



Review Article

Review of Authentication Systems based on Electroencephalogram

Asmaa Basher Hamza¹ 

Informatics Institute for Postgraduate Studies
Iraqi Commission for Computer and
Informatics.
Baghdad, Iraq
Ms202220724@iips.edu.iq

Rajaa K. Hasoun² 

Department of Information System
Management
University of Information Technology and
Communications.
Baghdad, Iraq
dr.rajaa@uoitc.edu.iq

ARTICLE INFO

Article History

Received: 18/12/2023

Accepted: 29/1/2024

Published: 1/5/2024

This is an open-access
article under the CC BY
4.0 license:

<http://creativecommons.org/licenses/by/4.0/>



ABSTRACT

Traditional authentication methods, such as the use of passwords and fingerprints, are susceptible to the theft, loss, and forgery. However, an innovative and secure alternative exists in the form of electroencephalogram (EEG)-based authentication systems, which operate by measuring distinctive brainwave patterns. This review undertakes a comprehensive analysis of the current state of EEG-based authentication, delving into its advantages, challenges, and potential future directions. In doing so, we examine the underlying principles governing the acquisition and processing of EEG signals, explore the various techniques employed for extraction and classification, and evaluate the performance of existing systems. Moreover, we emphasize the significant advantages offered by EEG-based authentication, including its exceptional accuracy, capacity for liveness detection, and robust resistance to spoofing attempts. Nevertheless, we must also acknowledge the various obstacles that must be overcome to facilitate wider adoption of this authentication method, encompassing concerns relating to hardware affordability, user acceptance, and data privacy. Finally, we identify a series of promising research avenues that can potentially address these challenges and unlock the full potential of EEG-based authentication, thereby enabling secure and convenient access control across a wide range of domains.

Keywords: *Biometric Authentication; Electroencephalogram (EEG); Information System Security; User Authentication*

1. INTRODUCTION

In guaranteeing the preservation of confidentiality, privacy, authorization, authentication, non-repudiation, and integrity, security is an essential and indispensable aspect in the formulation of information systems. These constituents are deemed the primary factors that contribute to the establishment of a firm and impenetrable framework. Contemporary information systems require adherence to security and privacy regulations and standards stipulated by legal statutes, thereby heightening the significance of integrating security systems across all aspects of design and execution [1].

User authentication (UA) plays a crucial and indispensable role in upholding the security of information systems by ensuring that access to protected information is exclusively granted to authorized individuals. UA outlines the process employed to verify the identity of a user engaging with a particular service, ensuring that their claimed identity aligns with their actual identity. Conventional UA techniques verify a user's identity by using information about the user such as password secrets, possessions such as credit cards, or user characteristics such as biometrics [2].

Nevertheless, recent research shows that many existing authentication systems fall short in terms of effectively guiding and educating users on how to implement secure authentication practices. Consequently, this deficiency in these systems means that users are highly likely to resort to employing insecure and predictable authentication methods, thereby jeopardizing the overall integrity of the system and severely compromising its security [3].

According to recent research, current knowledge-based authentication schemes do not offer an acceptable balance between security and usability. This situation can irritate users, who may then adopt insecure authentication practices, such as writing passwords on sticky notes and leaving them visible on a desk at work or reusing passwords across multiple online services. In addition, user-owned pictorial schemes are less secure because of their intrinsically small key spaces and associated security entropies, whereas PIN-based schemes are only used in conjunction with other elements (such as device login), also because of their small key spaces [4].

Personal authentication through the use of biometric data is known as biometric authentication. Biometric authentication, which uses information such as fingerprints, irises, faces, voiceprints, and more, has been extensively studied and developed. The information used in biometric authentication is more difficult to steal than traditional passwords. Fingerprints and iris scans are useful in practical applications, being effective at authenticating identities. However, the authentication mechanism could be impersonated and copied. One of the causes is that the irises and fingerprints needed for identification are always being made public [5].

Every biometric modality has advantages and disadvantages, and spoofing is one of the biggest issues with these modalities. Reliability in identity verification is crucial, especially for establishments such as government agencies and commercial businesses that need to have high-security systems in place. The adoption of electroencephalogram (EEG) as a biometric modality in security systems has been driven by this necessity. The brain's electrical activity is measured by an EEG. It is commonly used in medicine to identify a range of neurological conditions, including epilepsy, sleep disorders, and brain tumors. It is also utilized in post-stroke rehabilitation, emotion recognition, and brain-computer interfaces (BCIs), where brain signals are used to control external activities. Brain signals are sensitive to an individual's mental state. Thus, it is nearly impossible to fabricate or steal EEG signals, which makes them an especially appealing modality for use in high-level security systems [6].

2. CONCEPT OF AUTHENTICATION SYSTEMS

The authentication process is one of the most crucial elements of any system. Authentication mechanisms, which are often regarded as the first and last line of protection, can typically stop a thief from gaining unauthorized access to users' data [7].

Verifying a user's identity is the process of authentication. Several authentication methods are used to identify users. The authentication procedure in a security system verifies the data that the user has supplied to the database, and the user is given access to the security system if the data match that in the database. Three different authentication methods are employed. The first stage of access control is validation, which uses three standard variables for verification: something you have, something you know, and something you are [8].

The solutions provided by authentication systems answer the following queries: (i) Who is the user? (ii) Does the user actually embody what they claim to be? Therefore, one of the most promising approaches for enhancing apps' security and trust is authentication [9].

3. EEG AND BRAINWAVE SIGNALS

The measurement of potentials that represent the electrical activity of the human brain is known as EEG, which is an easily accessible test that shows how the brain changes over time. Medical professionals and researchers utilize EEGs extensively to investigate brain activity and identify neurological conditions [10].

BCIs are an emerging field for EEGs. Through the use of modern technologies, BCIs may now communicate with one another. A BCI is a computer system that receives and processes brain signals, converts them into commands, and then relays those commands to an output device so that the intended action can be performed. The main goal of BCI research is to use mental activity analysis to develop a new communication channel that will enable direct message transmission from the brain. An electrode cap is applied to the user's head to measure the EEG signal. A user imagines a certain activity, such as moving limbs or creating words, to instruct the machine. The EEG signal patterns are impacted by these tasks. To operate a machine (such as a wheelchair) or a computer application (such as a cursor movement), computers must recognize and categorize these patterns into distinct tasks [11].

The EEG-captured patterns of brainwaves are sinusoidal in shape, with amplitudes typically ranging from 0.5 μ V to 100 μ V. These patterns are classified into five groups, as indicated in Table 1 [12].

TABLE I. CLASSIFICATION OF EEG-CAPTURED PATTERNS BY FREQUENCY

EEG patterns	Frequency
Alpha	8–13 Hz
Beta	Above 13 Hz
Theta	4–8 Hz
Delta	0.5–4 Hz
Gamma	30–100 Hz

4. CONCEPT OF USING EEG SIGNALS FOR AUTHENTICATION

Researchers pay special attention to the use of biometric signals such as EEG, electrocardiogram, and electromyogram as appropriate tools for biometric authentication. These signals have distinguished advantages over other biometrics, such as being more robust against spoof attacks [13].

Among the biometric signals, EEGs have gained increasing interest. EEG biometrics has unique advantages that make it prominent among other biometric factors [14]:

- Biometric factors such as fingerprints or iris may be forged or imitated. For instance, researchers show that an intruder can simply make a fake fingerprint by just having a picture of one's finger. However, unlike the other biometric factors, EEGs are not exposed to the intruder, which makes them uncapturable and thus hard to forge.
- EEGs are emotional state dependent, and stress or fear changes the normal brainwaves' patterns regardless of the activity. As a result, EEG biometrics cannot be invoked under force and coercion situations, while in the other authentication methods, even in the challenge-based response ones, an adversary may gain access to a system by force or by threatening the user.
- In the other biometrics, one may use a dead (and warm) body to authorize his/her access to the system. However, a dead brain does not produce EEG signals. Hence, EEG itself guarantees that the user is alive and authenticating on his own.

5. EEG AUTHENTICATION

EEG authentication is a biometric authentication method that uses EEG to verify a person's identity. EEG measures the electrical activity of the brain, which is unique to each individual and relatively stable over time. This makes it a potentially more secure and reliable authentication method than traditional methods such as fingerprints or passwords, which can be stolen or forged [15].

EEG authentication works as follows [16]:

TABLE II. ADVANTAGES AND CHALLENGES OF EEG AUTHENTICATION

Advantages of EEG authentication	Challenges of EEG authentication
More secure: Brainwaves are difficult to forge or imitate, making EEG authentication more secure than traditional methods.	Technical complexity: EEG technology is still under development, and it can be expensive and difficult to use.
More reliable: Brainwaves are relatively stable over time, even if a person's appearance changes.	Privacy concerns: Collecting and storing brain data raises privacy concerns.
Continuous authentication: EEG can be used for continuous authentication, which means that a person's identity can be verified even while they are using a system.	Susceptibility to noise: EEG signals can be easily affected by noise from the environment or from the person's own body.

The steps for authentication using brainwaves can be summarized as follows:

- A. Brainwaves are extracted as follows:
 1. EEG: This non-invasive method uses electrodes placed on the scalp to measure the tiny electrical currents generated by the brain's neurons [17].
 2. Magnetic encephalography: This more expensive and complex technique uses sensors to detect the subtle magnetic fields produced by brain activity [18].
- B. Preprocessing and feature extraction
 1. Data import and filtering: The raw EEG data, typically stored in EDF or BDF formats, are imported into specialized software such as EEGLAB, Brain Vision, or MNE-Python [18].
 2. Filtering: Unwanted frequency components such as line noise (50/60 Hz) and muscle movement artifacts are removed using digital filters (e.g., band pass filters) [20].
 3. Segmentation and epoching
 - Segmentation: The continuous EEG data are divided into shorter segments or epochs around specific events of interest (e.g., stimulus presentation, motor response) [21].
 - Baseline correction: Each epoch is baseline-corrected by subtracting the average activity from a pre-stimulus period, removing slow drifts and enhancing event-related potentials.
 4. Artifact detection and removal
 - Visual inspection: EEG data are visually inspected for various artifacts such as blinks, eye movements, muscle activity, and electrode pops [22].
 - Automatic artifact detection: Independent component analysis (ICA) helps identify and remove independent components arising from non-brain sources such as muscle activity or eye blinks [23].
 5. Reference selection
 - Common average reference: EEG signals are re-referenced to the average of all electrodes, reducing common noise sources such as line noise [24].
 - Average mastoid reference: EEG signals are re-referenced to the average of mastoid electrodes located behind the ears, minimizing electrical activity from the face and neck [25].
 6. Bad channel identification and interpolation [26]
 - Channel rejection: Electrodes with excessive noise or technical issues are marked as bad and potentially excluded from further analysis.
 - Channel interpolation: Missing data from rejected channels can be interpolated based on the activity of surrounding electrodes, minimizing data loss.
 7. Additional preprocessing steps
 - Spatial filtering: Techniques such as beamforming and ICA can enhance specific brain regions or sources of interest.
 - Normalization: Scaling or normalization of EEG amplitudes across channels or subjects can facilitate comparison and analysis across different datasets.
- C. USING brainwaves for authentication

Machine learning algorithms are trained on a dataset of brain print profiles and their corresponding identities. During authentication, a user's brainwaves are compared with their stored profile, and a match confirms their identity.

Machine learning and deep learning play a crucial role in extracting patterns and insights from EEG signals for UA. Here are some commonly used algorithms:

1. Traditional machine learning [27]
 - Support vector machines (SVM): These powerful classifiers are suitable for high-dimensional data such as EEG and excel at separating individuals based on extracted features.
 - K-nearest neighbors (KNN): This simple yet effective algorithm classifies an individual based on the majority class of their closest neighbors in the EEG feature space.
 - Random forests: Combining multiple decision trees, random forests offer robustness against overfitting and provide interpretable feature importance insights.
2. Deep learning algorithms [28]
 - Convolutional neural networks (CNNs): CNNs excel at extracting spatial features from EEG data, thus being particularly useful for analyzing evoked potentials associated with specific stimuli used in authentication tasks.
 - Recurrent neural networks (RNNs): Long short-term memory (LSTM) and gated recurrent units (GRUs) are adept at capturing temporal dynamics in EEG signals, crucial for tasks such as analyzing continuous authentication data or motor imagery patterns.
 - Autoencoders: These unsupervised learning models can learn compressed representations of EEG data, effectively reducing dimensionality and potentially uncovering hidden patterns related to individual identity.
3. Hybrid approaches
 - CNN-RNN hybrids: Combining CNNs and RNNs leverages spatial and temporal features simultaneously, achieving high accuracy in EEG authentication tasks.
 - Deep feature learning: Training deep neural networks to extract features from raw EEG data can outperform traditional feature engineering methods, leading to more robust and adaptable authentication systems.

The specific algorithms used depend on various factors, including:

1. Type of EEG data: Evoked potentials (e.g., P300) require different approaches than continuous EEG data.
2. Task objective: Person identification, liveness detection, or continuous authentication have different requirements.
3. Computational resources: Deep learning models require significant computational power.

6. PROBLEM STATEMENT

While traditional authentication methods such as passwords and tokens face growing concerns regarding security and convenience, EEG-based authentication presents a promising biometrics solution with inherent advantages such as user-friendliness, continuous verification, and potential resistance to forgery [29]. However, despite its intriguing potential, the field lacks a comprehensive review that consolidates the current state of the art; critically evaluates existing systems; and clarifies the specific strengths, limitations, and open challenges associated with EEG-based authentication. This gap in knowledge hinders the broader adoption and further development of this promising technology. This paper addresses this issue by providing a meticulous review of existing EEG-based authentication systems, their strengths and weaknesses, and key considerations for implementation in practical applications. Through this review, we aim to equip researchers, developers, and potential users with valuable insights to advance the field and unlock the full potential of EEG-based authentication in securing our increasingly digital world.

7. RESEARCH OBJECTIVE

The primary aim of this research is to conduct a comprehensive review of authentication systems leveraging EEG signals. The study seeks to critically examine the existing literature on EEG-based authentication, with a focus on understanding the technological advancements, methodologies, and algorithms employed in these systems. Furthermore, the research aims to identify the strengths and limitations of EEG-based authentication methods, exploring their effectiveness in ensuring robust and secure UA. Specific objectives include analyzing the accuracy, reliability, and user-friendliness of EEG-based authentication systems; investigating the impact of various EEG acquisition techniques; and assessing the potential vulnerabilities and challenges associated with this innovative approach. By addressing these objectives, this review intends to provide valuable insights into the current state of EEG-based authentication systems, offer recommendations for improvements, and contribute to the advancement of secure and user-friendly authentication technologies.

8. LITERATURE REVIEW

In recent years, the use of brainwaves signals for authentication has arisen as an attractive topic of study. This study of the literature seeks to offer an overview of research that discusses the use of EEG for authentication.

In 2017, LI, Youjun, et al. [30] discussed the construction of EEG multidimensional feature image sequences to represent emotion variation with EEG signals. They proposed a hybrid deep neural network combining CNN and LSTM RNNs for recognizing human emotional states. The study used the open-source dataset DEAP and achieved significant improvements in emotion classification accuracy. The study also covered EEG feature extraction methods, the construction of emotion classification labels, and the results of the experiment. The proposed method demonstrates higher accuracy compared with baseline methods and peer-reviewed studies. The study provides insights into the integration of spatial, frequency domain, and time characteristics of EEG signals for emotion recognition.

In 2018, BARKADEHI, Mohammadreza Hazhirpasand, et al. [31] introduced a literature review and classification study that provides a comprehensive analysis of different types of authentication systems, their usage, similarity, usability, performance, and drawbacks. It discussed the shortcomings of traditional text-based passwords and explored alternative methods such as non-dictionary words, mixed symbols, and password aging. The study also covered multi-factor authentication, narrative reviews, developmental reviews, cumulative reviews, and literature review types. It delved into smartphone-centered, touch-based, EEG-based, web-centered, and classification of research papers. It also examined the feasibility of various attacks, usability items, and the implementation and cost-effectiveness of authentication factors. The study concluded by emphasizing the complexity of authentication systems and the need to balance security, usability, and availability.

In 2018, ZENG, Ying, et al. [32] introduced a framework for EEG-based identity authentication using face rapid serial visual presentation combined with EEG signals. It discussed the event-related potential components induced by self-face and non-self-face, proposing an authentication method based on hierarchical discriminant component analysis (HDCA) and genetic algorithm (GA) to build subject-specific models with optimized fewer channels. The document also covered the materials and methods used in the experiment, including participants, stimuli, experimental procedure, and electrophysiological recording. The results show that the proposed framework is effective, robust, and stable over time, achieving an averaged authentication accuracy of 94.26% within 6 seconds and 88.88% over a 30-day interval.

In 2019, Wilaiprasitporn, Theerawit, et al. [33] developed a deep learning method for precise individual recognition by analyzing EEG signals. CNNs and RNNs are combined in this method. In particular, they assessed the GRU and LSTM varieties of RNNs. With a mean correct recognition rate of up to 99.90%–100%, the suggested technique successfully identified people based on their EEG signals during various affective states. The study showed that while CNN-GRU had a quicker training period, both CNN-GRU and CNN-LSTM models performed similarly in terms of accuracy.

In 2019, Hendrawan, Muhammad Afif, et al. [34] demonstrated a biometric system that uses single-channel EEG when the eyes are closed during rest. Nine subjects' EEG data were gathered and segmented into 5-second segments, with an emphasis on the alpha band that was recovered using the discrete wavelet transform. For feature extraction, the system used power spectral density; for classification, it used linear discriminant analysis (LDA) and SVM. According to the study, the third 5-second EEG data segment had the best accuracy, scoring 86% using LDA. This finding highlights single-channel EEG's potential for high-security authentication with respectable accuracy and lower computational costs, as well as its viability and efficiency in biometric systems.

In 2019, Yingnan, Frank, Benny et al. [35] discussed the use of EEG signals for user identification systems in healthcare and IoT. They proposed a novel approach based on 1D convolutional LSTM neural network (1D-convolutional LSTM) for EEG-based user identification. The proposed network achieved a high accuracy of 99.58%

using only 16 channels of EEG signals, outperforming existing methods. The document also explored the trade-offs among performance, cost, and efficiency in EEG-based identification systems.

In 2019, WANG, Min, et al. [36] discussed a novel model for ongoing EEG biometric identification using EEG collected during a diverse set of tasks. They proposed representing EEG signals as a graph based on within-frequency and cross-frequency functional connectivity estimates and the use of graph CNN (GCNN) to automatically capture deep intrinsic structural representations from the EEG graphs for person identification. The study assessed the robustness of the method against diverse human states, including resting states under eye-open and eye-closed conditions and active states drawn during the performance of four different tasks. The document also explored the use of EEG to provide real-time human workload and fatigue indicators in highly secure operations such as air traffic control and supervisory control or teleoperations of autonomous systems. It compared the proposed method with state-of-the-art EEG features, classifiers, and models of EEG biometrics.

In 2020, Patel and Mohammad [37] proposed an EEG-based person authentication system using EEG data to measure neurophysiological reactions to specific music. During an EEG reading, participants listen to self-selected and other-selected music. An algorithm is trained on EEG readings of the attacker and the user by analyzing changes in alpha and beta band frequencies across eight EEG sensors. For dimension reduction and data representation, the researchers recommended using UMAP or a similar technique. This methodology aims to overcome biometric limitations and provide reliable authentication.

In 2020, Amir Jalaly, Hamed Jalaly, Zeynab. et al. [38] introduced a document that discussed EEG-based authentication, including the recording of electrical activities of the brain, dominant frequency bands, electrode placement, and EEG acquisition protocols. It also covered datasets used for EEG records, BCI competition IV datasets, and a dataset containing brain signals of 60 different subjects while listening to different types of music. The document explored EEG acquisition protocols, visual stimuli, filtering methods, spatial domain filtering, feature extraction methods, and shallow and deep classification methods. It also addressed security and privacy challenges of EEG biometrics, open challenges, and the need for universal EEG-based authentication systems. The document concluded with an overview of authentication and identification methods using brain signals.

In 2021, Rahman, Arafat, et al. [39] introduced a cutting-edge biometric system that combines the dynamics of keystrokes and EEG, improving security by utilizing distinct biometric signatures and user activity patterns. The EEG and keyboard dynamics signals from 10 participants during various sessions make up the dataset. The EMOTIV Insight gadget was used to monitor keyboard dynamics as users typed a specific password and to record EEG signals from different brain regions. The results indicate the suggested system's great accuracy and anti-spoofing capacity. The random forest classifier achieved identification and authentication accuracy of more than 99%.

In 2022, Ellen C. Ketola, et al. [40] investigated the reduction of the number of EEG electrodes for authentication during motor motions to improve user comfort and lighten the strain on the data processing system. They used a 32-channel public EEG dataset from 12 subjects performing motor tasks unrelated to authentication. A random forest-based machine learning model was trained using 12 features after dividing the data into five frequency bands. They found that only 14 EEG channels are needed for authentication with a 1% accuracy loss compared with using all 32 channels. This condition allows for a customized headset for real-time authentication. The report highlights the effectiveness of the gamma sub-band for authentication and suggests further research with a larger user base. Overall, the study emphasizes the importance of frequency band selection and offers a viable method for EEG-based verification.

In 2022, STERGIADIS, Christos, et al. [41] discussed the development of a personalized UA system based on EEG signals. The current UA methods face low-security issues and are vulnerable to malicious attacks, creating a need for more reliable systems. The proposed method uses EEG signals to ensure continuous UA and addresses individual user variability. Machine learning techniques are employed to identify the optimal classification algorithm for each user. The study extracted 15 power spectral density features from three central electrodes of 15 subjects. The proposed approach can reliably grant or deny access to the user, with a mean accuracy of 95.6%. This personalized UA system can provide a viable option for real-time applications, ensuring high-level security and continuous UA.

In 2022, WU, Bingkun; MENG, Weizhi; CHIU, Wei-Yang, et al. [42] proposed an enhanced EEG authentication framework with motor imagery, integrating signal processing, channel selection, and deep learning classification. It explored the uniqueness, permanency, and collectability of EEG biometrics, and evaluated the framework's performance in insider and outsider attack scenarios, cross-session performance, and influence of channel selection. The framework outperforms state-of-the-art methods with a mean EER-19 of 0.74% and 1.27% for insider and outsider attacks, respectively.

In 2022, ASADZADEH, Shiva, et al. [43] discussed the sLORETA method and dynamic graph CNN (DGCNN) for emotion EEG classification. The proposed algorithm improved accuracy and used EEG signals. Spatial resolution, MRI, and lead field accuracy were also covered. Music and ICA algorithms were explored for emotional EEG distribution. The proposed method was compared with other methods and showed superior accuracy. Emotional EEG source recognition, sLORETA calculation, and evaluation on SEED and DEAP datasets were detailed. The algorithm focuses on emotion-processing brain areas and has potential for future improvements.

In 2022, ASADZADEH, Shiva, et al. [44] used the sLORETA method and DGCNN to classify emotional EEG, resulting in improved accuracy. EEG signals were used to detect human emotions. Challenges and methods for increasing spatial resolution were discussed, along with the use of MRI and lead field accuracy. Music was used to stimulate the brain, and ICA algorithms were used to calculate emotional EEG signal distribution. The proposed method outperforms existing approaches in emotion recognition. Emotional EEG source recognition, sLORETA algorithm calculation, and evaluation on SEED and DEAP datasets are detailed. The algorithm focuses on brain areas involved in emotion processing and has potential for future improvements.

In 2023, JESWANI, Jahanvi, et al. [45] presented research on using boring stimuli as a unique neuronal response for developing EEG-based biometrics. Different emotional stimuli were compared, and LVLA stimuli-based EEG signals were better for biometric applications than HVLA stimuli. The LVLA-based system achieved high accuracy, with skewness, Higuchi's fractal dimension, and sample entropy being standout features in both LVLA and HVLA stimuli. The study suggested further research on time-frequency domain features and performance comparison on different datasets. Authentication using audio-visual evoked EEG signals was successful, with LVLA stimuli being identified as a better candidate for biometric applications. Skewness is an important feature in both LVLA and HVLA stimuli. The results suggest that with more development, EEG-based biometric systems have the potential to revolutionize authentication methods. The proposed model achieved high accuracies of 80.97% and 99.41% for multi-class and binary classification respectively.

In 2023, TAJDINI, Mahyar, et al. [46] explored the feasibility of using brainwaves for user recognition and authentication. The data were collected using electrodes placed on the head to measure brainwaves, and features such as blinking, attention concentration, and picture recognition emotion sequences were used to generate different types of brainwaves. The collected data were then trained using the SVM algorithm, and a robust classifier was generated using adaptive boosting (AdaBoost). The proposed method achieved an authentication error rate of 0.52% and a classification rate of 99.06% when verifying legitimate users and intruders. The document highlighted the advantages of brainwave-based authentication over traditional methods and discussed the potential applications and developments in the field of BCIs.

In 2023, ALSUMARI, Walaa, et al. [47] discussed the development of a lightweight CNN model for EEG-based person recognition and authentication. The study addressed the limitations of existing EEG-based recognition methods and proposed a robust and efficient system using deep learning. The proposed CNN model consists of a small number of learnable parameters, enabling training and evaluation on a limited amount of available EEG data. The study presented detailed experiments, model architectures, and results, demonstrating the effectiveness of the proposed system for person recognition and authentication using EEG signals. The system achieved high recognition accuracy and authentication rates, making it suitable for high-level security applications. The system was validated on a public domain benchmark dataset and achieved a rank 1 identification result of 99% and an equal error rate of authentication performance of 0.187%. Table III shows a comparison between previous studies.

TABLE III. COMPARISON BETWEEN PREVIOUS STUDIES

Ref.	Method	Domain of Operation	Accuracy
[30]	CNN-LSTM-RNN (CLRNN)	Emotion recognition	75.21%
[32]	HDCA-GA	UA	94.26%
[33]	CNN-RNN	Individual identification	99.9%–100%
[34]	LDA-SVM	Biometric authentication	86%
[35]	1D-Convolutional-LSTM	User identification	99.58%
[39]	RF	Biometric authentication	99%
[40]	RF	Authentication systems	83.15%
[41]	-	UA	95.6%

[42]	Mixed-FBCNet-10	EEG-based authentication	74%
[43]	Linear SVM Non-linear SVM KNN	Emotional EEG pattern recognition	Nonlinear SVM (97.4%)
[44]	DGCNN	Emotional EEG pattern recognition	99.25%
[45]	LVLA	Biometric EEG-based authentication	99.41%
[46]	SVM-AdaBoost	EEG-based user identification	99.06%
[47]	CNN	EEG-based person identification and authentication	99%

We can note the following from Table 3:

1. Moderate accuracy
CNN-LSTM-RNN (CLRNN) achieves 75.21%, indicating potential for improvement.
2. High accuracy
 - HDCA-GA attains 94.26%, demonstrating effectiveness in EEG-based authentication.
 - CNN-RNN achieves 99.9%–100%, indicating a robust and reliable authentication system.
 - 1D-convolutional-LSTM demonstrates 99.58% accuracy, showcasing promise for secure authentication.
3. Reasonable accuracy
LDA-SVM shows 86% accuracy, providing a reasonable level of performance.
4. Random forest variability
One instance achieves 99% accuracy, while another achieves 83.15%, indicating variability within the random forest approach.
5. Challenges in mixed models
Mixed-FBCNet-10 exhibits 74% accuracy, suggesting potential challenges in combining different models.
6. Combined approaches' success
Linear SVM, nonlinear SVM, and KNN together achieve 97.4% accuracy, demonstrating the effectiveness of combined approaches.
7. Promising deep learning methods
DGCNN, LVLA, SVM-AdaBoost, and CNN show high accuracy (ranging from 99.06% to 99.41%), indicating promise in deep learning and ensemble methods for EEG-based authentication.

9. CONCLUSIONS

In this review, we provided a comprehensive overview of the current state and advancements in the field of EEG-based authentication systems from 2013–2023. This review highlighted the unique advantages of EEG signals in biometric authentication, such as high resistance to forgery and inherent liveness detection.

The analysis of various methodologies and technologies evidently shows that EEG-based systems offer a promising avenue for secure and user-specific authentication. The integration of advanced machine learning algorithms and improvements in EEG hardware technology has significantly enhanced the accuracy and feasibility of these systems.

This review underscores the potential of EEG-based authentication as a robust alternative to traditional methods, paving the way for more secure and personalized access control systems in the digital age.

In conclusion, EEG-based authentication systems are a promising alternative to traditional methods, offering increased security and user convenience. While challenges remain in terms of accuracy, scalability, and cost, ongoing research and development efforts are rapidly addressing these limitations. As technology advances and consumer acceptance grows, EEG-based authentication has the potential to revolutionize our approach to security in a wide range of applications, from mobile banking to border control. Further research is crucial to optimize electrode placement, refine signal processing algorithms, and address privacy concerns. However, the inherent uniqueness and non-repudiable nature of brainwave patterns suggest that EEG-based authentication is poised to become a cornerstone of future security infrastructures.

References



- [1] A. Almeahmadi and K. El-Khatib, "The state of the art in electroencephalogram and access control," in Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT), Jun. 2013, pp. 49–54, doi: 10.1109/iccitechnology.2013.6579521.
- [2] Alzhab, N. Abo. Design and implementation of techniques for the secure authentication of users based on electroencephalogram (EEG) signals. Diss. Master's thesis, Marche Polytechnic University, 2021.
- [3] Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. *International journal of scientific & technology research*, 5(11), 246-249.
- [4] A. Constantinides, M. Belk, C. Fidas, R. Beumers, D. Vidal, W. Huang, J. Bowles, T. Webber, A. Silvina, and A. Pitsillides, "Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three healthcare organizations," *ACM Trans. Comput. Healthcare*, vol. 4, no. 1, pp. 1–40, Jan. 2023, doi: 10.1145/3564610.
- [5] TajDini, Mahyar, et al. "Brainwave-based authentication using features fusion." *Computers & Security* 129 (2023): 103198.
- [6] Alsumari, Walaa, et al. "EEG-Based Person Identification and Authentication Using Deep Convolutional Neural Network." *Axioms* 12.1 (2023): 74.
- [7] Barkadehi, Mohammadreza Hazhirpasand, et al. "Authentication systems: A literature review and classification." *Telematics and Informatics* 35.5 (2018): 1491-1511.
- [8] Lal, Nilesh A., Salendra Prasad, and Mohammed Farik. "A review of authentication methods." *International journal of scientific & technology research* 5.11 (2016): 246-249.
- [9] Idrus, Syed Zulkarnain Syed, et al. "A review on authentication methods." *Australian Journal of Basic and Applied Sciences* 7.5 (2013): 95-107.
- [10] Siuly, Siuly, Yan Li, and Yanchun Zhang. "EEG signal analysis and classification." *IEEE Trans Neural Syst Rehabil Eng* 11 (2016): 141-144.
- [11] Siuly, Siuly, and Yan Li. "Discriminating the brain activities for brain–computer interface applications through the optimal allocation-based approach." *Neural Computing and Applications* 26 (2015): 799-811.
- [12] Zainuddin, Balkis Solehah, Zakaria Hussain, and Iza Sazanita Isa. "Alpha and beta EEG brainwave signal classification technique: A conceptual study." 2014 IEEE 10th International Colloquium on Signal Processing and its Applications. IEEE, 2014.
- [13] Abo-Zahhad, Mohammed, Sabah M. Ahmed, and Sherif N. Abbas. "A new multi-level approach to EEG based human authentication using eye blinking." *Pattern Recognition Letters* 82 (2016): 216-225.
- [14] Bidgoly, Amir Jalaly, Hamed Jalaly Bidgoly, and Zeynab Arezoumand. "A survey on methods and challenges in EEG based authentication." *Computers & Security* 93 (2020): 101788.
- [15] Puengdang, S., Tuarob, S., Sattabongkot, T., & Sakboonyarat, B. (2019, January). EEG-based person authentication method using deep learning with visual stimulation. In 2019 11th International Conference on Knowledge and Smart Technology (KST) (pp. 6-10). IEEE.
- [16] Bidgoly, A. J., Bidgoly, H. J., & Arezoumand, Z. (2020). A survey on methods and challenges in EEG based authentication. *Computers & Security*, 93, 101788.
- [17] Biasucci, A., Franceschiello, B., & Murray, M. M. (2019). Electroencephalography. *Current Biology*, 29(3), R80-R85.
- [18] Wheless, J. W., Castillo, E., Maggio, V., Kim, H. L., Breier, J. I., Simos, P. G., & Papanicolaou, A. C. (2004). Magnetoencephalography (MEG) and magnetic source imaging (MSI). *The neurologist*, 10(3), 138-153.
- [19] Serhani, M. A., El Menshawy, M., Benharref, A., Harous, S., & Navaz, A. N. (2017). New algorithms for processing time-series big EEG data within mobile health monitoring systems. *Computer methods and programs in biomedicine*, 149, 79-94.
- [20] Burgess, R. C. (2019). Filtering of neurophysiologic signals. *Handbook of clinical neurology*, 160, 51-65.
- [21] Michel, C. M., & Koenig, T. (2018). EEG microstates as a tool for studying the temporal dynamics of whole-brain neuronal networks: a review. *Neuroimage*, 180, 577-593.



- [22] Kaya, I. (2019). A brief summary of EEG artifact handling. *Brain-computer interface*, (9).
- [23] Islam, M. K., Rastegarnia, A., & Yang, Z. (2016). Methods for artifact detection and removal from scalp EEG: A review. *Neurophysiologie Clinique/Clinical Neurophysiology*, 46(4-5), 287-305.
- [24] Ludwig, K. A., Miriani, R. M., Langhals, N. B., Joseph, M. D., Anderson, D. J., & Kipke, D. R. (2009). Using a common average reference to improve cortical neuron recordings from microelectrode arrays. *Journal of neurophysiology*, 101(3), 1679-1689.
- [25] Yang, P., Fan, C., Wang, M., & Li, L. (2017). A comparative study of average, linked mastoid, and REST references for ERP components acquired during fMRI. *Frontiers in neuroscience*, 11, 247.
- [26] Björnell, J., Sternad, M., Phan-Huy, D. T., & Grieger, M. (2023). Channel Interpolation of Fading Channels and the Pilot Density Required for Predictor Antennas. *IEEE Transactions on Vehicular Technology*.
- [27] Wang, P., Fan, E., & Wang, P. (2021). Comparative analysis of image classification algorithms based on traditional machine learning and deep learning. *Pattern Recognition Letters*, 141, 61-67.
- [28] Shrestha, A., & Mahmood, A. (2019). Review of deep learning algorithms and architectures. *IEEE access*, 7, 53040-53065.
- [29] Bidgoly, Amir Jalaly, Hamed Jalaly Bidgoly, and Zeynab Arezoumand. "Towards a universal and privacy preserving EEG-based authentication system." *Scientific Reports* 12.1 (2022): 2531.
- [30] Li, Y., Huang, J., Zhou, H., & Zhong, N. (2017). Human emotion recognition with electroencephalographic multidimensional features by hybrid deep neural networks. *Applied Sciences*, 7(10), 1060.
- [31] Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, 35(5), 1491-1511.
- [32] Zeng, Y., Wu, Q., Yang, K., Tong, L., Yan, B., Shu, J., & Yao, D. (2018). EEG-based identity authentication framework using face rapid serial visual presentation with optimized channels. *Sensors*, 19(1), 6.
- [33] Wilaiprasitporn, Theerawat, et al. "Affective EEG-based person identification using the deep learning approach." *IEEE Transactions on Cognitive and Developmental Systems* 12.3 (2019): 486-496.
- [34] Hendrawan, Muhammad Afif, Pramana Yoga Saputra, and Cahya Rahmad. "Identification of optimum segment in single channel EEG biometric system." *Indonesian Journal of Electrical Engineering and Computer Science* 23.3 (2019): 1847-1854.
- [35] Sun, Y., Lo, F. P. W., & Lo, B. (2019). EEG-based user identification system using 1D-convolutional long short-term memory neural networks. *Expert Systems with Applications*, 125, 259-267.
- [36] Wang, M., El-Fiqi, H., Hu, J., & Abbass, H. A. (2019). Convolutional neural networks using dynamic functional connectivity for EEG-based person identification in diverse human states. *IEEE Transactions on Information Forensics and Security*, 14(12), 3259-3272.
- [37] Patel, Meetkumar J., and Mohammad I. Husain. "An approach to developing EEG-based person authentication system." *2020 IEEE International Conference on Big Data (Big Data)*. IEEE, 2020.
- [38] Bidgoly, A. J., Bidgoly, H. J., & Arezoumand, Z. (2020). A survey on methods and challenges in EEG based authentication. *Computers & Security*, 93, 101788.
- [39] Rahman, Arafat, et al. "Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms." *IEEE Access* 9 (2021): 94625-94643.
- [40] Ketola, Ellen C., et al. "Channel Reduction for an EEG-Based Authentication System While Performing Motor Movements." *Sensors* 22.23 (2022): 9156.
- [41] Stergiadis, C., Kostaridou, V. D., Veloudis, S., Kazis, D., & Klados, M. A. (2022). A Personalized User Authentication System Based on EEG Signals. *Sensors*, 22(18), 6929.
- [42] Wu, B., Meng, W., & Chiu, W. Y. (2022, December). Towards enhanced EEG-based authentication with motor imagery brain-computer interface. In *Proceedings of the 38th Annual Computer Security Applications Conference* (pp. 799-812).
- [43] Ray-Dowling, A. (2022). Examining Uniqueness and Permanence of the WAY EEG GAL dataset toward User Authentication. *arXiv preprint arXiv:2209.04802*.



- [44] Asadzadeh, S., Yousefi Rezaii, T., Beheshti, S., & Meshgini, S. (2022). Accurate emotion recognition using Bayesian model based EEG sources as dynamic graph convolutional neural network nodes. *Scientific Reports*, 12(1), 10282.
- [45] Jeswani, J., Govarthan, P. K., Selvaraj, A., Prince, A., Thomas, J., Kalathe, M., ... & JF, A. R. (2023). Low Valence Low Arousal Stimuli: An Effective Candidate for EEG-Based Biometrics Authentication System. *Studies in Health Technology and Informatics*, 302, 257-261.
- [46] TajDini, M., Sokolov, V., Kuzminykh, I., & Ghita, B. (2023). Brainwave-based authentication using features fusion. *Computers & Security*, 129, 103198.
- [47] Alsumari, W., Hussain, M., Alshehri, L., & Aboalsamh, H. A. (2023). EEG-Based Person Identification and Authentication Using Deep Convolutional Neural Network. *Axioms*, 12(1), 74.