BrainNet: Improving Brainwave-based Biometric Recognition with Siamese Networks

Matin Fallahi
KASTEL Security Research Labs, KIT
Karlsruhe, Germany
matin.fallahi@kit.edu

Thorsten Strufe
KASTEL Security Research Labs, KIT
Karlsruhe, Germany
strufe@kit.edu

Patricia Arias-Cabarcos
Paderborn University
Paderborn, Germany
pac@mail.upb.de

***Abstract*—With the advent of consumer wearables that capture brain activity, the use of brainwaves to verify a user's identity has been proposed as a convenient alternative to passwords. While recent work on brain biometrics shows feasible performance, it falls short in considering practical applicability. We propose a new solution, BrainNet, which trains a Siamese Network to measure the similarity of two electroencephalogram (EEG) inputs, and uses time-locked brain reactions instead of continuous mental activity to improve accuracy. This approach removes the need for retraining the brainwave recognition system, a common pitfall in current solutions, facilitating practical deployment. Furthermore, BrainNet achieves Equal Error Rates (EERs) of 0.14% in verification mode and 0.34% in identification mode, outperforming the state of the art even when evaluated under unseen attacker scenarios.**

***Index Terms*—brain biometrics, user authentication, computer security, electroencephalogram (EEG)**

I. Introduction

Modern wearable technology incorporates a range of sensors that allow for the implementation of rich innovative services, such as novel forms of biometrics. In particular, the democratization of Brain Computer interfaces (BCIs) [1], [2], brings about the potential to identify users by their mental activity through electroencephalogram (EEG) readings, which record electrical signals produced by the brain. Here, the ongoing miniaturization and integration of EEG sensors into wearables, such as earbuds or Virtual Reality headsets (see Figure 1), might play a positive role in adoption, especially in upcoming scenarios, like the Metaverse [3], where passwords and traditional biometrics become unpractical [4]. Another benefit for pervasive systems is the possibility of having hands-free authentication, which can be specially useful in cases were face recognition is not viable (e.g., workers wearing masks, no camera available, poor lightning conditions).

Brainwaves are a promising biometric: they sport high distinguishability, are difficult to steal (non-observable), and provide intrinsic support for liveness detection [7]. However, while research around brainwave-based recognition has experienced great interest, the lack of sufficiently high amounts of data for designing and evaluating these systems has led to the development of solutions that may not be practical to deploy in real-world applications.

Most brainwave-based recognition proposals rely on models that are learned on the entire enrollment database. Such models need to be retrained whenever a new subject is enrolled to maintain performance. As an alternative, training a similarity measure on available databases that then allows for comparing two arbitrary submitted inputs – for instance a known sample of the claimed individual as well as a corresponding proof sample – yields the potential of implementing a general brainwave recognition system with independence of the training and the actual enrollment/verification data. We extend this line of work with the following contributions:

Fig. 1: Virtual Reality devices incorporating Electroemcephalogram (EEG) readers: a) Galea VR headset with EEG sensors from Varjo/OpenBCI [5], b) BESA DSI-VR300 BCI integrated with HTC [6].

- (1) We design and build BrainNet, a brain biometric recognition system based on a Siamese Neural Network (SNN) architecture (Section III) to avoid the need for retraining. We propose the use of a triplet loss function to increase recognition performance.
- (2) We comprehensively evaluate the performance of BrainNet, including seen and unseen attacker models, and reporting a complete set of standard metrics to facilitate comparability [8] (Section IV).
- (3) We release BrainNet's code for reproducing the results and providing a foundation for future research. [1]

II. Background and State of the Art

This section provides a brief overview of brain biometric recognition fundamentals, explains the adversary model for BrainNet, and summarizes state-of-the-art solutions.

[1] BrainNet GitLab repository: https://git.scc.kit.edu/ps-chair/brainnet

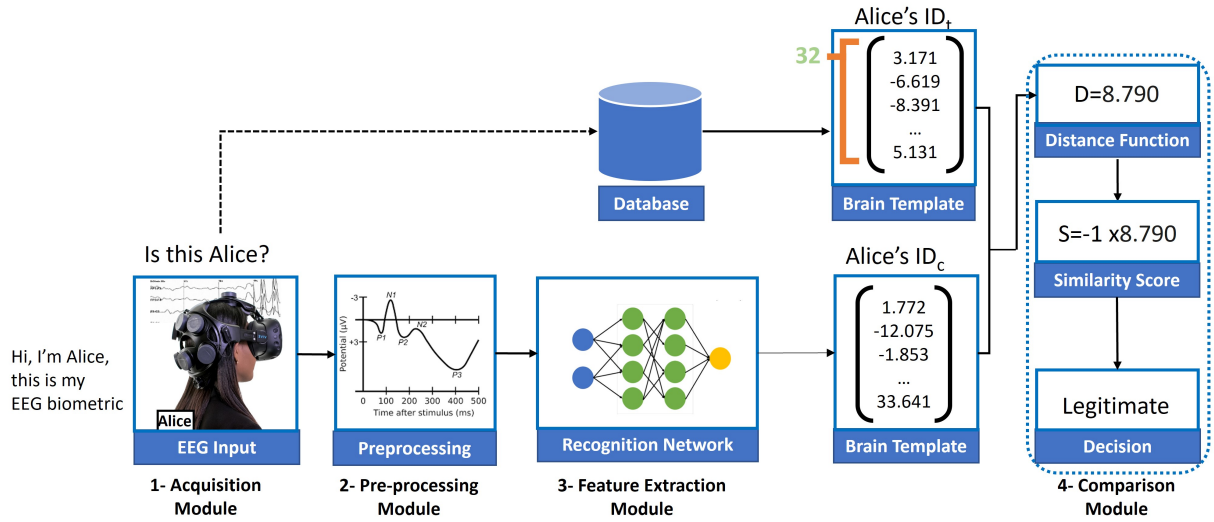


Fig. 2: Brainwave-based recognition system operating in verification mode. Alice's brain activity is acquired with an Electroencephalogram (EEG) wearable, pre-processed, and fed to a Feature Extraction Module that compacts her brain data into a smaller vector with 32 features (brain template). This claimed identity (Alice's IDc) is compared to Alice's registered true identity (Alice's IDt), i.e., her brain template stored during the enrolment phase. The Comparison Module decides is Alice is legitimate or not.

A. *Brainwave-based Biometric Recognition*

Biometric recognition covers both verification and identification [9]. A system in verification mode determines if a person presenting a biometric that was previously registered for an identity is indeed the same person. It is a 1-1 comparison, answering the question *"are you who you say you are?"*. Instead, in identification mode, the goal is to search if the presented biometric is attributable to a single individual in the system database, i.e., determining *"who are you?"* in a 1-N comparison. The typical use-case for verification is user authentication, where you ensure that the person accessing an application or service is a legitimate user and not a fraudster with an stolen identity. Identification is often used in border control use-cases, e.g., running someone's fingerprint against a database to see if it matches against a previously captured print. Identification can be closed-set, if it is known *a priori* that the user is in the database, or open-set otherwise, this latter case being a harder problem.

Independently of the biometric trait, be it a face, fingerprint, or brain data, recognition systems have common blocks to: 1) **acquire** user's data through sensors, 2) **pre-process** these data to improve their quality, 3) **extract** biometric features, and 4) **compare** those features to stored biometric templates. This general architecture is depicted in Figure 2.

The specific case of brainwave-based recognition is characterized by some particularities regarding data acquisition that are relevant for the system design. Brainwaves are captured by electroencephalograph (EEG) sensors while the user is performing a task designed to verify/identify the user. Prior work [7] has investigated the use of EEG data for authentication, either while the subject is resting or performing mental tasks, which can be motor-imaginary, such as thinking of moving a hand, or not, such as thinking about a song. These implementations use the continuous EEG signal sensed through the whole duration of the task, which is complex to de-noise and process. An alternative acquisition paradigm is to expose the user to chosen stimuli (visual, auditive), and measure the consequential time-locked brain reactions, called Event-Related Potentials (ERPs). Since ERPs demonstrated higher signal-to-noise ratio and therefore improved accuracy, as well as the possibility of being revoked by changing the stimuli [10] in brainwave-based verification systems, we use this type of signals in the design of BrainNet. In the following, we clarify our adversary model and explain the state of the art on algorithms for brainwave-based recognition, highlighting the existing limitations that justify our design beyond data acquisition.

B. *Adversary Model*

We consider a brainwave-based recognition system that protects access to applications in a desktop or laptop computer. For verification, the user must complete an *enrollment phase*, where their brain signals are collected and stored as a template associated to the user identity (e.g., a username). Then, during the *verification*, a user supplies their identity and brain data recording, which is compacted into a brain template and compared to the enrolment template to decide whether denying or granting access. Therefore, for each user with true identity ID_t and claimed identity ID_c, we test the hypotheses:

$$H_0 : ID_t = ID_c \quad vs. \quad H_1 : ID_t \neq ID_c \tag{1}$$

to decide if the user is genuine or not (accept/reject H_0). In this scenario, we consider a passive "zero effort" adversary [11], who presents their own biometric characteristic to the system in an attempt to impersonate a legitimate user. In verification,

this is accomplished by claiming the identity of the target victim and presenting it to the system as their own. Furthermore, we further subdivide adversaries into unseen attackers, whose brain data have not been seen by the recognition network during training, and seen attackers, otherwise [12], [13].

We also consider an identification scenario, where the user is identified as a previously enrolled user just by providing their brain data. The same type of zero effort attacker is considered: the adversary tries to be identified as another user in the system database by presenting their own brain data.

The main metrics to measure performance against zero effort attackers are the False Acceptance Rate (FAR) and the False Rejection Rates (FRR).

C. Related Work

Most of the methods in brain biometric recognition can be classified as similarity-based or supervised learning-based recognition systems [7]. Additionally, some recent works use representation learning as an initial step before applying the above methods. In the following, we introduce these categories, highlighting the best performing approaches to which we compare (see summary in Table II). For a more comprehensive and detailed state of the art, we refer the reader to Gui et al.'s survey [7], which covers 188 works in the field of brain biometrics.

Similarity-based methods measure the distance between raw brain signals or between selected features (e.g., power spectral density) to make a decision if brainwaves belong to the same person [14]–[16]. The advantages of these approaches are that they are simple to understand and that they do not require training a model involving other users in order to make a decision, as we will see in the case of supervised-learning approaches. However, designing similarity measures has demonstrated to be difficult due to the noisy and high dimensional nature of EEG signals [7]. One of the relevant works in this area reporting best performance is that of Das et al. [15], where they obtained an Equal Error Rate (EER) of 10% by applying a cosine similarity measure on raw ERP signals. To acquire these signals, subjects were asked to focus on circles between different shapes, or to concentrate on digits within a sequence of alphabet elements and digits.

In **supervised learning** approaches to brain biometric recognition, different machine learning methods have been employed to classify users [17]–[22]. Their operation consists of extracting a series of features from the brain data and use them to train a prediction model. While the performance improves in terms of accuracy with regard to similarity-based solutions, these approaches require retraining the model or training a new model every time a new user is added to the system, which is impractical. Following the supervised learning approach, Yu et al. [17] proposed a Convolutional Neural Network (CNN). They employed a soft voting scheme to fuse the predictions of the CNN on multiple samples and improve the results. They achieved a Half Total Error Rate (HTER=(FAR+FRR)/2) of 1.6%.

Recently, a number of proposals [23]–[26] have used **representation learning** to learn an embedding of the brain data and then apply either a similarity-based measure or a supervised classification method on these representations. This improves manual feature selection and yields better accuracy. In this direction, Schons et al. [23] trained a CNN to learn users' brain representations based on 12-second samples taken while resting. Applying euclidean distance, they achieve a 0.19 % EER for biometric verification. Similarly, Bidgoly et al. [24] use 5-second resting samples and combine a CNN with a cosine distance comparison, to attain a 1.96 EER. While the performance is worse than Schons et al.'s CNN, the evaluation was conducted in a more realistic attack scenario, assuming attackers that have not been seen by the model during training. Nonetheless, the main handicap in using deep learning techniques to learn brain representations is that they require big amounts of data for training and are not yet fully applicable due to the typically small size of brainwave datasets [27].

A promising approach to overcome the necessity of large datasets is the use of Siamese Networks (SNs). SNs are a type of Neural Network architecture for one-shot learning [28], which enable predictions after training with just a few samples, having been widely and successfully applied in face recognition [29]. In the brainwave-based recognition realm, Maiorana's work [26] takes advantage of the Siamese Network architecture to learn brain data representations and fed them to a Support Vector Machine classifier that outcomes predictions. Trained with multi-session samples of 5-second brain data for resting users, they achieve a 4.8% EER, being a good performance considering brain data variations across sessions.

BrainNet Novelty. While promising, no further works beyond [26] have explored the use of Siamese Networks for brainwave-based recognition. We aim at improving this line of work on three fronts. First, drawing from results in face recognition, we hypothesize that training a SN with a triplet-loss function (§ Section III-A) will improve the recognition performance. Second, we hypothesize that using ERPs as input can improve accuracy with respect to continuous EEG data. Finally, the third challenge we aim at addressing comes from looking at the state of the art regarding evaluation practices. None of the related works provide a full report of performance metrics as recommended to allow for comprehension and comparability [8]. They cover mostly verification but not identification, and the evaluation is in many cases performed with attackers that have been previously seen by the system and therefore easier to recognize, or without cross-validation, biasing the performance towards optimistic results. Additionally, the implementation of these solutions is not open-sourced, which would facilitate reproducibility. To counter these limitations, we perform a comprehensive evaluation and reporting, and make the BrainNet model implementation and benchmark publicly available.

III. BrainNet System Design

In this section we explain the design of BrainNet. We start with preliminaries on the SN approach, then delve on the different architectural modules depicted in Figure 2

A. Using Siamese Networks for Biometric Recognition

A Siamese Network is a class of neural networks that contains one or more identical sub-networks connected in parallel. Each parallel NN branch is designed to produce an embedding, which is a vector containing a reduced dimensional representation of the input. The parallel architecture is used to find the similarity of the inputs by comparing its feature vectors. In recent years, Siamese Networks have become popular due to their ability to learn from small amounts of data, being face recognition one of their most well-known applications.

Learning in SNs can be trained using different loss functions [30], with the *triplet loss* approach being specially suitable for biometric recognition. FaceNet, a face recognition pipeline proposed in 2015 by Google researchers [29], introduced the use of triplet loss for this purpose. The training process consists of providing three types of inputs: an *anchor*, a *positive* sample (subject with same identity of the anchor) , and a *negative* sample (subject with a different identity than the anchor). After this process, the embeddings for faces of the same person will have small distances and those of faces of distinct people will have large distances. Therefore, once the embeddings are produced, a similarity metric (tipically Euclidean distance) can be used for verification/identification.

Based on FaceNet, the general idea for BrainNet is using a SN with triplet loss to embed the high dimensional and noisy brainwave samples into a latent space so that samples from the same subject are at low distance, and samples from different subjects at high distance.

B. Data Acquisition

We use two publicly available brainwave datasets collected with medical-grade EEG reading devices, and containing time-locked brain reactions to stimuli: the subjects' ERPs. This fulfills our ERP input requirement and our goal to make our solution reproducible and comparable. These datasets were the best option from the few open alternatives in terms of data quality and number of subjects. We describe them below:

Dataset 1: ERP CORE [31]. The ERP CORE (Compendium of Open Resources and Experiments), published in 2021, includes brain recordings of 40 subjects while exposed to 6 different types of stimuli that generate specific ERP reactions. We focus on two types of ERPs, so called P300 and N400 [32], which are most commonly used in brainwave verification [33]. The P300 and N400 reactions were obtained while users look at visual and textual stimuli, respectively, and contain 1345 and 2268 samples. Brainwaves were collected with a 30-electrode EEG headset at a frequency of 1024 Hz. We therefore consider two sub-datasets and refer to them as P300:ERP CORE and N400:ERP CORE

Dataset 2: Brain Invaders (bi2015a) [34]. This dataset contains P300 brain reactions of 41 subjects while playing a video game called "Brain Invaders" (visual stimuli). The data was collected using a cap with 32 EEG sensors at 512 Hz. We ignored the last subject in bi2015a in order to have the same number of subjects in both datasets. The total number of samples for these 40 subjects is 10614. We refer to this dataset as P300:bi2015.

C. Pre-processing

In the pre-processing flow, we follow best practices in ERP treatment to extract P300/N400 sections [7], [35] by cutting the signal 0.2 seconds before stimulus presentation and ending at 0.8 seconds after the event. The time before the event (baseline) was used to reduce the drifting effect by subtracting the mean baseline period from all time points of an sample for each channel[2]. Finally, the samples were organized as a 2D array, in which each row belongs to an electrode data or channel, and each column represents a single measurement point in time. This makes an appropriate input for our convolutional neural network branches in the subsequent feature extraction module.

D. Feature Extraction: the Siamese Network

BrainNet's core is the Extraction Module, for which we use a Siamese Neural Network with three CNN branches, trained with a triplet loss function. The general idea, as anticipated in Section III-A is to tune the network to output brain data representations or *embeddings* such that samples of the same subject remain close, but even similar samples from a different subject are distinguished correctly. The triplet loss function L is formulated as the Euclidean distance:

$$L(A,P,N) = max(\|(f(A)-f(P)\|^2-\|(f(A)-f(N)\|^2+\alpha,0) \tag{2}$$

where f is an embedding, A is an anchor input, P is a positive input (brain sample for the same subject as A), and N is a negative input of a different subject. The parameter α is a margin to be enforced between positive and negative pairs. It defines the minimum level of dissimilarity acceptable for the loss function, aiding in the better differentiation of samples. Therefore, we seek to minimize:

$$\sum_{n=i}^{N} \|(f(A_i) - f(P_i)\|^2 - \|(f(A_i) - f(N_i)\|^2 + \alpha \tag{3}$$

where the indices i refer to the individual triplet inputs used in training. Triplet selection is based on the strategy proposed in FaceNet to facilitate quick convergence in learning [29]. Training with the triplet loss function establishes the weights and parameters of the CNN used in the siamese sub-networks, so it can later be used to output brain vector templates for verification/identification. For these CNNs, we required an architecture that would reduce the high dimensionality of brainwaves (number of electrodes $\times$ sample rate $\times$ time) to a smaller space, while preserving the characteristics of

[2]A channel is a recording from a specific EEG electrode

individual brainwaves. Using fully connected layers would be prohibitively expensive in terms of training hyperparameters. We hence designed our system using a CNN with 5 convolution layers, as depicted in Figure 3. The network architecture was kept the same for both datasets but we added an average pooling layer before the first convolution layer to downsample the ERP CORE dataset, which was collected at 1024Hz vs the 512 Hz of the bi2015a dataset.

E. Comparison in Verification Mode

Once brain templates can be represented in a vectorial form as the output of the CNN network, verification entails a comparison of the user claimed template with the previously enrolled one. Our Comparison Module uses the euclidean distance metric and we implement three measurement strategies to evaluate the system performance:

- **Fixed Threshold-One Sample (S1)**. This approach consists of comparing the claimed verification sample with just one enrollment sample of the subject. The idea is to test how well the system performs if we decide to have a light and quick enrollment process.
- **Fixed Threshold-Best Match (S2)**. When several enrollment samples per subject are available, they can be used in verification to improve performance. In this approach, the best match between the verification sample and all enrollment samples is picked for decision making.
- **Tailored Threshold (S3).** Same approach as S2, but selecting configuration thresholds tailored to each individual. We expect improved performance at the cost of an increased number of enrollment samples needed to determine a reliable threshold for subjects.

F. Comparison in Identification Mode

The Comparison Module operates in closed and open-set identification. In the first case, it calculates the euclidean distance between the identification sample and all enrollment samples, sorts the results by similarity, and chooses the first sample and associated subject ID. We use the same approach to simulate the open-set scenario, but removing the subject that is trying to be identified from the enrollment database. If the similarity score for the best match sample is above the decision threshold, this subject ID is output, otherwise the system determines that the user is not in the database.

IV. Results and discussion

This section introduces the testbed settings and shows the results for different comparison strategies and attacker models.

A. Testbed and Evaluation Metrics

The subjects used for training the Siamese Network should differ from those used for evaluating the recognition system to ensure that the system will continue to function effectively without retraining as new subjects enroll in the system. Accordingly, we used group 8-fold cross-validation, grouping the datasets by subject ID and using 35 subjects for training and 5 unseen subjects for testing. This process was repeated in 8 rounds of cross-validation, using the Leave-One-Out Cross-Validation (LOOCV) approach. To evaluate performance under seen-attacker scenarios, we used an 8-fold stratified cross-validation strategy to split training and evaluation data, using 40 subjects for training, and testing it also with 40 subjects.

TABLE I: BrainNet's verification performance under unseen and seen attacker adversary models. Average Equal Error Rate (EER) and FRR at FAR=1% for three different comparison strategies on three brainwave datasets.

		EER (%)		FRR at 1%(%)	
Dataset	Strategy	Unseen	Seen	Unseen	Seen
P300:ERP CORE	S1	9.39	4.0	30.77	14.46
	S2	2.31	2.31	6.44	8.56
	S3	2.01	0.48	5.36	0.31
N400:ERP CORE	S1	8.97	1.79	25.23	2.79
	S2	1.96	0.75	3.76	0.66
	S3	1.37	0.62	2.67	1.13
P300:bi2015a	S1	3.34	0.55	9.96	0.25
	S2	0.17	0.18	0.15	0.04
	S3	0.14	0.008	0.21	0.00

To measure performance, we use the standard metrics for zero effort attacker testing, FAR and FRR. For completeness, we also provide the Equal Error Rate (EER) as a summary metric, which is the point at which both FAR and FRR are equal and minimum. Then, we report the FRR at FAR=1%, a common evaluation point to understand how usable is the system in terms of rejecting legit users when meeting minimum security requirements [36]. Finally, we use DET curves (Detection-Error Tradeoff) to show the operation range when varying the decision thresholds in the Comparison Module. We show FRRs with FAR moving in the range of 0.01% to 5%, providing additional insights into how the system could be configured.

B. Biometric Verification Results

Results are summarized in Table I for unseen and seen attackers, respectively. Table I displays two notable trends in the verification results. First, results show steady improvements from comparison strategy S1 to S3. For instance, using the P300 brain reactions in the ERP CORE dataset, the system achieves a 9.39 % EER for the Fixed Threshold-One Sample strategy S1, 2.31 % when using more enrollment samples in the S2 strategy, and 2.01 % for the the tailored thresholding in S3, indicating a 78 % improvement. Additionally, the N400 brain reactions from the ERP CORE and the bi2015a dataset with P300 ERPs, respectively, demonstrate an 84% and 95% improvement. Secondly, the results improve from the first to the third dataset, and we believe that this is primarily due to an increase in the number of samples that are available per subject in each task; for example, the best performance of each dataset, 2.01%, 1.37%, and 0.14% EER, correspond to 1345, 2268, and 10614 samples.

Figure 4 (d,e,f) illustrates how FRR changes when the FAR varies between 0.01%, as a strict security policy, to 5%, as a generous policy that provides maximum usability for legitimate users. We did not begin at zero, as this predictably

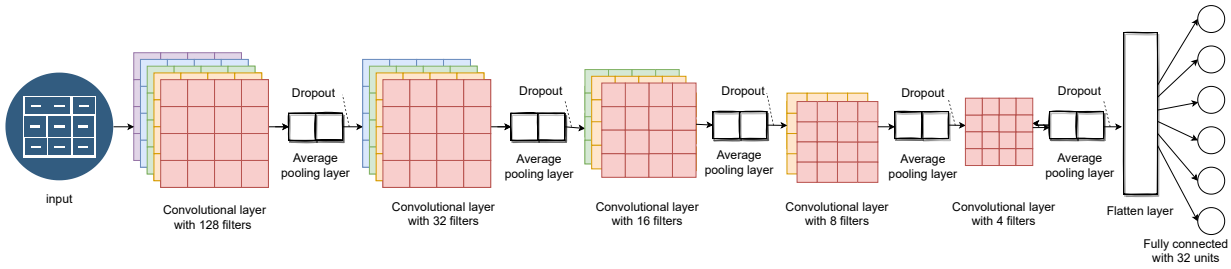
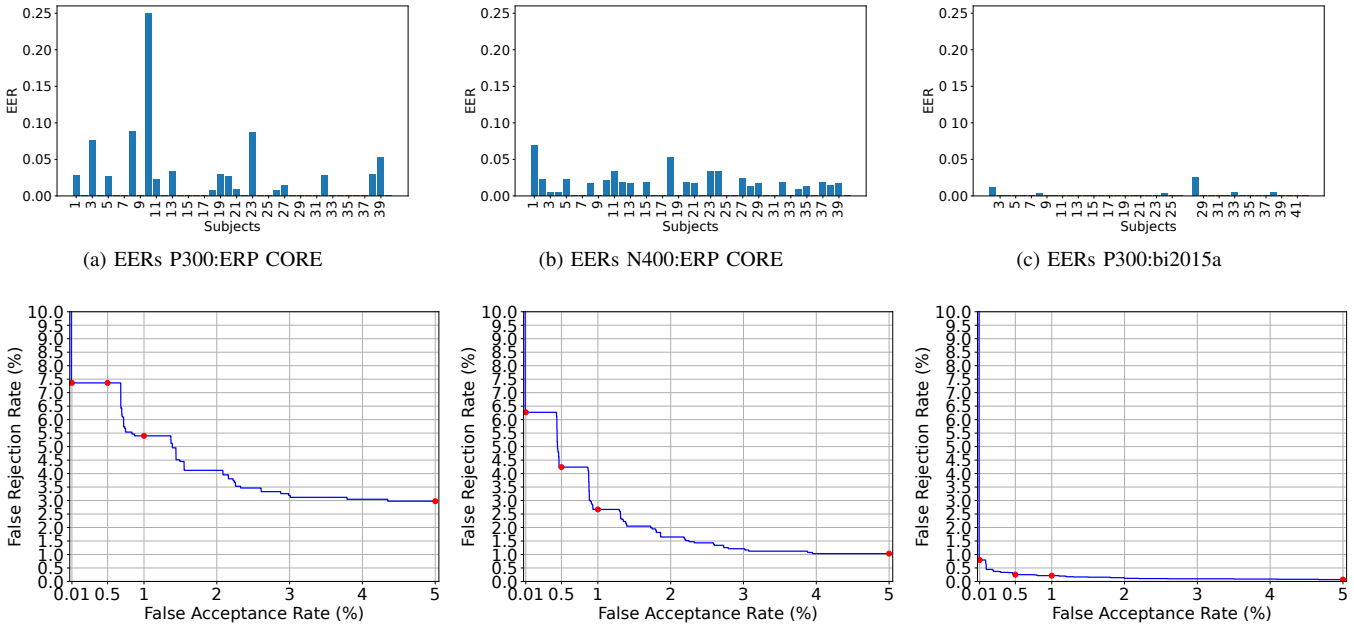


Fig. 3: Architecture of the Convolutional Neural Network used in the BrainNet's Siamese Network to compute a latent representation of brain data samples (input) in a compact 32-bit embedding (output)



(a) EERs P300:ERP CORE (b) EERs N400:ERP CORE (c) EERs P300:bi2015a

(d) DET P300:ERP CORE (e) DET N400:ERP CORE (f) DET P300:bi2015a

Fig. 4: Up: EER per subject for BrainNet's verification on three brainwave datasets using a tailored threshold per subject as comparison strategy. Bottom: average Detection Error Tradeoff (DET) curves.

yields a prohibitively high FRR.We consider the reported FRR at 1% as the baseline. Hence, a FAR equal to 0.5% provides two times higher security, and when equal to 0.01%, it provides 100 times higher security. The DET plots represent an average of 40 subjects; therefore, they do not behave exactly like a single DET. In spite of this, all three plots exhibit a similar trend. Based on the DET, we can have 100 times more security by spending less than three times the FRR. However, we cannot improve usability at that rate by charging more FAR. We suspect that there are noisy samples in the dataset. Therefore, we have to significantly decrease the threshold to include a few of them as accepted samples and improve FRR, but at the expense of including more attacker samples in the authenticated set and compromising system security.

Finally, we plotted EERs per subject for the tailored threshold strategy. Since we did cross-validation, we gathered the results of the test set on all rounds in this plot. As it can be seen in Figure 4, the model provides the optimal (0%) result for the majority of subjects, which reinforces our previous guess about the possibility of some noisy samples that are very far from legitimate subject samples. For instance, 34 out of 40 subjects in the P300:bi2015 dataset in Figure 4 yield 0% EER, which shows that BrainNet can compare unseen samples perfectly on the majority of the subjects. In other words, by neglecting subject 28, the average EER would be 0.08% rather than 0.14%. This performance, evaluated with different test-train subject sets, shows that BrainNet can authenticate subjects without retraining the weights for each new enrollment.

C. Biometric Identification Results

Table III shows BrainNet's performance in identification mode, under closed-set and open-set scenarios. For closed-set identification, BrainNet achieves an accuracy of 95.63%, 99.39%, and 99.92% for the three brain datasets. As expected, the performance of the open-set scenario is significantly lower. It amounts to 95.06%, 96.78%, and 99.76% accuracy.

TABLE II: Summary of state-of-the-art brain biometric verification s olutions, o rdered b y t ype o f a pproach: S imilarity D istance ([SD]), Supervised Learning ([SL]), and Representation Learning ([RL]). Solutions are compared regarding Equal Error Rates (EER), brain data acquisition, attacker model, and whether they were evaluated through multiple sessions (Sess.>1) and using cross-validation (Cross-V.)

Brain Biometric Verification Solutions						
Publication	Acquisition	Attacker	Sess.>1	[Approach]- Feature Extraction, Comparison	EER (%)	Cross-V.
Das *et al.* [15], 2016	Stimuli Reaction (ERP)	unseen	✓	[SD]-Manual, Cosine Dist.	10	✓
Schons *et al.* [23], 2017	Resting EEG	seen	×	[SL]-CNN, Euclidean Dist.	0.19	×
Bidgoly *et al.* [24], 2022	Resting EEG	unseen	×	[SL]-CNN, Cosine Dist.	1.96	×
Maiorana [26], 2021	Resting EEG	unseen	✓	[RL]-Siamese Net. (twin), SVM	4.8	✓
Our work: BrainNet	Stimuli-Reaction (ERP)	unseen	×	[RL]-Siamese Net. (triplet), Euclidean Dist.	0.14	✓

TABLE III: BrainNet's performance for identification.

	Identification Scenario	
Dataset	closed-set Accuracy (%)	open-set EER (%)
P300:ERP CORE	95.63	4.94
N400:ERP CORE	99.39	3.22
P300:bi2015a	99.92	0.34

D. Comparison with other works

We compare BrainNet with the closest related work in authentication as summarized in Table II, and against the performance of identification solutions in the state of the art.

Authentication: **Das et al.** [15] reported a 10% EER, which shows that using raw data in a similarity-based approach is impractical. Afterward, **Schons et al.** [23] proposed a solution combining supervised learning with Euclidean distance, reporting an excellent EER of 0.19%. However, the evaluation was only conducted under a seen-attacker adversary model, which is unrealistic. This evaluation approach includes all subjects during the training phase; so the system's accuracy is unknown when a subject outside of the training study is requested and the performance would worsen significantly. This argument is supported by the drastic increase in the EER from the unseen attacker scenario in Table II. Indeed, following a similar approach, but evaluating the system under am unseen adversary, **Bidgoly et al.'s solution** [37] yields an increased EER. Their results, with a 1.96% EER, are the closest to our work. BrainNet achieves 2.01%, 1.37%, and 0.14% EER in different datasets. While our best result is 92.8% better, our worst result is still comparable. This shows that the quality of the EEG data can significantly affect the final results. It is to note that Bidgoly et al.'s approach can be biased to over-optimistic results due to the lack of cross-validation. In our study, we observed multiple rounds of cross-validation with 0% EER or significantly lower than average. Additionally, using Siamese Networks removes the need for retraining the system, which provides and extra benefit in terms of efficiency. The only other work using Siamese Networks was conducted by **Maiorana's** [26]. This solution provides an EER of 4.8%. Though worse than BrainNet, it was evaluated using data from multiple sessions. For a fair comparison, it would remain to be explored whether our performance degrades when evaluated in the same conditions. Finally, using ERPs instead of a resting task, as it is common in the state of the art, provides potential for implementing revocability for users [10], which is an important advantage of BrainNet.

Identification: Several papers [24], [38] have reported close to 100% accuracy for closed-set identification with brain biometrics. However, as far as we know, only Panzino et al. [39] and BrainNet consider the open-set scenario. While our results seem to be better, their testing sets were larger; therefore, performance comparison would be unfair in this case. We however highlight that our identification system does not need to retrain when adding new subjects to the enrollment set. In contrast, Panzino et al. [39], and Wang et al. [40] have to retrain their network when registering new users.

V. Research limitations

This study has three major limitations due to the lack of publicly available brainwave datasets, which could be addressed in future research. First, the datasets were based on single-session ERP data, which made the problem less difficult to solve. Seha et al. [41] showed that moving from a single session to a multi-session can triple EER in the worst-case scenario. To fully investigate this issue, we are seeking to collect multi-session ERP-based datasets. Second, we used high-quality datasets collected with medical-grade EEG sensors rather than with consumer-grade BCIs. Consumer-grade datasets will have a smaller number of channels and a lower quality of data recording, which may affect the overall performance, but would help better in understanding applicability to real-world pervasive computing scenarios. Third, since there are only 40 subjects per task, we are restricted from evaluating our solution with this limited number of subjects. Despite using cross-validation to mitigate the issue, larger datasets are necessary to investigate practical application.

VI. Conclusion

Using triplet loss Siamese Networks, we have developed a similarity-based recognition system to verify and identify users by their brain activity. Trained as a one-shot classifier, our system successfully incorporates new subjects without retraining or explicit enrollment. Using event-related potentials, it achieves an EER of 0.14% for verification and 0.34% EER when extended to biometric open-set identification, in both cases evaluating the systems with unseen attackers. Our investigations indicate that this approach is successful even when trained with only a limited number of inputs and greatly benefits from additional samples. We also observe that noisy samples negatively affect the results of verification. We hence suggest to investigate prior filtering as potential future work.

ACKNOWLEDGMENTS

This work was funded by the Helmholtz Association (HGF) within topic "46.23 Engineering Secure Systems" (KASTEL Security Research Labs) and Germany's Excellence Strategy (EXC 2050/1 'CeTI'; ID 390696704).

REFERENCES

[1] S. Pathirana, D. Asirvatham, and G. Johar, "A critical evaluation on low-cost consumer-grade electroencephalographic devices," in *2018 2nd International Conference on BioSignal Analysis, Processing and Systems (ICBAPS)*. IEEE, 2018, pp. 160–165.

[2] G. A. M. Vasiljevic and L. C. de Miranda, "Brain–computer interface games based on consumer-grade eeg devices: A systematic literature review," *International Journal of Human–Computer Interaction*, vol. 36, no. 2, pp. 105–142, 2020.

[3] H. Guo and W. Gao, "Metaverse-powered experiential situational english-teaching design: An emotion-based analysis method." *Frontiers in Psychology*, vol. 13, pp. 859 159–859 159, 2022.

[4] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain," *IEEE Access*, 2022.

[5] Galea: Bringing next generation neurotechnology to mixed reality. [Online]. Available: https://galea.co

[6] Varjo and OpenBCI partner to bring neurotechnology to spatial computing. [Online]. Available: https://varjo.com/company-news/openbci-and-varjo-partner-to-bring-neurotechnology-to-spatial-computing/

[7] Q. Gui, M. V. Ruiz-Blondet, S. Laszlo, and Z. Jin, "A survey on brain biometrics," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–38, 2019.

[8] S. Sugrim, C. Liu, M. McLean, and J. Lindqvist, "Robust performance metrics for authentication systems," in *Network and Distributed Systems Security (NDSS) Symposium 2019*, 2019.

[9] "Information technology — Vocabulary — Part 37: Biometrics," International Organization for Standardization and International Electrotechnical Commission, Standard, Mar. 2022.

[10] F. Lin, K. W. Cho, C. Song, W. Xu, and Z. Jin, "Brain password: A secure and truly cancelable brain biometrics for smart headwear," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, 2018, pp. 296–309.

[11] A. J. Mansfield and J. L. Wayman, "Best practices in testing and reporting performance of biometric devices," 2002.

[12] Q. Wu, Y. Zeng, C. Zhang, L. Tong, and B. Yan, "An eeg-based person authentication system with open-set capability combining eye blinking signals," *Sensors*, vol. 18, no. 2, p. 335, 2018.

[13] H. Dao, D.-H. Nguyen, and M.-T. Tran, "Face recognition in the wild for secure authentication with open set approach," in *Int. Conference on Future Data and Security Engineering*. Springer, 2021, pp. 338–355.

[14] I. Nakanishi and M. Hattori, "Biometric potential of brain waves evoked by invisible visual stimulation," in *International Conference on Biometrics and Kansei Engineering (ICBAKE)*. IEEE, 2017, pp. 94–99.

[15] R. Das, E. Maiorana, and P. Campisi, "Eeg biometrics using visual stimuli: A longitudinal study," *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 341–345, 2016.

[16] S. Barra, A. Casanova, M. Fraschini, and M. Nappi, "Eeg/ecg signal fusion aimed at biometric recognition," in *International conference on image analysis and processing*. Springer, 2015, pp. 35–42.

[17] T. Yu, C.-S. Wei, K.-J. Chiang, M. Nakanishi, and T.-P. Jung, "Eeg-based user authentication using a convolutional neural network," in *2019 9th International IEEE/EMBS Conference on Neural Engineering (NER)*. IEEE, 2019, pp. 1011–1014.

[18] S. Puengdang, S. Tuarob, T. Sattabongkot, and B. Sakboonyarat, "Eeg-based person authentication method using deep learning with visual stimulation," in *2019 11th International Conference on Knowledge and Smart Technology (KST)*. IEEE, 2019, pp. 6–10.

[19] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new multi-level approach to eeg based human authentication using eye blinking," *Pattern Recognition Letters*, vol. 82, pp. 216–225, 2016.

[20] G. Safont, A. Salazar, A. Soriano, and L. Vergara, "Combination of multiple detectors for eeg based biometric identification/authentication," in *2012 IEEE international carnahan conference on security technology (ICCST)*. IEEE, 2012, pp. 230–236.

[21] T. Xu, H. Wang, G. Lu, F. Wan, M. Deng, P. Qi, A. Bezerianos, C. Guan, and Y. Sun, "E-key: an eeg-based biometric authentication and driving fatigue detection system," *IEEE Trans. on Affective Computing*, 2021.

[22] Y. Sun, F. P.-W. Lo, and B. Lo, "Eeg-based user identification system using 1d-convolutional long short-term memory neural networks," *Expert Systems with Applications*, vol. 125, pp. 259–267, 2019.

[23] T. Schons, G. J. Moreira, P. H. Silva, V. N. Coelho, and E. J. Luz, "Convolutional network for eeg-based biometric," in *Iberoamerican Congress on Pattern Recognition*. Springer, 2017, pp. 601–608.

[24] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "Towards a universal and privacy preserving eeg-based authentication system," *Scientific Reports*, vol. 12, no. 1, pp. 1–12, 2022.

[25] E. Maiorana, "Eeg-based biometric verification using siamese cnns," in *International Conference on Image Analysis and Processing*. Springer, 2019, pp. 3–11.

[26] E. a. Maiorana, "Learning deep features for task-independent eeg-based biometric verification," *Pattern Recognition Letters*, vol. 143, pp. 122–129, 2021.

[27] F. Lotte, L. Bougrain, A. Cichocki, M. Clerc, M. Congedo, A. Rakotomamonjy, and F. Yger, "A review of classification algorithms for eeg-based brain–computer interfaces: a 10 year update," *Journal of neural engineering*, vol. 15, no. 3, p. 031005, 2018.

[28] G. Koch, R. Zemel, R. Salakhutdinov *et al.*, "Siamese neural networks for one-shot image recognition," in *ICML deep learning workshop*, vol. 2. Lille, 2015, p. 0.

[29] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proc. of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 815–823.

[30] B. Ghojogh, M. Sikaroudi, S. Shafiei, H. R. Tizhoosh, F. Karray, and M. Crowley, "Fisher discriminant triplet and contrastive losses for training siamese networks," in *2020 international joint conference on neural networks (IJCNN)*. IEEE, 2020, pp. 1–7.

[31] E. S. Kappenman, J. L. Farrens, W. Zhang, A. X. Stewart, and S. J. Luck, "Erp core: An open resource for human event-related potential research," *NeuroImage*, vol. 225, p. 117465, 2021.

[32] M. Kutas and K. D. Federmeier, "Thirty years and counting: Finding meaning in the n400 component of the event related brain potential (erp)," *Annual review of psychology*, vol. 62, p. 621, 2011.

[33] P. Arias-Cabarcos, T. Habrich, K. Becker, C. Becker, and T. Strufe, "Inexpensive brainwave authentication: new techniques and insights on user acceptance," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 55–72.

[34] L. Korczowski, M. Cederhout, A. Andreev, G. Cattan, P. L. C. Rodrigues, V. Gautheret, and M. Congedo, "Brain invaders calibration-less p300-based bci with modulation of flash duration dataset (bi2015a)," Ph.D. dissertation, GIPSA-lab, 2019.

[35] S. Sur and V. K. Sinha, "Event-related potential: An overview," *Industrial psychiatry journal*, vol. 18, no. 1, p. 70, 2009.

[36] A. Stoianov and A. Cavoukian, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," *office of the information and Privacy Commissioner of ontario*, 2007.

[37] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "A survey on methods and challenges in eeg based authentication," *Computers & Security*, vol. 93, p. 101788, 2020.

[38] D. La Rocca, P. Campisi, B. Vegso, P. Cserti, G. Kozmann, F. Babiloni, and F. D. V. Fallani, "Human brain distinctiveness based on eeg spectral coherence connectivity," *IEEE transactions on Biomedical Engineering*, vol. 61, no. 9, pp. 2406–2412, 2014.

[39] A. Panzino, G. Orrù, G. L. Marcialis, and F. Roli, "Eeg personal recognition based on 'qualified majority'over signal patches," *IET Biometrics*, vol. 11, no. 1, pp. 63–78, 2022.

[40] M. Wang, H. El-Fiqi, J. Hu, and H. A. Abbass, "Convolutional neural networks using dynamic functional connectivity for eeg-based person identification in diverse human states," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3259–3272, 2019.

[41] S. N. A. Seha and D. Hatzinakos, "A new approach for eeg-based biometric authentication using auditory stimulation," in *2019 International Conference on Biometrics (ICB)*. IEEE, 2019, pp. 1–6.