Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

TASK-INDEPENDENT EEG-BASED AUTHENTICATION

ABOOTHAR MAHMOOD SHAKIR *
Department of Information Technology and Computer Engineering, University of Qom, Iran.
Computer Techniques Engineering Department, College of Technical Engineering, The Islamic University, Najaf, Iraq. *Corresponding Author Email: abathermahmood560@gmail.com

AMIR JALALY BIDGOLY
Department of Information Technology and Computer Engineering, University of Qom, Iran.

Abstract

This paper introduces a cutting-edge approach to Electroencephalography (EEG) based authentication that transcends traditional task-specific requirements, significantly enhancing user experience and authentication accuracy. By employing a convolutional neural network (CNN) to develop a deep learning model, the study successfully extracts feature vectors from EEG signals without necessitating predefined tasks, offering a more adaptable and user-friendly alternative. The proposed system achieved a notable accuracy rate through experiments, including Single-Task and Multi-Task Feature Extraction methods. The study model achieved an accuracy rate of 95% in authentication by making enhancements to the Multi-Task methodology. These experimental insights underscore the viability and efficiency of task-independent EEG authentication while maintaining robust security measures.

Keywords: Authentication, EEG, User-Friendly, Task-Independent.

I. INTRODUCTION

In recent years, there has been a surge of interest in developing biometric authentication systems based on electroencephalography (EEG) signals. These systems hold great potential for revolutionizing the security field by offering a new level of authentication that is extremely difficult to falsify. Various protocols have been employed in EEG systems, encompassing non-task methods (such as resting state), motor and motor imagery tasks (e.g., hand movements), sensory input tasks (e.g., visual or auditory stimuli), and cognitive tasks (e.g., problem-solving, memory retrieval, and object recognition) [1]. Some studies have even explored the combination of multiple protocols or tasks, which can present greater challenges and complexity for users compared to single-task approaches [2], [3]. Despite EEG signals' numerous advantages as a biometric factor in authentication systems, their practical application is still in the research and testing stage, with several challenges impeding their use in real-life scenarios. One of the major challenges is to ensure user-friendliness [4]. Several factors should be considered to enhance the user-friendly nature of EEG-based authentication systems.

One crucial factor is the ease of use of both the hardware and software components of the system. Additionally, the speed and efficiency of the authentication process play a vital role, as users expect fast and accurate systems, with delays or errors diminishing the overall user-friendliness. Another significant factor is the nature of the tasks involved. Implementing complex tasks within the system might not be pleasant to users, potentially leading to a perception of unfriendliness in practice.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

An important concern with EEG-based authentication is requiring users to perform specific tasks, such as mental calculations or motor movements, which can be time-consuming and challenging for some individuals. Furthermore, the accuracy of task-based EEG authentication can be influenced by factors such as fatigue and cognitive load, further compromising the system's user-friendliness. To tackle this challenge, our proposed solution is to eliminate the need for users to perform specific tasks and instead offer a selection of tasks from which they can choose. This approach allows users to select the most suitable and convenient task for authentication, granting them access to the system. The main goal of this study is to answer the following inquiries: Can a viable approach be devised to establish task-independent EEG-based authentication? Can deep learning methods be utilized to accomplish this? Is it feasible to train a model on different tasks? By exploring these questions, our research aims to offer solutions and contribute to advancing EEG-based authentication systems that are more efficient and adaptable.

The rest of this paper is organized as follows. In the next section, we present a brief review of previous research conducted in the field of EEG-based authentication, covering studies that involve various tasks as well as those that are not task-dependent. In Section 0, the proposed authentication method is discussed and analyzed across three distinct sections. A thorough description of the experiments conducted and their results is presented in Section 0. Finally, the paper concludes by summarizing the findings and providing suggestions for future research endeavors.

II. RELATED WORKS

Compared to alternative methods such as facial recognition or fingerprints, the utilization of EEG signals as a biometric system presents unique challenges in terms of spoofing. Brain-based systems demonstrate resilience against tampering and coercion, as stress signals within brain waves can prevent unauthorized access [5]. Some studies have extensively explored EEG-based authentication and provided valuable insights into various protocols and methodologies. Specifically, they focused on the Resting State protocol in their research, which serves as a foundation for understanding baseline brain patterns [6-8].

Other studies investigated the use of auditory [9] and visual [10] stimuli in EEG-based authentication. Additionally, some investigations utilized protocols involving mental activities like motor imagery [11], while others explored hybrid approaches combining multiple methods [12]. Although these studies have contributed valuable insights, their complexity can pose challenges and be time-consuming for users.

In summary, while there is extensive literature on task-specific EEG authentication utilizing various protocols and methods, a careful analysis of these studies reveals limitations and gaps the proposed task-independent approach seeks to overcome. Currently, there is a lack of extensive research on task-independent EEG-based authentication methods. Maiorana [13] conducted a study to investigate whether EEG-based biometric recognition could be achieved independent of specific tasks. They

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

employed deep learning techniques, specifically Siamese convolutional neural networks, to extract personalized template representations from EEG recordings. The study utilized EEG data collected from 45 subjects who performed diverse tasks. The objective was to assess if individuals could be identified based solely on their brain signals, regardless of the task being performed. While achieving low error rates, the study did not explicitly mention the authentication accuracy rate of this method, leaving room for further evaluation.

The use of EEG signals for subject identification was investigated by V. D et al.[14], with a focus on extracting subject-specific traits and addressing temporal stability challenges. The study compared different classifiers and evaluated their performance in intrasession and intersession testing scenarios. Data from 40 subjects, collected using a 128-channel EEG system, is analyzed using features like autoregressive coefficients and spectral features. The UBM-GMM classifier demonstrates strong performance in both classical and intersession testing, indicating its effectiveness for subject identification. The study concludes that subject-specific signatures can be identified in EEG signals irrespective of the task performed, highlighting the potential of EEG-based subject identification methods. This paper concentrates solely on utilizing auditory stimuli for conducting EEG-based authentication tests, without considering other protocols.

Addressing the need for task-independent EEG-based authentication, Kumar et al. [15] proposed new techniques for identifying individuals using EEG signals. By modifying the i-vector and x-vector systems and incorporating multi-channel information, the authors achieved improved performance in person identification.

The study emphasizes the presence of person-specific signatures in EEG data and underscores the importance of handling channel information differently. While the exact accuracy rate is not provided, the modified i-vector system shows a significant absolute improvement over the baseline, indicating the potential of task-independent EEG-based authentication methods. The available literature in this field is limited, with a predominant emphasis on evaluating the feasibility of task-independent EEG-based biometric authentication. However, the studies conducted thus far have explored a restricted range of tasks and protocols.

III. PROPOSED METHOD

To enhance the user-friendliness of the EEG-based authentication system, we propose the adoption of a deep learning model that offers flexibility across different tasks. The suggested model follows a convolutional neural network (*CNN*) architecture well-suited for deep learning tasks. The input to the model consists of EEG signal samples collected from individuals, containing valuable information about brain activity that can be utilized for distinguishing individuals. The model processes these EEG samples through its layers, including convolutional and pooling layers, to extract relevant features from the input data. Fig 1 depicts the overall structure of the utilized model.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

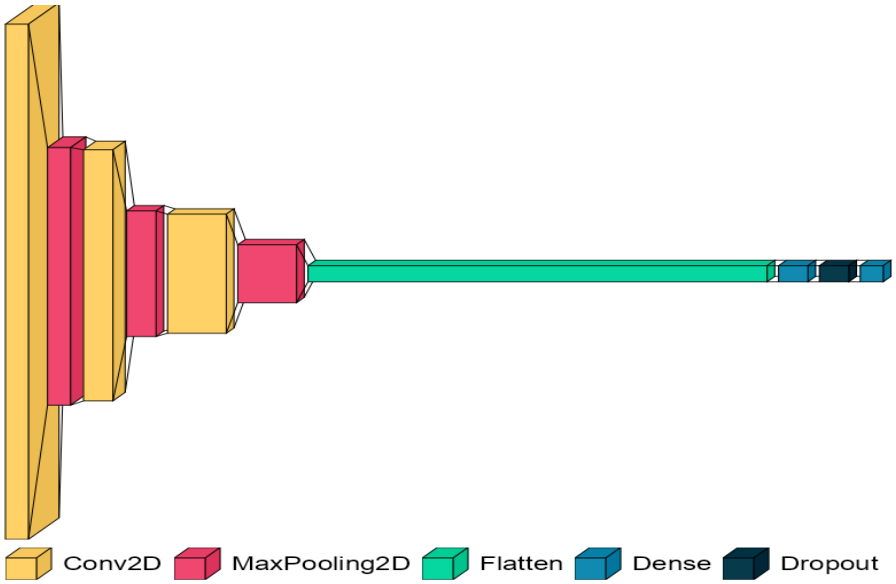

Fig 1: The architecture of *CNN* the model

The last layer of the classification model is eliminated to acquire feature vectors for individuals. The output of the preceding layer, the penultimate layer, contains high-level abstract representations of the EEG signals. These representations, referred to as feature vectors, capture the essential characteristics and discriminative information of each individual's EEG patterns. The extracted feature vectors are then securely stored in a database and used for user authentication. During the authentication process, the input EEG signals from a user are compared to the stored feature vectors. By measuring the similarity or dissimilarity between the input signals and the stored feature vectors, the system can determine the authenticity and identity of the user. The architectural layers of the CNN model are derived from [8], as depicted in Fig 2. The sole modification pertained to adjusting the number of neurons in the first dense layer.

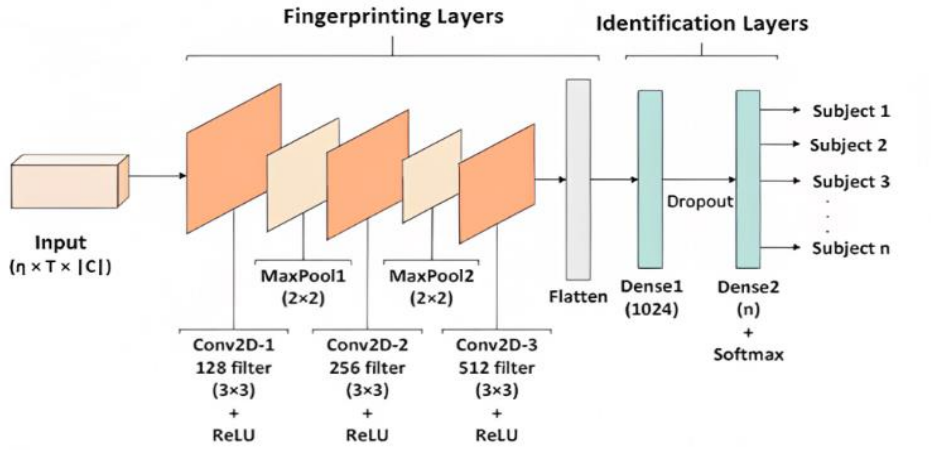

Fig 2: Layers of the CNN model [8]

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

The implementation and testing of our proposed method were carried out in two parts. Both phases aimed to enhance the user-friendliness of the authentication system and develop a model that allows users to log in using their preferred protocol.

A. Single-Task Feature Extraction

In this approach, the model undergoes signal pre-processing before being exclusively trained on examples from a specific "source task." Following training, feature vectors are extracted from individuals' data for the source task and stored in the system. When individuals interact with the system, they choose one of the suggested "target tasks" to perform. The corresponding feature vector is then extracted and compared to the stored feature vectors for authentication. The method's process is illustrated in Fig 3.

This method is referred to as *STFE* (Single-Task Feature Extraction). In simple terms, the *STFE* method involves training the model on a single task, but it can be used for authentication purposes with other tasks present in the dataset. The primary objective of this step is to assess the model's generalizability. By training the model on the source task and evaluating its performance on target tasks, we aim to demonstrate that our proposed model can accurately identify individuals' identities without relying on a specific task.

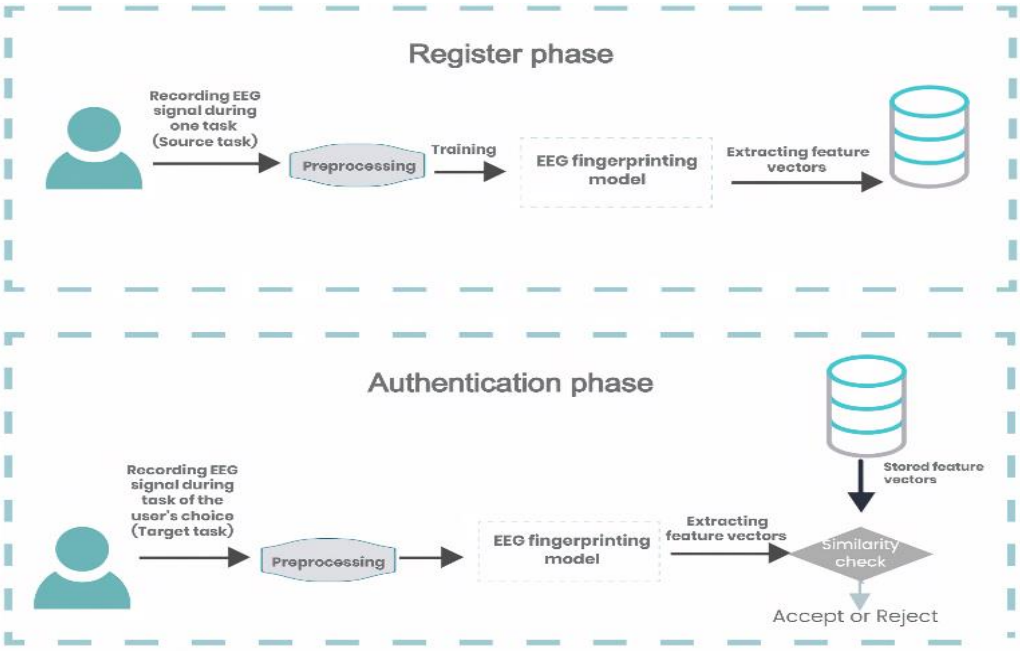

Fig 3: STFE Feature Extraction

B. Multi-Task Feature Extraction

The innovative aspect of this research becomes evident in this particular section of the experiments. To date, no prior studies in EEG-based authentication have trained their proposed models using multiple tasks, as most research in this field has focused on utilizing only a single task.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

The first step involves signal pre-processing to prepare the samples of individuals for model training. Following pre-processing, a *CNN* model is trained using samples from all available tasks. Unlike previous studies in EEG-based biometric authentication, which typically focused on training models with a single protocol, our approach involves training the model with multiple protocols.

The feature vectors obtained from this training process are stored in the system for authentication. We refer to this method as *MTFE* (Multi-Task Feature Extraction). The distinction between this method and the previous one lies in the training stage of the model. In the *STFE* approach, the model is trained using the signal from a single source task, such as task number 1. However, in the *MTFE* approach, the model is trained using signals associated with several source tasks, such as tasks 1 to 4.

To log a user into the system and authenticate their identity, the user is presented with a selection of tasks from which they can choose. The system records the user's EEG signals while they perform the chosen task and extracts the corresponding feature vector. In the final step, this feature vector is compared to the stored feature vectors in the system to authenticate the user's identity.

C. Authentication Phase

Our main focus in this section is to thoroughly examine and explore the intricacies of the authentication stage, regardless of the specific model architecture chosen. We aim to thoroughly understand the mechanisms and processes involved in authenticating and verifying individuals, by delving into the details and complexities of this stage.

At the heart of the *CNN* model lies a fingerprint model, achieved by excluding the identification layers. The primary objective of the fingerprint section is to produce feature vectors for individuals. By comparing these feature vectors with others, we can ascertain whether they belong to the same person or not [8].

To assess the similarity between feature vectors and determine the identity of a person, the distance between the vectors is computed. This involves utilizing methods such as *Manhattan*, *Euclidean*, or *Cosine* distance measurements. These techniques enable the comparison of fingerprints or feature vectors and aid in confirming or rejecting an individual's identity.[8] During our experiments, we chose to employ the *cosine* distance due to its superior performance in terms of authentication accuracy compared to other methods. The formula for computing the *cosine* distance is as follows:

$$cosine\_dist(A,B) = \frac{\mathrm{A}\,.\mathrm{B}}{\|\mathrm{A}\|_2\|\mathrm{B}\|_2} = \frac{\sum_{i=1}^{m} a_i b_i}{\sqrt{\sum_{i=1}^{m} a_i^2}\sqrt{\sum_{i=1}^{m} b_i^2}} \qquad (1)$$

Where $A \in \mathbb{R}^m$ and $B \in \mathbb{R}^m$ are vectors, and $\| \|_2$ is 2-norm.

To summarize, the authentication process includes capturing the user's EEG signal during registration and creating a fingerprint using a deep neural network [8]. This fingerprint is stored as the user's authentication data. During login, the system records the user's EEG signal once more and compares the generated fingerprint with the stored

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

information using the cosine distance. The threshold parameter can be adjusted using the ROC plot to minimize both the false acceptance rate and false rejection rate [8]. If the distance between the fingerprints is below the defined threshold, the user is authenticated; otherwise, they are denied access.

IV. EXPERIMENTS AND RESULTS

A. Dataset

The *Physionet EEG Motor Movement/Imagery* dataset [16], [17] was employed in our experiments. This dataset demonstrated satisfactory accuracy for the proposed authentication model described in [8]. Consequently, we conducted further tests using the MMI dataset to enhance the model's robustness and ensure data security. The MMI dataset comprises more than 1500 EEG recordings, each lasting between one and two minutes, acquired from 109 healthy individuals. These recordings were collected using 64 channels at a sampling rate of 160 Hz.

The study encompassed 14 experimental sessions where participants engaged in a diverse range of tasks. These tasks included baseline activities with both eyes open and closed, as well as activities involving motor movement and mental imagery. The motor movement tasks involved responding to a target appearing on the screen by physically opening and closing the corresponding fist or both fists/feet. In contrast, the imagery tasks required participants to imagine performing the same actions. Following each task, participants were instructed to relax. The inclusion of these tasks provided diverse data for analysis and exploration in the study.

B. Evaluation

The provided model is a sequential convolutional neural network (*CNN*) to classify EEG signals. It includes three convolutional layers with progressively increasing filter numbers, followed by max-pooling layers for downsampling. The flattened output is then passed through two fully connected layers with ReLU activation. A dropout layer is incorporated to prevent overfitting, and the final output layer applies softmax activation for multi-class classification. The model is compiled using categorical cross-entropy loss and RMSprop optimizer.

The *Gram-Schmidt* orthogonalization process was applied in the cited paper [8] to identify the effective channels Oz, T7, and Cz. Out of the total 64 channels available, these top three channels were specifically chosen and employed in our experimental tests.

1) STFE method

During the initial phase of the experiments, we aimed to assess the capability of the model by training it on a particular task and then evaluating its performance on different tasks. In each experiment, the model is trained using one task's signals. The resulting feature vectors are stored in the system. Additionally, the model extracts feature vectors related to other tasks. To assess authentication accuracy, the distance between these vectors is

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

measured. The findings of the *STFE* phase tests are presented in *Table I*. The average accuracy obtained in this method is about 89%.

Table I: Authentication accuracy for STFE experiments

		Testing Tasks					
		Task1	Task2	Task3	Task4	Task5	Task6
Training Tasks	Task1	-----	0.86	0.85	0.91	0.87	0.89
	Task2	0.86	-----	0.87	0.89	0.85	0.87
	Task3	0.90	0.88	-----	0.91	0.93	0.90
	Task4	0.92	0.90	0.90	-----	0.90	0.89
	Task5	0.88	0.86	0.91	0.91	-----	0.86
	Task6	0.90	0.88	0.88	0.91	0.88	-----

2) MTFE method

During this stage, experiments were conducted to train the model using several distinct tasks. In the preceding experimental phase, only a single task was employed for model training. However, in the current phase, multiple tasks are simultaneously utilized to train the model. These tasks encompass activities such as resting with eyes open, resting with eyes closed, opening and closing the left or right fist, and imagining the action of opening and closing the left fist or right fist.

Once the model was trained, the system extracted and stored the feature vectors associated with each task. To assess the accuracy of authentication, the feature vectors for a particular task were selected as tests and compared against the stored feature vectors in the system. The outcome of the initial set of tests, which evaluated the authentication accuracy, is presented in Table *II*.

Table II: The first test in the MTFE phase to evaluate authentication accuracy

		Stored Tasks In The System	
		Task1	Task2
Testing Tasks	Task1	-----	0.70
	Task2	0.70	-----
	Task3	0.72	0.74
	Task4	0.71	0.73

In the initial experiment, we trained the model using four tasks, and two feature vectors associated with tasks 1 and 2 were stored in the system. For the test, we assumed that the user aims to log in to the system using one of the four tasks (numbered 1 to 4). In each case, we evaluated the accuracy of authentication and measured it using a ROC curve. The initial test results yielded an average accuracy of 71%.

To enhance authentication accuracy in the subsequent phase, we decreased the number of neurons in the final dense layer. Before this adjustment, the model's feature vectors had a size of 256. By reducing the neurons in the last layer, the output feature vectors were also downsized. We conducted tests at various stages, and after each reduction, we assessed the authentication accuracy.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

We gradually reduced the number of neurons in the last layer from 250 to 10 and trained the model with 4 tasks. Each time, we extracted and stored feature vectors to check the authentication accuracy. To assess this accuracy, we compared the feature vectors of each task one by one and measured their distances. The authentication accuracy was then reported using the ROC curve. For example, **Error! Reference source not found.** shows the ROC curves associated with the state where the number of neurons is 30. The reported AUC value indicates the authentication accuracy. In this instance, the average authentication accuracy stood at 95%.

The last layer of the model was evaluated using various neuron values, and Table *III* provides a breakdown of the test results. The significant finding from these experiments was that decreasing the number of neurons enhanced the accuracy of authentication for different tasks. This observation highlights the crucial role of this parameter in the model's architecture.

Table III: The investigation into how the number of neurons in the last layer of the model impacts authentication accuracy across different tasks

The number of neurons		Task1	Task2	Task4
256	Task1	1.00	0.70	0.71
	Task2	0.70	1.00	0.73
	Task3	0.72	0.74	0.72
100	Task1	0.99	0.82	0.84
	Task2	0.82	0.99	0.84
	Task3	0.84	0.84	0.85
50	Task1	0.99	0.90	0.89
	Task2	0.90	0.99	0.86
	Task3	0.89	0.88	0.90
30	Task1	0.99	0.94	0.95
	Task2	0.94	0.99	0.96
	Task3	0.94	0.96	0.97
20	Task1	0.99	0.94	0.94
	Task2	0.94	0.99	0.94
	Task3	0.94	0.96	0.95
10	Task1	0.99	0.95	0.96
	Task2	0.95	0.99	0.95
	Task3	0.96	0.96	0.96

To determine the best value for the parameter (number of neurons in the last layer), we calculated the average accuracy from each experiment. Fig 4 illustrates the average accuracy achieved in each test. Based on the figure, the optimal number of neurons appears to be 30. In this case, the average authentication accuracy reaches 95%. This finding suggests that if users attempt to log into the system using any of the four available tasks, they can expect a 95% accuracy rate for authentication.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

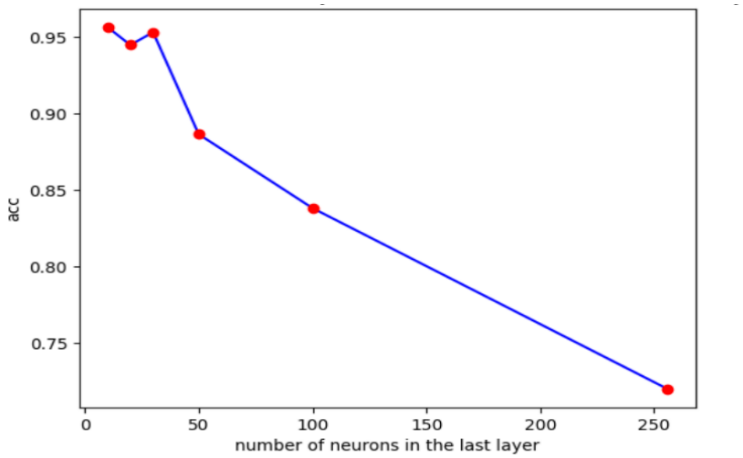

Fig 4: The impact of the number of neurons in the last layer of the model on the average authentication accuracy for different tasks.

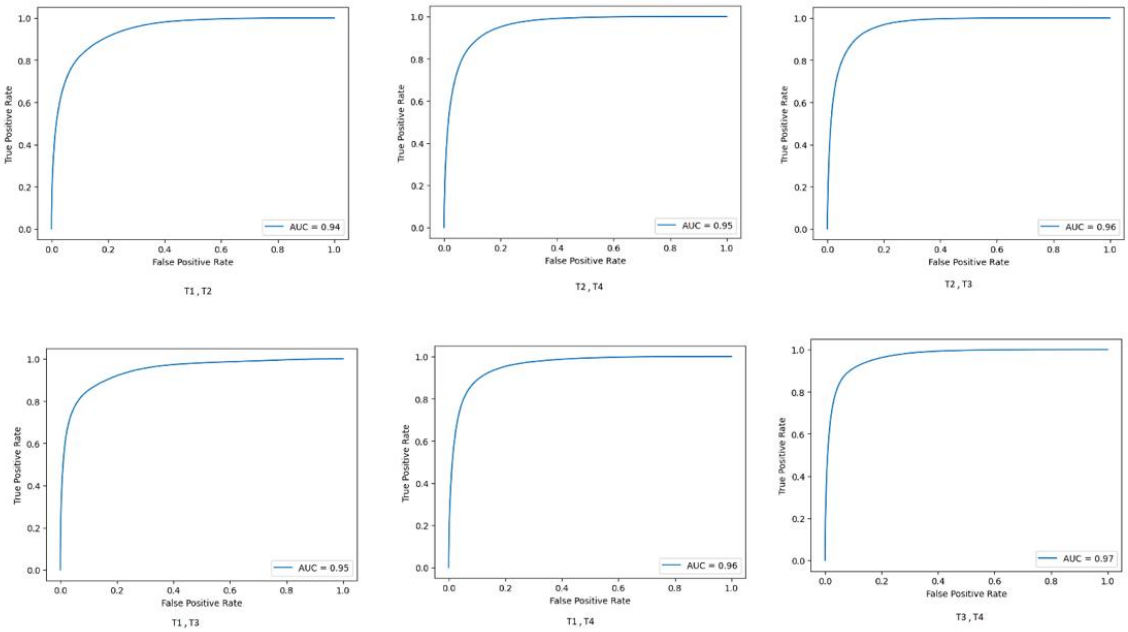

Fig 5: ROC curves to assess the authentication accuracy when the neural network's last layer contains 30 neurons

V. COMPARISON WITH OTHER METHODS

In the field of EEG-based identity authentication, various methods have been developed and evaluated for their accuracy and reliability. The following comparison highlights the performance of different methods based on recent studies:

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

Table IV: Comparison With Other Methods

Method	Accuracy	Reference
PSD	95%	Stergiadis et al. [18]
FSP	88.88%	Zeng et al. [19]
SVM	97%	Shinde and Kamthekar [20]
NN	99%	Ortega et al. [22]
NN & BN	95%	Zeynali and Seyedarabi [21]
Proposed Model	**95%**	**This Study**

Stergiadis et al. [18] Stergiadis et al. utilized PSD for EEG signal authentication, achieving an accuracy of 95%. Their method focuses on leveraging the power spectral density features of EEG signals, which are indicative of the brain's electrical activity and useful for identifying individuals. Zeng et al. [19] introduced a framework that combines face image-based rapid serial visual presentation with EEG signals, achieving an accuracy of 88.88%. This method relies on event-related potential (ERP) components induced by self and non-self faces, combined with Hierarchical Discriminant Component Analysis (HDCA) and Genetic Algorithm (GA) for optimized channel selection. Shinde and Kamthekar [20] applied the Chirplet transform for feature extraction and used SVM for classification, reaching an accuracy of 97%. Their study emphasizes the efficiency of SVM in improving the recognition rates of EEG-based authentication systems. Ortega et al. [21] implemented a neural network for EEG signal classification, achieving an impressive accuracy of 99%. This method demonstrates the potential of neural networks in capturing complex patterns in EEG data for reliable identity authentication. Zeynali and Seyedarabi [22] combined neural networks with Bayesian networks to develop a single-channel EEG authentication system, achieving an accuracy of 95%. Their approach optimizes electrode placement based on different mental activities, enhancing the overall system performance. The proposed model in this study also achieves an accuracy of 95%. This model enhances the Mask R-CNN architecture for brain tumor segmentation, integrating advanced feature extraction, ROI generation, ROI alignment, and mask acquisition components to improve the segmentation accuracy. The model's performance is on par with other high-accuracy methods, demonstrating its effectiveness in the domain of EEG-based authentication. Overall, the comparison reveals that neural network-based methods, particularly those incorporating additional layers or optimization techniques, tend to achieve higher accuracy rates. The proposed model, with its innovative enhancements, performs competitively, underscoring its potential for practical application in EEG-based identity authentication systems.

VI. DISCUSSION

The comparison of various EEG-based identity verification methods offers valuable insights into the strengths and limitations of different approaches. Assessing the performance of the proposed model within the context of existing methods provides a comprehensive understanding of its position in the broader landscape of EEG-based authentication systems. The proposed model achieves a 95% accuracy, competing with

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

other high-accuracy methods such as the neural network (NN) approach by Ortega et al. [21] with 99% accuracy and the support vector machine (SVM) method by Shinde and Kamthekar [20] with 97% accuracy. This demonstrates the robustness and reliability of the proposed model in EEG-based authentication. Improvements to the CNN architecture in feature extraction, ROI generation, ROI alignment, and mask acquisition contribute to the model's high accuracy and showcase the potential of advanced neural network architectures in processing and classifying EEG signals. The comparison highlights a range of methodologies, from traditional SVM techniques to more complex neural networks and hybrid models (NN & BN). Each method offers distinct advantages, such as neural networks' ability to capture intricate EEG data patterns or SVM's efficiency in handling high-dimensional feature spaces.

The high accuracy rates achieved by these methods, including the proposed model, emphasize the potential of EEG-based authentication systems in offering secure and reliable biometric solutions. These systems can be particularly useful in scenarios where traditional biometric methods like fingerprint or facial recognition may be compromised or inadequate. A significant advantage of the proposed model is its versatility across various tasks. By utilizing advanced neural network enhancements, the model is not only effective for identity verification but also excels in other EEG-based applications, such as cognitive state monitoring, emotion recognition, and neurological disorder diagnosis. This broad applicability further highlights the model's robustness and potential for widespread use in diverse domains. While the proposed model shows promising results, further research and development could enhance its performance and applicability. Future studies should evaluate the model's scalability and generalization across larger and more diverse datasets to ensure its effectiveness in different real-world scenarios with varying EEG signal characteristics. Investigating the feasibility of real-time implementation of the proposed model is crucial, involving optimizing the model for faster processing times while maintaining accuracy for practical use in live authentication systems.

EEG signals often encounter noise and artifacts that can impact authentication system accuracy. Developing robust preprocessing techniques and incorporating noise-robust algorithms could further enhance the reliability of the proposed model. Ensuring that the authentication process is user-friendly and does not cause discomfort or inconvenience is vital for widespread adoption. Future work could explore the ergonomic aspects of EEG device design and overall user experience. The proposed model, with its innovative enhancements to the Mask R-CNN architecture, shows significant potential in the field of EEG-based identity verification. Its competitive accuracy, combined with the strengths of neural network-based approaches, positions it as a viable option for secure biometric systems. Continued research and development, focusing on scalability, real-time implementation, robustness, and user experience, will be crucial in realizing the full potential of EEG-based authentication technologies. By building on these findings, future studies can contribute to advancing secure and reliable biometric systems, leveraging the unique capabilities of EEG signals for identity verification and beyond.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

VII. CONCLUSION

In conclusion, this study introduces a promising task-independent EEG-based authentication system that significantly enhances user-friendliness by allowing flexibility in task selection. By employing deep learning techniques and optimizing neural network architecture, particularly by determining the optimal number of neurons in the last layer to be 30, the system achieves an impressive authentication accuracy of 95%. This approach effectively addresses the limitations of current EEG-based authentication systems which require specific tasks, thereby offering a more convenient and efficient method for user verification. The findings underscore the potential of the proposed system for broad and reliable applications in secure authentication, highlighting the importance of further research to refine the technology for even greater accuracy, stability, and user convenience.

References

1) H. L. Chan, P. C. Kuo, C. Y. Cheng, and Y. S. Chen, “Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition,” Front. Neuroinform., vol. 12, no. October, pp. 1–15, 2018, doi: 10.3389/fninf.2018.00066.

2) A. Vahid and E. Arbabi, “Human identification with EEG signals in different emotional states,” 2016 23rd Iran. Conf. Biomed. Eng. 2016 1st Int. Iran. Conf. Biomed. Eng. ICBME 2016, no. November, pp. 242–246, 2017, doi: 10.1109/ICBME.2016.7890964.

3) T. Pham, W. Ma, D. Tran, D. S. Tran, and D. Phung, “A study on the stability of EEG signals for user authentication,” Int. IEEE/EMBS Conf. Neural Eng. NER, vol. 2015-July, pp. 122–125, 2015, doi: 10.1109/NER.2015.7146575.

4) A. Jalaly Bidgoly, H. Jalaly Bidgoly, and Z. Arezoumand, “A survey on methods and challenges in EEG based authentication,” Comput. Secur., vol. 93, 2020, doi: 10.1016/j.cose.2020.101788.

5) J. Klonovs, C. Petersen, H. Olesen, and A. Hammershoj, “ID proof on the go: Development of a mobile EEG-based biometric authentication system,” IEEE Veh. Technol. Mag., vol. 8, no. 1, pp. 81–89, 2013, doi: 10.1109/MVT.2012.2234056.

6) T. Schons, G. J. P. Moreira, P. H. L. Silva, V. N. Coelho, and E. J. S. Luz, “Convolutional network for EEG-based biometric,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10657 LNCS, pp. 601–608, 2018, doi: 10.1007/978-3-319-75193-1_72.

7) L. Ma, J. W. Minett, T. Blu, and W. S. Y. Wang, “Resting State EEG-based biometrics for individual identification using convolutional neural networks,” Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS, vol. 2015-Novem, pp. 2848–2851, 2015, doi: 10.1109/EMBC.2015.7318985.

8) A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, “Towards a universal and privacy preserving EEG-based authentication system,” Sci. Rep., vol. 12, no. 1, pp. 1–9, 2022, doi: 10.1038/s41598-022-06527-7.

9) N. A. Alzahab, A. Di Iorio, M. Baldi, and L. Scalise, “Effect of Auditory Stimuli on Electroencephalography-based Authentication,” 2022 IEEE Int. Work. Metrol. Ext. Reality, Artif. Intell. Neural Eng. MetroXRAINE 2022 - Proc., pp. 388–392, 2022, doi: 10.1109/MetroXRAINE54828.2022.9967652.

10) Q. Gui, Z. Jin, and W. Xu, “Exploring EEG-based biometrics for user identification and authentication,” 2014 IEEE Signal Process. Med. Biol. Symp. IEEE SPMB 2014 - Proc., 2014, doi: 10.1109/SPMB.2014.7002950.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 09:2024
DOI: 10.5281/zenodo.13734700

11) Y. Sun, F. P. W. Lo, and B. Lo, “EEG-based user identification system using 1D-convolutional long short-term memory neural networks,” Expert Syst. Appl., vol. 125, pp. 259–267, 2019, doi: 10.1016/j.eswa.2019.01.080.

12) F. Yousefi, H. Kolivand, and T. Baker, “SaS-BCI: a new strategy to predict image memorability and use mental imagery as a brain-based biometric authentication,” Neural Comput. Appl., vol. 33, no. 9, pp. 4283–4297, 2021, doi: 10.1007/s00521-020-05247-1.

13) E. Maiorana, “Learning deep features for task-independent EEG-based biometric verification,” Pattern Recognit. Lett., vol. 143, pp. 122–129, 2021, doi: 10.1016/j.patrec.2021.01.004.

14) V. D et al., “Task-Independent EEG based Subject Identification using Auditory Stimulus,” Proc. Work. Speech, Music Mind, vol. 2018, no. 2018, pp. 26–30, 2018, doi: 10.21437/smm.2018-6.

15) M. G. Kumar, M. S. Saranya, S. Narayanan, M. Sur, and H. A. Murthy, “Subspace techniques for task-independent EEG person identification,” Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS, pp. 4545–4548, 2019, doi: 10.1109/EMBC.2019.8857426.

16) A. L. Goldberger et al., “PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals,” Circulation, 2000.

17) G. Schalk, D. J. McFarland, T. Hinterberger, N. Birbaumer, and J. R. Wolpaw, “BCI2000: a general-purpose brain-computer interface (BCI) system,” IEEE Trans. Biomed. Eng., vol. 51, no. 6, pp. 1034–1043, 2004.

18) Birbaumer, and J. R. Wolpaw, “BCI2000: a general- purpose brain-computer interface (BCI) system,” IEEE Trans. Biomed. Eng., vol. 51, no. 6, pp. 1034–1043, 2004.

19) Zeng, Ying, et al. "EEG-based identity authentication framework using face rapid serial visual presentation with optimized channels." Sensors 19.1 (2018): 6

20) Shinde, Sonal Suhas, and Swati S. Kamthekar. "Person Authentication Using EEG Signal that Uses Chirplet and SVM." Computational Vision and Bio-Inspired Computing: ICCVBIC 2019. Springer International Publishing, 2020.

21) Ortega, Jordan, et al. "Biometric person authentication using a wireless EEG device." Innovation in Information Systems and Technologies to Support Learning Research: Proceedings of EMENA-ISTL 2019 3. Springer International Publishing, 2020.

22) Zeynali, M., and H. Seyedarabi. "EEG-based single-channel authentication systems with optimum electrode placement for different mental activities. Biomed J 42 (4): 261–267." (2019).