with Real-Time Capability from the Neural Response of Face Rapid Serial Visual Presentation. *Biomed. Eng. Online* **2018**, *17*, 55. [\[CrossRef\]](#)
7. Ortega-Rodríguez, J.; Gómez-González, J.F.; Pereda, E. Selection of the Minimum Number of EEG Sensors to Guarantee Biometric Identification of Individuals. *Sensors* **2023**, *23*, 4239. [\[CrossRef\]](#)
8. Haukipuro, E.-S.; Kolehmainen, V.; Myllärinen, J.; Remander, S.; Salo, J.; Takko, T.; Nguyen, L.N.; Sigg, S.; Findling, R.D. Mobile Brainwaves: On the Interchangeability of Simple Authentication Tasks with Low-Cost, Single-Electrode EEG Devices. *IEICE Trans. Commun.* **2019**, *E102.B*, 760–767. [\[CrossRef\]](#)
9. Farik, M.; Lal, N.A.; Prasad, S. A Review Of Authentication Methods. *Artic. Int. J. Sci. Technol. Res.* **2016**, *5*, 246–249.
10. Zeng, Y.; Wu, Q.; Yang, K.; Tong, L.; Yan, B.; Shu, J.; Yao, D. EEG-Based Identity Authentication Framework Using Face Rapid Serial Visual Presentation with Optimized Channels. *Sensors* **2018**, *19*, 6. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Thomas, K.P.; Vinod, A.P. EEG-Based Biometric Authentication Using Gamma Band Power During Rest State. *Circuits Syst. Signal Process.* **2018**, *37*, 277–289. [\[CrossRef\]](#)
12. TajDini, M.; Sokolov, V.; Kuzminykh, I.; Ghita, B. Brainwave-Based Authentication Using Features Fusion. *Comput. Secur.* **2023**, *129*, 103198. [\[CrossRef\]](#)
13. Waili, T.; Johar, M.G.M.; Sidek, K.A.; Nor, N.S.H.M.; Yaacob, H.; Othman, M. EEG Based Biometric Identification Using Correlation and MLPNN Models. *Int. J. Online Biomed. Eng. IJOE* **2019**, *15*, 77. [\[CrossRef\]](#)
14. Suppiah, R.; Vinod, A.P. Biometric Identification Using Single Channel EEG during Relaxed Resting State. *IET Biom.* **2018**, *7*, 342–348. [\[CrossRef\]](#)
15. Rathi, N.; Singla, R.; Tiwari, S. Brain Signatures Perspective for High-Security Authentication. *Biomed. Eng.* **2020**, *32*, 2050025. [\[CrossRef\]](#)
16. Mu, Z.; Yin, J.; Hu, J. Application of a Brain-Computer Interface for Person Authentication Using EEG Responses to Photo Stimuli. *J. Integr. Neurosci.* **2018**, *17*, 113–124. [\[CrossRef\]](#)
17. Chen, Y.; Atnafu, A.D.; Schlattner, I.; Weldtsadik, W.T.; Roh, M.-C.; Kim, H.J.; Lee, S.-W.; Blankertz, B.; Fazli, S. A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2635–2647. [\[CrossRef\]](#)
18. Kaongoen, N.; Yu, M.; Jo, S. Two-Factor Authentication System Using P300 Response to a Sequence of Human Photographs. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 1178–1185. [\[CrossRef\]](#)
19. Gui, Q.; Jin, Z.; Xu, W. Exploring EEG-Based Biometrics for User Identification and Authentication. In Proceedings of the 2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), Philadelphia, PA, USA, 13 December 2014; pp. 1–6.
20. Merrill, N.; Curran, M.T.; Gandhi, S.; Chuang, J. One-Step, Three-Factor Passthrough Authentication with Custom-Fit, In-Ear EEG. *Front. Neurosci.* **2019**, *13*, 447553. [\[CrossRef\]](#) [\[PubMed\]](#)
21. Goldberger, A.L.; Amaral, L.A.N.; Glass, L.; Hausdorff, J.M.; Ivanov, P.C.; Mark, R.G.; Mietus, J.E.; Moody, G.B.; Peng, C.-K.; Stanley, H.E. PhysioBank, PhysioToolkit, and PhysioNet. *Circulation* **2000**, *101*, e215–e220. [\[CrossRef\]](#)
22. Kim, D.; Kim, K. Resting State EEG-Based Biometric System Using Concatenation of Quadrantal Functional Networks. *IEEE Access* **2019**, *7*, 65745–65756. [\[CrossRef\]](#)
23. Bidgoly, A.J.; Bidgoly, H.J.; Arezoumand, Z. Towards a Universal and Privacy Preserving EEG-Based Authentication System. *Sci. Rep.* **2022**, *12*, 2531. [\[CrossRef\]](#)

24. Cui, J.; Su, L.; Wei, R.; Li, G.; Hu, H.; Dang, X. EEG Authentication Based on Deep Learning of Triplet Loss. *Neural Netw. World* **2022**, *32*, 269–283. [[CrossRef](#)]
25. Panzino, A.; Orrù, G.; Marcialis, G.L.; Roli, F. EEG Personal Recognition Based on ‘Qualified Majority’ over Signal Patches. *IET Biom.* **2022**, *11*, 63–78. [[CrossRef](#)]
26. Aggarwal, S.; Chugh, N. Signal Processing Techniques for Motor Imagery Brain Computer Interface: A Review. *Array* **2019**, *1–2*, 100003. [[CrossRef](#)]
27. Nicolas-Alonso, L.F.; Gomez-Gil, J. Brain Computer Interfaces, a Review. *Sensors* **2012**, *12*, 1211–1279. [[CrossRef](#)] [[PubMed](#)]
28. Rimbert, S.; Al-Chwa, R.; Zaepffel, M.; Bougrain, L. Electroencephalographic Modulations during an Open- or Closed-Eyes Motor Task. *PeerJ* **2018**, *6*, e4492. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.