Brain Organoid and Systems Neuroscience Journal 2 (2024) 17–22

Contents lists available at ScienceDirect

Brain Organoid and Systems Neuroscience Journal

journal homepage: www.sciencedirect.com/journal/bosn

Research Articles

Personalized user authentication system using wireless EEG headset and machine learning

Tron Baraku[a], Christos Stergiadis[b], Simos Veloudis[a], Manousos A. Klados[c,d,*]

[a] Department of Computer Science, City College, University of York Europe Campus, 24 Proxenou Koromila Street, Thessaloniki 546 22, Greece
[b] Department of Electronic Engineering, University of York, York YO10 5DD, UK
[c] Department of Psychology, City College, University of York Europe Campus, 24 Proxenou Koromila Street, Thessaloniki 546 22, Greece
[d] Neuroscience Research Center (NEUREC), City College, University of York Europe Campus, Thessaloniki 546 22, Greece

ARTICLE INFO

Keywords:
Biometrics
EEG
Security
User authentication
Machine learning

ABSTRACT

In the realm of authentication, biometric verification has gained widespread adoption, especially within high-security user authentication systems. Although convenient, existing biometric systems are susceptible to a number of security vulnerabilities, including spoofing tools such as gummy fingers for fingerprint systems and voice coders for voice recognition systems. In this regard, brainwave-based authentication has emerged as a novel form of biometric scheme that has the potential to overcome the security limitations of existing systems while facilitating additional capabilities, such as continuous user authentication. In this study, we focus on a data-driven approach to Electroencephalography (EEG)-based authentication, guided by the power of machine learning algorithms. Our methodology addresses the fundamental challenge of distinguishing real users from intruders by training classification algorithms to the unique EEG signatures of every individual. The system is characterized by its convenience, ensuring real-time applicability without compromising its efficiency. By employing a commercially available single-channel EEG sensor and extracting a set of 8 power spectral features (delta [0–4 Hz], theta [4–8 Hz], low alpha [8–10 Hz], high alpha [10–12 Hz], low beta [12–20 Hz], high beta [20–30 Hz], low gamma [30–60 Hz], high gamma [60–100 Hz]), a commendable mean accuracy of 85.4% was achieved.

1. Introduction

Security and privacy have become sought-after necessities in today's digital landscape. Reliance on digital platforms for communication, financial transactions, and access to resources has amplified the need and demand for robust user authentication systems. Traditional means of authentication, such as passwords or PINs, are vulnerable to data leaks and can be compromised with brute-forcing techniques or social engineering attacks (Herley et al., 2009). In addition, they burden the user with the task of credential management. On the other hand, prominent biometric systems are susceptible to spoofing tools such as the gummy fingers for fingerprint systems (Matsumoto et al., 2002), or voice coders for voice recognition systems (Wenger et al., 2021). Once biometric data are compromised, they remain permanently compromised as the biometrics of an individual cannot be forced to change, leaving users vulnerable. Furthermore, legitimate users are exposed to potential violent attacks, posing a significant threat to their safety and well-being.

In the field of biometrics, EEG-based authentication systems have emerged as a promising tool for granting access to the user and effectively rejecting intruders. They have the potential to eliminate security and convenience limitations associated with the aforementioned biometric authentication schemes. More specifically, this form of authentication utilizes the highly individualistic nature of EEG, which is characterized by low intra-subject variability and high inter-subject variability (Yu et al., 2019), making it significantly resistant to intruder attacks and identity theft. Attempting to coerce a user to authenticate is futile, as stress and pressure heavily affect an individual's EEG signals (Abo-Zahhad et al., 2016), making it impossible to generate the key-signal pattern that grants entry to the system. Moreover, EEG signals are hard to replicate and can only be generated while the subject is alive, thus ensuring the well-being of the user. In addition to enhancing security, EEG-based authentication can also enable continuous user verification through wearable devices, ensuring that the system remains accessible only to the legitimate user (Nakanishi et al., 2009).

* Corresponding author at: Department of Psychology, City College, University of York Europe Campus, 24 Proxenou Koromila Street, Thessaloniki 546 22, Greece.
E-mail addresses: tbaraku@citycollege.sheffield.eu (T. Baraku), cs2486@york.ac.uk (C. Stergiadis), sveloudis@york.citycollege.eu (S. Veloudis), mklados@york.citycollege.eu (M.A. Klados).

https://doi.org/10.1016/j.bosn.2024.03.003
Received 22 December 2023; Received in revised form 24 March 2024; Accepted 24 March 2024
Available online 1 April 2024

Over the past decade, there has been a substantial body of research dedicated to the exploration and refinement of techniques that utilize EEG characteristics in user authentication systems. Numerous approaches have been proposed regarding the selection of the EEG features and the classification techniques used, with the overarching aim of enhancing efficiency and at the same time promoting usability. Popular methods for selecting EEG features include the usage of Autoregressive (AR) models (Hine et al., 2017; Paranjape et al., 2001; Brigham and Kumar, 2010; Cai et al., 2015), Power Spectral Density (PSD) (Cai et al., 2015; Ong et al., 2018), and the Wavelet Transform (WT) (Cai et al., 2015; Liew et al., 2015). For example, Hine et al. (2017) used AR coefficients on resting stage EEG to reach a classification accuracy of up to 95% when testing with 50 subjects. On the other hand, Ong et al. (2018) achieved an accuracy of 89.21% after using PSD features from 10 participants, while Liew et al. (2015) used wavelets to reach a mean accuracy of 95% in a similar-sized cohort. It is worth mentioning that multiple features can also be combined to provide better authentication performances, as in the case of Valsaraj et al. (2020) where an accuracy of 98.28% was achieved by combining AR with PSD features.

In terms of classifiers, prominent approaches include the usage of machine learning algorithms such as the K-Nearest Neighbor (KNN) (Cai et al., 2015; Ong et al., 2018; Valsaraj et al., 2020), Random Forests (RF) (Chowdhury and Imtiaz, 2023; Rahman et al., 2021), Linear Discriminant Analysis (LDA) (Valsaraj et al., 2020; Seha and Hatzinakos, 2020), and Support Vector Machine (SVM) (Brigham and Kumar, 2010; Keshishzadeh et al., 2016). Keshishzadeh et al. (2016) extracted AR features from the resting state (eyes closed) EEG of 104 individuals and achieved an accuracy of 97.43% using an SVM classification model. On the other hand, Seha and Hatzinakos (2020) used LDA classification to achieve an accuracy of 96.46% when classifying features collected from 40 subjects that were exposed to auditory tasks. Apart from classifiers that use shallow classification, developments in deep learning have also had an impact on EEG-based authentication modeling. Studies using Convolutional Neural Networks (CNN) have achieved impressive results. For instance, Das et al. (2018) combined motor imagery tasks with CNN models, achieving up to 99.3% accuracy in identifying users. However, it should be stated that these models typically require larger amounts of data and are considered to be computationally more expensive than shallow classification methods.

Another factor that has a substantial effect on the performance of the system is the protocol used for acquiring the EEG signals. The most commonly used procedures are generally classified into three groups: resting state EEG (Hine et al., 2017), EEG during mental tasks (Brigham and Kumar, 2010), and EEG during tasks with an external stimulus (Seha and Hatzinakos, 2020). Recording EEG signals in a resting state condition is the simplest form of acquisition, as no additional equipment or instructions are required (Jalaly Bidgoly et al., 2020). Typically, individuals are asked to sit and relax in a quiet environment for the duration of the recording procedure. In comparison, procedures that use external stimuli rely on the individual's reaction to a visual or acoustic stimulus. This method measures the electrical potential generated by the brain in response to stimulation, such as viewing a sequence of pictures or listening to a piece of music (Jalaly Bidgoly et al., 2020). Lastly, in mental tasks, the individual is asked to perform a mental activity, such as imagining a particular body movement (Altahat et al., 2015).

In a recent study, Stergiadis et al. (2022) proposed a user-specific technique that caters to the unique characteristics of each patient's EEG dataset. In this study, machine learning algorithms were used to classify a set of 15 power spectral features (delta, theta, lower alpha, higher alpha, and alpha) extracted from three EEG channels, resulting in a mean accuracy of 95.6%. However, the authors reported practical challenges related to the data acquisition process, as a specialized medical device (EGI GES 300 system) was used to collect the EEG data, which greatly limited the system's usability. In response to this challenge, the present study explores the feasibility of utilizing a mobile consumer-grade EEG headset to build a practical EEG-based authentication system. By introducing a simplified recording procedure and leveraging the mobility offered by a wireless EEG headset, this study aims to streamline the authentication process and enhance user convenience while at the same time maintaining high-level performance.

The remainder of the paper is organized as follows. Section 2 describes the EEG system, the participants, and the overarching methodology followed to conduct the study. Section 3 presents the results obtained from training and testing the proposed system. Finally, in Section 4, we engage in a discussion of our findings within the context of the existing literature, concluding with an assessment of our work's limitations and future directions.

2. Materials and methods

2.1. Participants

Twenty-five healthy adult individuals participated in the study (17 males and 8 females). The exclusion criteria for participation focused on factors such as a history of neurological and psychiatric disorders, substance abuse, medication use, and other elements that might impact the neurophysiology of the brain. All participants had normal or corrected to normal vision and were instructed to abstain from consuming alcohol or caffeine on the day prior to their participation.

2.2. EEG data acquisition

All EEG data in the present study were recorded using the Mindwave Mobile 2 system (NeuroSky, San Jose, California USA). A singular dry electrode was placed on the frontal lobe (FP1 point) and recorded with a sampling rate of 1 Hz. All data was recorded during the resting state, where the participants were asked to relax and focus on the center of the screen with their eyes open. The study consisted of two phases. In the first phase, EEG signals from 10 of the participants were recorded. Data collected from these participants was used to create a repository that served as the training data for the ML classifiers. In the second phase, the remaining 15 participants were asked to complete both the registration and the authentication process, which together required a total of 7 minutes per participant. Within this time frame, the majority of it (6 min) was allocated to the registration process, which involved collecting EEG data for 3 minutes and dedicating an additional 3 minutes to the Auto-WEKA tool for selecting and training the optimal classifier for the user. Finally, the user-specific classifier that was trained during the registration phase was used to classify the EEG data provided during the authentication phase.

2.3. Preprocessing and feature extraction

Filtered data and band-specific brain wave components were automatically acquired through NeuroSky's embedded algorithms. The device produced eight values per second representing the delta [0–4 Hz], theta [4–8 Hz], low alpha [8–10 Hz], high alpha [10–12 Hz], low beta [12–20 Hz], high beta [20–30 Hz], low gamma [30–60 Hz], high gamma [60–100 Hz] frequencies. The data were divided into segments of 6 seconds. To increase the number of data points, an overlap of 3 seconds was introduced in each segment. Each of the resulting segments contained eight values, representing the mean values taken from the 6-second intervals across the eight frequency bands.

2.4. Classification procedure

Classification was performed on an individual basis where, for each user, two separate datasets were formed. The first dataset was created during registration, where EEG data was collected from the user for three minutes. These data were processed according to the procedure explained in Section 2.3, resulting in 59 instances, and then combined with 60 randomly selected instances from the repository of data collected from the initial 10 participants during the first phase. This was done so that a classifier could be trained to distinguish the instances

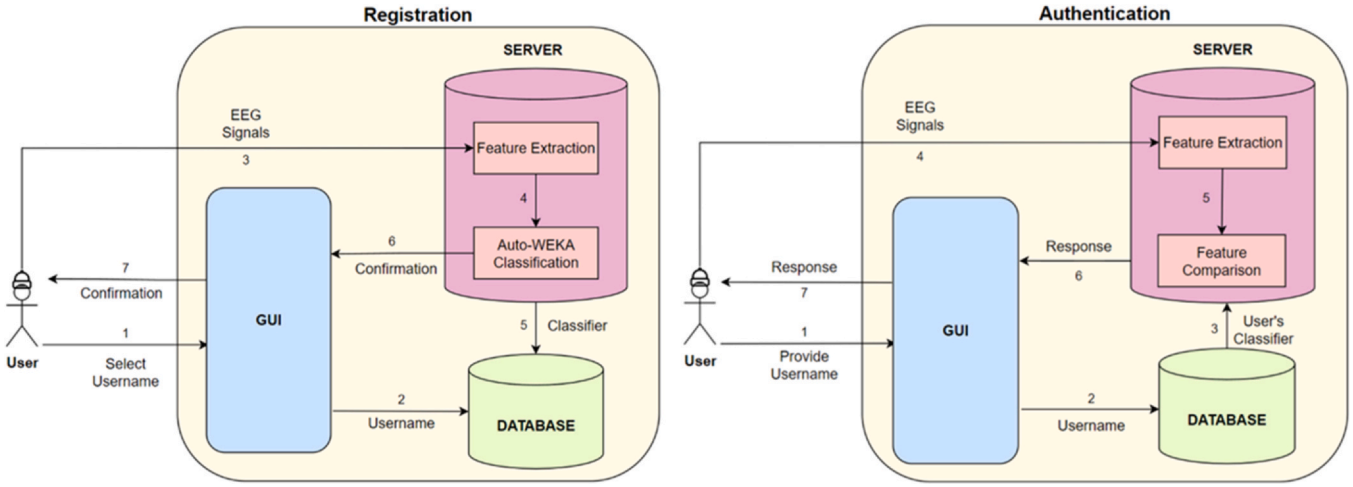

Fig. 1. System illustration of the registration and authentication processes. During registration, the user selects a username and wears the EEG headset to provide the EEG signals. The server determines and trains the optimal user-specific classifier, which is ultimately stored in a database. During authentication, the user provides the selected username and wears the EEG headset to provide the EEG signals. The server retrieves the user's classifier and classifies the EEG features to determine whether the user is granted or denied access.

belonging to the user from non-user (imposter) instances. The resulting data set was fed to Auto-WEKA (Thornton et al., 2013), an automated machine learning tool, to perform the selection of the optimal classification algorithm and hyperparameters for the training of the classifier. Throughout this process, Auto-WEKA utilizes 10-fold cross-validation to assess the performance of various models. To streamline the registration process, the time limit for Auto-WEKA was set to 3 minutes.

The second dataset was created during the authentication phase, where EEG data was collected from the user for one minute. The resulting 19 user instances were combined with 20 randomly chosen data instances belonging to other individuals. The accuracy of the system was assessed by evaluating the classifier's performance in distinguishing user-specific instances from others. Ideally, the system should grant access to the 19 user instances while effectively denying all the remaining instances.

2.5. Evaluation

The proposed methodology has been assessed using three conventional metrics commonly employed in the domain of biometrics: the False Acceptance Rate (FAR), the False Rejection Rate (FRR), and the Area Under the Receiver Operating Characteristic curve (AUC). The False Acceptance Rate (FAR) represents the percentage of genuine attempts incorrectly identified as impostors, while the False Rejection Rate (FRR) signifies the percentage of legitimate attempts erroneously rejected. The ROC curve plots the True Acceptance Rate (TAR) against the False Acceptance Rate (FAR) at different classification thresholds, providing insights into the trade-off between sensitivity and specificity. The AUC score summarizes this area into a single numerical value, describing the overall performance of a model across multiple thresholds.

In the developed system (Fig. 1), the user initially registers by providing a username and wearing a wireless EEG headset for 3 minutes. Thereafter, approximately 3 minutes are dedicated to the selection and training of the user-specific classification algorithm in WEKA (Thornton et al., 2013). The results of the classifier are saved in a database so that they can be used for the authentication phase. Once the optimal classifier has been trained, users can start over by providing their username (Fig. 2) and wearing the headset for 1 minute to gain access to the system (Fig. 3 and 4).

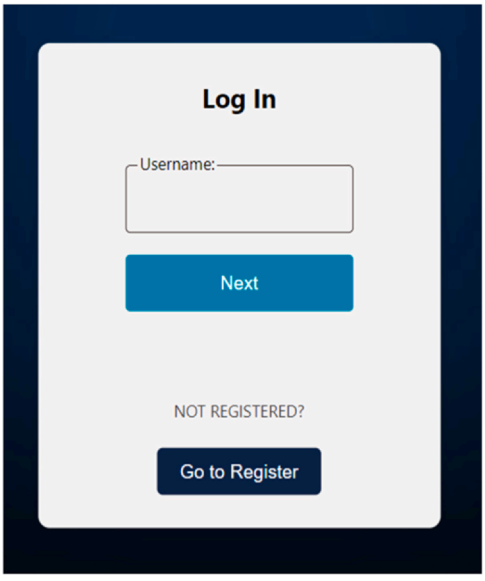

Fig. 2. The user interface of the developed authentication system.

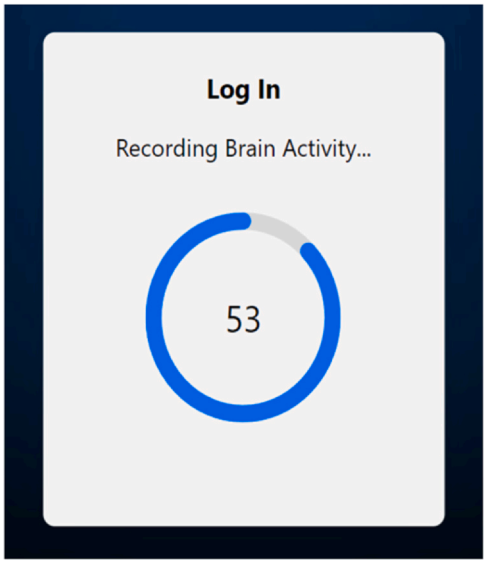

Fig. 3. The authentication process is depicted, where the user provides their username and wears the wireless EEG headset for 1 minute.

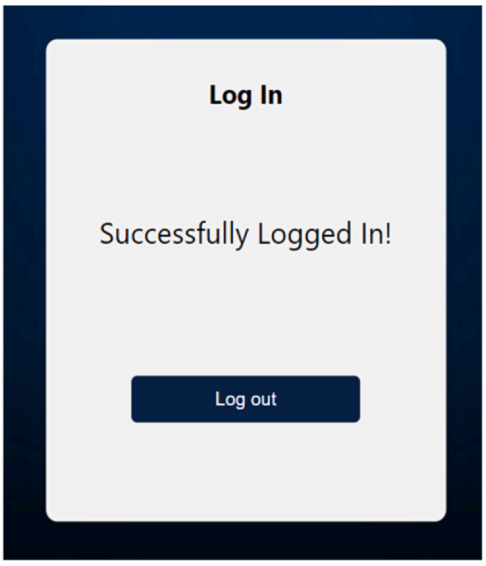

Fig. 4. Then, in real-time, the system evaluates the identity of the user and provides a decision.

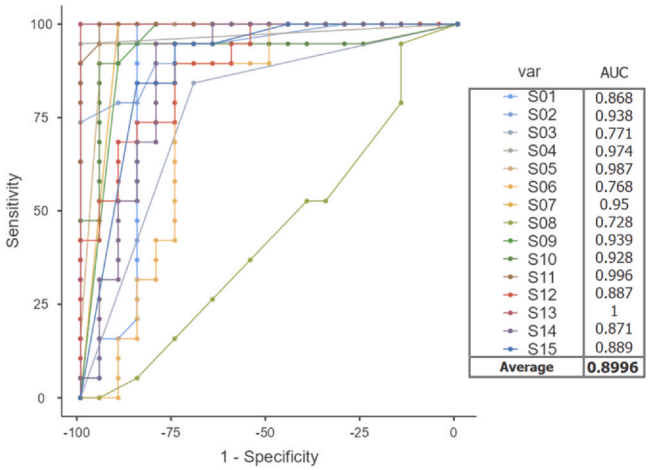

Fig. 5. Visual representation of ROC curves.

3. Results

The results from the authentication process of the 15 subjects are depicted in Table 1. The mean obtained accuracy was 85.4%. The best classification results (100%) were achieved for Participant 13, as the system accurately classified all the instances belonging to this subject while denying access to all the imposter instances. On the contrary, Participant 8 exhibited the lowest accuracy (62%), characterized by a False Rejection Rate (FRR) equal to 0.47. The system's average AUC value across the 15 subjects was found to be 0.8996, as shown in Fig. 5.

The mean sensitivity of the system was found to be 0.88 (± 0.01), while the specificity was 0.83 (± 0.01). The sensitivity, denoted by the True Acceptance Rate (TAR), represents the ratio of legitimate instances that were correctly granted access out of the total instances (39). The specificity, evaluated through the True Rejection Rate (TRR), describes the proportion of imposter instances that were correctly denied access out of the total 39 instances.

Upon observing the results, Participant 8 seems to be an outlier. Despite the overall normal distribution of the data, as confirmed by the Shapiro–Wilk test ($W = 0.94$ and $p = 0.42$), after visualizing the data through a cumulative distribution plot (Fig. 6) and plotting the detrended normal quantile-quantile (Q-Q) plot (Fig. 7), it becomes apparent that the accuracy for Participant 8 deviates significantly from the majority of subjects. Furthermore, the cumulative distribution plot of the accuracy distribution for all participants (Fig. 6) revealed that only 20% of the subjects had accuracies lower than 80%, while over 50% of the subjects had an accuracy of above 87%.

Despite the apparent results, we still employed statistical analysis to demonstrate the effectiveness of the developed system. We tested the

Table 1
Authentication results from testing with 15 participants.

	GRANT ACCESS		*DENY ACCESS*		*Sensitivity*	*Specificity*			
SUBJECT	GRANT	DENY	GRANT	DENY	TAR	TRR	FAR	FRR	**Accuracy**
S01	19	0	3	17	1	0.85	0.15	0	**92%**
S02	17	2	4	16	0.895	0.8	0.2	0.105	**85%**
S03	16	3	6	14	0.842	0.7	0.3	0.158	**77%**
S04	14	5	0	20	0.737	1	0	0.263	**87%**
S05	19	0	5	15	1	0.75	0.25	0	**87%**
S06	13	6	5	15	0.684	0.75	0.25	0.316	**72%**
S07	19	0	2	18	1	0.9	0.1	0	**95%**
S08	10	9	6	14	0.526	0.7	0.3	0.474	**62%**
S09	17	2	2	18	0.895	0.9	0.1	0.105	**90%**
S10	17	2	2	18	0.895	0.9	0.1	0.105	**90%**
S11	19	0	2	18	1	0.9	0.1	0	**95%**
S12	17	2	5	15	0.895	0.75	0.25	0.105	**82%**
S13	19	0	0	20	1	1	0	0	**100%**
S14	18	1	5	15	0.947	0.75	0.25	0.053	**85%**
S15	17	2	5	15	0.895	0.75	0.25	0.105	**82%**
Average					0.881	0.827	0.173	0.119	**85.4%**

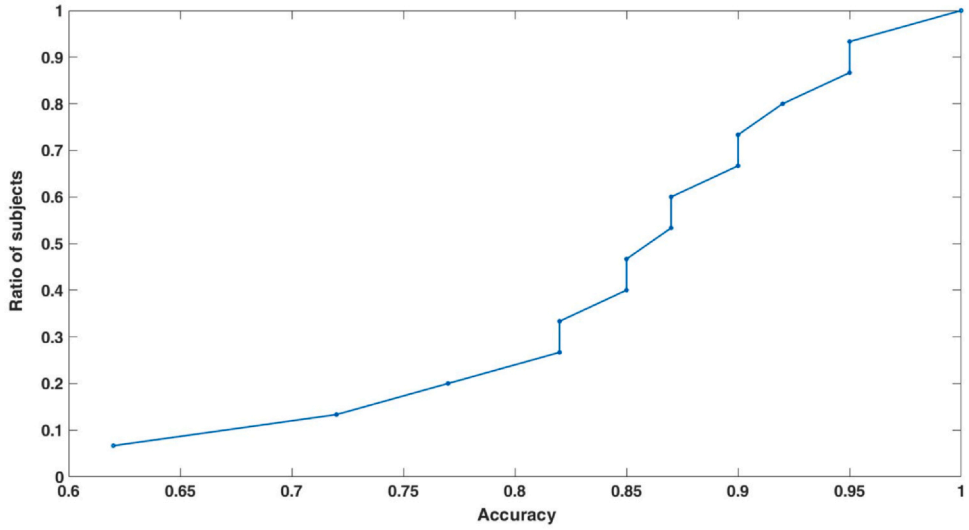

Fig. 6. Cumulative distribution plot of accuracy distribution in subject classification.

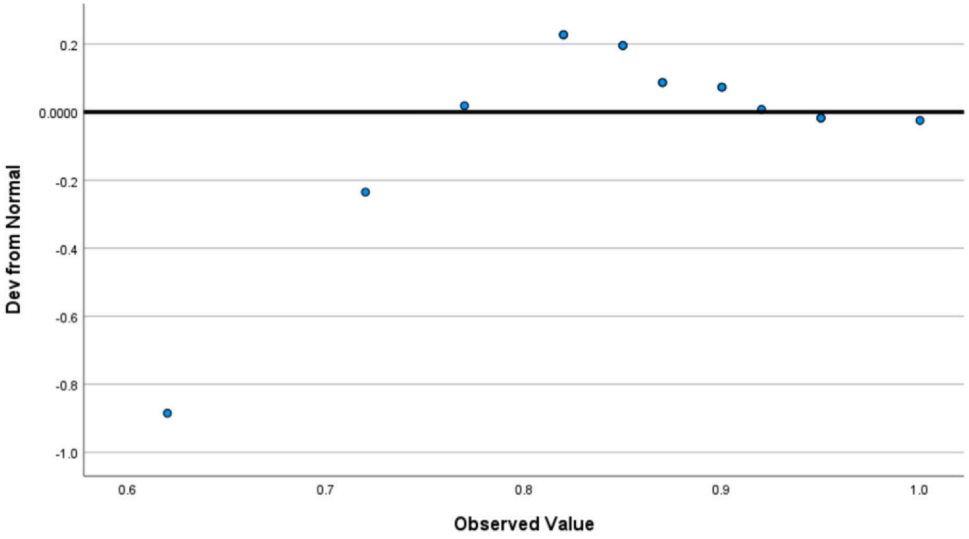

Fig. 7. Detrended normal Q-Q plot of accuracy values.

accuracy, FAR, and FRR using a one-sample t-test or a one-sample Wilcoxon W test when the variables were not normally distributed. The Shapiro–Wilk test of normality revealed that the accuracy ($W = 0.944$, $p = 0.429$) and FAR ($W = 0.884$, $p = 0.054$) are normally distributed while the FRR ($W = 0.813$, $p = 0.005$) is not. The one-sample t-test confirmed that the accuracy ($M = 85.4\%$, $SD = 9.7\%$) is notably higher than random guessing $t(14) = 14.2$, $p = 0.001$, and the FAR ($M = 0.17$, $SD = 0.1$) is substantially lower than random guessing $t(14) = -12.5$, $p = 0.001$. On the other hand, the W test revealed that the FRR ($M = 0.12$, $SD = 0.13$) is significantly lower than random guessing $W(14) = 0$, $p = 0.001$.

4. Discussion and conclusion

The integration of EEG signals into systems for human authentication has emerged as a promising remedy for the limitations inherent in existing biometric authentication methods that rely on features such as fingerprints (Matsumoto et al., 2002) or voice recognition (Wenger et al., 2021). EEG-based authentication offers a convenient and non-intrusive form of authentication coupled with robust security measures. Moreover, its applicability extends to high-security environments, ensuring both the vitality of the individual seeking access and compatibility with continuous user authentication systems (Nakanishi et al., 2009).

The novelty of this research lies in the adoption of a commercially available EEG sensor in combination with the use of Auto-WEKA, a machine-learning algorithm that selects and trains the optimal classification algorithm for each user. As a result, a promising overall mean accuracy of 85.4% was achieved. It is important to recognize that this performance was achieved despite the challenges posed by the low sampling rate in the recordings and the fact that the EEG setup was a single-channel device. This last realization adds value to our results, as previous works on EEG-based user authentication have achieved similar levels of performance after using a multi-channel EEG configuration. For instance, Paranjape et al. (2001) achieved an average classification accuracy of 80% using 8-channel EEG recordings, while Maiorana et al. (2016) utilized 19 channels to achieve a mean accuracy of 85.6%. In another study, Ong et al. (2018) achieved a maximum average accuracy of 89.21% through the use of 32 channels.

While traditional machine learning approaches, as demonstrated in this study, offer promising results, it is essential to acknowledge the importance of deep learning models that can excel in extracting intricate features from EEG signals, potentially leading to higher accuracy rates. However, it is crucial to consider the computational complexity, resource requirements, and interpretability issues associated with deep learning models. These models often demand large amounts of data for training, which might not always be readily available, especially in

specialized domains like EEG-based authentication. In comparison, a strong asset of our research is the speed at which authentication can be completed. The system has been designed to prioritize user convenience, as the authentication process can be completed within 1 minute. The fact that our proposed system successfully combines speed, accuracy, and user convenience makes it a promising piece of technological work and moves the field of biometric authentication a step closer to the development of high-security, practical user authentication configurations.

Regarding the future trajectory of EEG-based user authentication, several critical aspects need to be considered and addressed. Foremost, the sensitivity of EEG signals to external influences poses a noteworthy concern. A spectrum of external factors, ranging from the consumption of medication and coffee to variations in the environment of the recording (external noise and artifacts) can significantly impact the accuracy of the EEG recordings and subsequently the performance of the EEG-based authentication system. Robust methods to account for these influences must be developed to ensure consistent and reliable authentication outcomes. Furthermore, the permanence of brain waves remains largely unknown, primarily due to a lack of comprehensive, long-term studies. The evolution of brain waves with age and the change of patterns over an individual's lifespan could largely impact the consistency of the authentication system. A potential solution could involve implementing periodical recordings to provide updates to the biometric dataset. Lastly, in the present work, the accuracy of the developed system was tested with 15 individuals. Although this is a reasonable sample size in comparison to similar studies, conducting additional tests with larger data sets could further enhance the reliability of the findings. Conducting long-term research with repetitive experiments can be valuable for identifying the variability of EEG patterns over time as well as quantifying the degree of influence exerted by external factors, thus revealing their implications for the system's performance.

Funding

This research received no external funding.

Institutional review board statement

The research was approved by the Ethics Committee of the University of Sheffield. Participation was anonymous and confidential.

Declaration of Competing Interest

The authors declare no conflict of interest.

References

Abo-Zahhad, M., Ahmed, S.M., Abbas, S.N., 2016. A new multi-level approach to EEG based human authentication using eye blinking. Pattern Recognit. Lett. 82, 216–225. https://doi.org/10.1016/j.patrec.2015.07.034

Altahat, S., Wagner, M., Martinez Marroquin, E., 2015. Robust electroencephalogram channel set for person authentication. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Apr. 2015, pp. 997–1001. doi: 10.1109/ICASSP.2015.7178119.

Brigham, K., Kumar, B.V.K.V., 2010. Subject identification from electroencephalogram (EEG) signals during imagined speech. In: Proceedings of the fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Sep. 2010, pp. 1–8. doi: 10.1109/BTAS.2010.5634515.

Cai, D., Liu, K., Su, F., 2015. Local metric learning for EEG-based personal identification. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Apr. 2015, pp. 842–846. doi: 10.1109/ICASSP.2015.7178088.

Chowdhury, A.M.M., Imtiaz, M.H., 2023. A machine learning approach for person authentication from EEG signals. In: Proceedings of the IEEE 32nd Microelectronics Design & Test Symposium (MDTS), May 2023, pp. 1–5. doi: 10.1109/MDTS58049.2023.10168149.

Das, R., Maiorana, E., Campisi, P., 2018. Motor imagery for eeg biometrics using convolutional neural network. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Apr. 2018, pp. 2062–2066. doi:10.1109/ICASSP.2018.8461909.

Herley, C., Van Oorschot, P.C., Patrick, A.S., 2009. Passwords: if we're so smart, why are we still using them? Financial cryptography and data security. In: Dingledine, R., Golle, P. (Eds.), Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 230–237. https://doi.org/10.1007/978-3-642-03549-4_14

Hine, G.E., Maiorana, E., Campisi, P., 2017. Resting-state eeg: a study on its non-stationarity for biometric applications. In: Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Sep. 2017, pp. 1–5. doi:10.23919/BIOSIG.2017.8053519.

Jalaly Bidgoly, A., Jalaly Bidgoly, H., Arezoumand, Z., 2020. A survey on methods and challenges in EEG based authentication. Comput. Secur. 93, 101788. https://doi.org/10.1016/j.cose.2020.101788

Keshishzadeh, S., Fallah, A., Rashidi, S., 2016. Improved EEG based human authentication system on large dataset. In: Proceedings of the 24th Iranian Conference on Electrical Engineering (ICEE), May 2016, pp. 1165–1169. doi: 10.1109/IranianCEE.2016.7585697.

Liew, S.-H., Choo, Y.-H., Low, Y.F., Yusoh, Z.I.M., Yap, T.-B., Muda, A.K., 2015. Comparing features extraction methods for person authentication using EEG signals, pattern analysis, intelligent security and the internet of things. In: Abraham, A., Muda, A.K., Choo, Y.-H. (Eds.), Pattern Analysis, Intelligent Security and the Internet of Things. Springer International Publishing, Cham, pp. 225–235. https://doi.org/10.1007/978-3-319-17398-6_21

Maiorana, E., La Rocca, D., Campisi, P., 2016. On the permanence of EEG signals for biometric recognition. IEEE Trans. Inf. Forensics Secur. 11 (1), 163–175. https://doi.org/10.1109/TIFS.2015.2481870

Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S., 2002. Impact of artificial 'gummy' fingers on fingerprint systems. In: Optical Security and Counterfeit Deterrence Techniques IV, SPIE, Apr. 2002, pp. 275–289. doi: 10.1117/12.462719.

Nakanishi, I., Baba, S., Miyamoto, C., 2009. EEG based biometric authentication using new spectral features. In: Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Kanazawa, Japan: IEEE, Dec. 2009, pp. 651–654. doi: 10.1109/ISPACS.2009.538375.

Ong, Z. Ying, Saidatul, A., Ibrahim, Z., 2018. Power spectral density analysis for human EEG-based biometric identification. In: Proceedings of the International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA), Aug. 2018, pp. 1–6. doi:10.1109/ICASSDA.2018.8477604.

Paranjape, R.B., Mahovsky, J., Benedicenti, L., Koles, Z., 2001. The electroencephalogram as a biometric. In: Proceedings of the Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No. 01TH8555), vol. 2, May 2001, pp. 1363–1366. doi: 10.1109/CCECE.2001.933649.

Rahman, A., et al., 2021. Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms. IEEE Access, vol. 9, 94625–94643. https://doi.org/10.1109/ACCESS.2021.3092840

Seha, S.N.A., Hatzinakos, D., 2020. EEG-based human recognition using steady-state AEPs and subject-unique spatial filters. IEEE Trans. Inf. Forensics Secur., vol. 15, 3901–3910. https://doi.org/10.1109/TIFS.2020.3001729

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), 18. https://doi.org/10.3390/s22186929

Thornton, C., Hutter, F., Hoos, H.H., Leyton-Brown, K., 2013. Auto-WEKA: combined selection and hyperparameter optimization of classification algorithms. In: Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, in KDD '13. New York, NY, USA: Association for Computing Machinery, Aug. 2013, pp. 847–855. doi: 10.1145/2487575.2487629.

Valsaraj, A., Madala, I., Garg, N., Patil, M., Baths, V., 2020. Motor imagery based multimodal biometric user authentication system using EEG. In: Proceedings of the International Conference on Cyberworlds(CW), Sep. 2020, pp. 272–279. doi: 10.1109/CW49994.2020.00050.

Wenger, E., , 2021. Hello, it's me': deep learning-based speech synthesis attacks in the real world. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, in CCS '21. New York, NY, USA: Association for Computing Machinery, Nov. 2021, pp. 235–251. doi: 10.1145/3460120.3484742.

Yu, T., Wei, C.-S., Chiang, K.-J., Nakanishi, M., Jung, T.-P., 2019. EEG-based user authentication using a convolutional neural network. In: Proceedings of the 9th International IEEE/EMBS Conference on Neural Engineering (NER), March 2019, pp. 1011–1014. doi: 10.1109/NER.2019.8716965.