MindID: Person Identification from Brain Waves through Attention-based Recurrent Neural Network

XIANG ZHANG, University of New South Wales, Australia
LINA YAO, University of New South Wales, Australia
SALIL S. KANHERE, University of New South Wales, Australia
YUNHAO LIU, Tsinghua University, China
TAO GU, RMIT University, Australia
KAIXUAN CHEN, University of New South Wales, Australia

Person identification technology recognizes individuals by exploiting their unique, measurable physiological and behavioral characteristics. However, the state-of-the-art person identification systems have been shown to be vulnerable, e.g., anti-surveillance prosthetic masks can thwart face recognition, contact lenses can trick iris recognition, vocoder can compromise voice identification and fingerprint films can deceive fingerprint sensors. EEG (Electroencephalography)-based identification, which utilizes the user's brainwave signals for identification and offers a more resilient solution, has recently drawn a lot of attention. However, the state-of-the-art systems cannot achieve similar accuracy as the aforementioned methods. We propose MindID, an EEG-based biometric identification approach, with the aim of achieving high accuracy and robust performance. At first, the EEG data patterns are analyzed and the results show that the Delta pattern contains the most distinctive information for user identification. Next, the decomposed Delta signals are fed into an attention-based Encoder-Decoder RNNs (Recurrent Neural Networks) structure which assigns varying attention weights to different EEG channels based on their importance. The discriminative representations learned from the attention-based RNN are used to identify the user through a boosting classifier. The proposed approach is evaluated over 3 datasets (two local and one public). One local dataset (EID-M) is used for performance assessment and the results illustrate that our model achieves an accuracy of **0.982** and significantly outperforms the state-of-the-art and relevant baselines. The second local dataset (EID-S) and a public dataset (EEG-S) are utilized to demonstrate the robustness and adaptability, respectively. The results indicate that the proposed approach has the potential to be widely deployed in practical settings.

CCS Concepts: • **Security and privacy → Biometrics**; • **Computing methodologies → Machine learning algorithms**;

Additional Key Words and Phrases: EEG, biometric identification, EEG pattern decomposition, deep learning, attention mechanism

Authors' addresses: Xiang Zhang, University of New South Wales, CSE, UNSW, Sydney, NSW, 2052, Australia, xiang.zhang3@student.unsw.edu.au; Lina Yao, University of New South Wales, CSE, UNSW, Sydney, NSW, 2052, Australia, lina.yao@unsw.edu.au; Salil S. Kanhere, University of New South Wales, CSE, UNSW, Sydney, NSW, 2052, Australia, salil.kanhere@unsw.edu.au; Yunhao Liu, Tsinghua University, School of Software, Tsinghua University, Beijing, Beijing, 100084, China, yunhao@tsinghua.edu.cn; Tao Gu, RMIT University, Melbourne, VIC, 3001, Australia, tao.gu@rmit.edu.au; Kaixuan Chen, University of New South Wales, CSE, UNSW, Sydney, NSW, 2052, Australia, kaixuan.chen@student.unsw.edu.au.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2018 Association for Computing Machinery.
2474-9567/2018/9-ART149 $15.00
https://doi.org/10.1145/3264959

ACM Reference Format:
Xiang Zhang, Lina Yao, Salil S. Kanhere, Yunhao Liu, Tao Gu, and Kaixuan Chen. 2018. MindID: Person Identification from Brain Waves through Attention-based Recurrent Neural Network. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 149 (September 2018), 23 pages. https://doi.org/10.1145/3264959

1 INTRODUCTION

Over the past decade, biometric information has been widely used in identification and have gained more acceptance due to their reliability and adaptability. Existing biometric identification systems are mainly based on individuals' unique intrinsic physiological features (e.g., face [11], iris [22], retina [32], voice [28], and fingerprint [38]). However, the state-of-the-art person identification systems have been shown to be vulnerable, e.g., anti-surveillance prosthetic masks can thwart face recognition, contact lenses can trick iris recognition, vocoder can compromise voice identification and fingerprint films can deceive fingerprint sensors. In this perspective, the EEG (Electroencephalography) based biometric person identification systems are emerging as promising alternatives due to their high attack-resilience [16, 35]. EEG-based identification systems measure an individual's brain response to a number of stimuli in the form of EEG signals, which record the electromagnetic and invisible electrical neural oscillations. An individual's EEG signals are virtually impossible to mimic for imposter, thus making this approach highly resilient to spoofing attacks encountered by other identification techniques [1].

However, research on EEG-based identification is still in its infancy, and several key challenges exist. One of the most significant issues is the low identification accuracy as a result of the inherent low precision of EEG signals. Accurate identification is challenging because the EEG data has very low signal-to-noise ratio. The state-of-the-art approaches can achieve accuracy in the range of 80% to 95% [4, 16, 21, 37], which is not sufficient for practical deployments, particularly in high security environments. Additionally, the identification algorithms are highly dependent on the environment in which the EEG signals were collected and thus not robust and adaptable to a broader range of scenarios. Changes in the application environment (e.g., the number of channels, the sampling rate, and the training data size) may lead to the decrease of accuracy[2]. Thus, an EEG-based identification model that may work well under one kind of application environment (e.g., 64 channels and 160 Hz), may not achieve good performance in another application environment (e.g., 14 channels and 128 Hz). So far, we have not seen a universal EEG-based identification algorithm which can perform well in a variety of real environments.

To address the aforementioned problems, we propose MindID, a Delta pattern EEG-based person identification algorithm which is based on an attention-based recurrent neural network. At first, to eliminate the interference of the slight shift brought by the environmental noise and the physical and mental state of the individuals, we attempt to learn the robust and reliable representation by decomposing the EEG patterns. For this, we decompose the full spectrum of EEG data into specific patterns (Delta, Theta, Alpha, Beta, and Gamma). Decomposed EEG patterns (e.g., Theta, Alpha, Beta, and Gamma), have been employed for EEG signal classification (e.g., movement task classification [27]) in some works. However, there is few existing work that has focused on the Delta pattern. In this paper, we discover that the Delta pattern is the most discriminative and efficient pattern through our analysis in Section 3. Moreover, we introduce the attention-based RNNs (Recurrent Neural Networks) [2] which can automatically detect the most distinguishable information from the input EEG data. More importantly, the attention mechanism[3] automatically re-allocates the weights to extract most discriminative features that are

[1]For example, people can easily trick a fingerprint-based identification system by using a fake fingerprint film (*http://www.instructables.com/id/How-To-Fool-a-Fingerprint-Security-System-As-Easy-/*) or a face-recognition-based identification system by simply wearing a 200 dollars' worth anti-surveillance mask (*http://www.urmesurveillance.com/urme-prosthetic/*)
[2]This statement can be demonstrated in Section 5.7.
[3]Simply, attention mechanism refers to select the most pertinent piece of information rather than using all available information. Attention Mechanisms in Neural Networks are based on the visual attention mechanism found in humans, and has been applied in computer version, NLP areas.

resilient to the change in environmental factors. Therefore, the proposed approach is robust under different collection environments with changes to the EEG collection hardware, sampling rate, and channel numbers. The efficiency of attention-based RNN framework has been demonstrated by the studies in speech recognition [2, 5], NLP (Natural Language Processing) [1, 23, 39], and computer version [25].

Our main contributions in this paper are highlighted as follows:

- We present an EEG-based identification approach, MindID, which adopts a novel attention-based Encoder-Decoder RNN framework for learning discriminative features among the user's brainwaves and utilizes the learned features to identify user identity through a boosting classifier. The attention mechanism enables our approach to automatically search the most discriminative features for identification, and consequently achieve robust and adaptive operation over different datasets collected from environments with varying characteristics.
- We analyze the EEG pattern decomposition and propose that the Delta pattern is the most steady and distinguishable pattern for user identification. Moreover, we design and conduct a set of experiments to verify the proposed hypothesis.
- We design and conduct an experiment setting for collecting EEG data and use it to collect two two real-world local datasets (EID-M and EID-S) which are under single and multi trial settings, respectively[4].
- We evaluate the proposed approach on 3 datasets (2 local and 1 public). The results illustrate that our model achieves an accuracy of **0.982** which significantly outperforms the state-of-the-art and baselines. We demonstrate the robustness and adaptability by the comparison between 3 datasets.

Note that all the necessary reusable codes and datasets in this paper have been open-sourced for reproduction, please refer to this link [5].

The remainder of this paper is organized as follows. Section 2 introduces the literature related to this paper. Section 3 analyzes the characteristics of EEG patterns. Section 4 details the methodology of the MindID identification system. Section 5 evaluates the proposed approach on the local and public dataset and provides analysis of the experimental results. Section 6 discussed the limitation of our work and the future research potentials. Finally, Section 7 summarizes this paper and gives the conclusion.

2 RELATED WORK

In this section, we separately present literature on three aspects: EEG-based person identification models, EEG pattern decomposition, and applications of attention-based RNN.

2.1 EEG-based Person Identification

Since EEG can be gathered in a safe and non-intrusive way, researchers have paid great attention to exploring this kind of brain signals. For person identification, EEG is promising for being confidential and attack-resilient but on the other hand, complex and hard to be analyzed [37]. Jayarathne et al. [15] decompose the EEG data and pay attentions on the Alpha and Beta wave. The Common Spatial Patterns (CSP) values were extracted as main features to train the Linear discriminant analysis (LDA) classifier which achieves accuracy of 96.97% for a 12 participants dataset. Thomas and Vinod [37] take advantage of individual alpha frequency (IAF) and delta band signals to compose specific feature vectors. They also prefer PSD features but only perform the extraction merely on gamma band. However, all of the above approaches only work in one specific environment. Few studies attempt to build a universal EEG-based identification model.

[4]Single trial refers to that the dataset is collected in one session (the period from one subject putting the EEG headset on until all the experiment are finished then putting off). Multi-trials represents the EEG data is collected from different trials, which considered the effect on EEG data quality caused by the headset position errors.

[5]https://drive.google.com/open?id=1t6tL434ZOESb06ZvA4Bw1p9chzxzbRbj

Table 1. EEG patterns and corresponding characters. Awareness Degree denotes the awareness the degree of being aware of an external world.

Patterns	Frequency (*Hz*)	Amplitude	Brain State	Awareness Degree	Produced Location
Delta	0.5-4	Higher	Deep sleep pattern	Lower	Frontally and posteriorly
Theta	4-8	High	Light sleep pattern	Low	Entorhinal cortex, hippocampus
Alpha	8-12	Medium	Closing the eyes, relax state	Medium	Posterior regions of head
Beta	12-30	Low	Active thinking, focus, high alert, anxious	High	Most evident frontally
Gamma	30-100	Lower	During cross-modal sensory processing	Higher	Somatosensory cortex

2.2 EEG Pattern Decomposition

Generally, the EEG data could be decomposed into several patterns (delta, theta, alpha, beta, and gamma) corresponding to various brain states [24]. So far, the majority of user ID identification studies have focused on features generated from the Alpha and Beta patterns.[21, 35]. Moreover, these works assume that the EEG data is collected from the most favorable settings, i.e., when the subject is resting/relaxed for Alpha waves or concentrating for Beta waves. The rest and relax states are represented by the Alpha wave, therefore, a number of studies decompose EEG raw signals into the Alpha pattern for future analysis. Bashar et al. [4] use the filtered signals with frequency ranges from $0.5 - 59Hz$ (including Delta, Theta, Alpha, Beta and part of Gamma patterns) and calculate the statistics for user ID classification. Kumari and Vaish [21] employ wavelet analysis to decompose original EEG signals into 5 patterns (Delta to Gamma) and extract statistical measures of each pattern. Thomas and Vinod [37] take Alpha peak frequency and peak power and Delta band power as recognition features and achieves the highest recognition rate as 0.9. To our best knowledge, this paper is the very first work which specially focused on the decomposition and analysis of Delta pattern and studies the person identification based on it (the justification is given in Section 3).

2.3 Attention-based RNN

Attention-based RNN [25] introduces an attention mechanism to the RNN framework. The attention mechanism enables RNN to allocate different weights to different parts of the input, and consequently, improve the exploration of the corresponding relationship between the input sequence and the output sequence. Generally, attention module is added to the original RNN framework as an external module, but is trained instantaneously with the RNN structure [40]. Attention-based RNN has achieved success in speech recognition [2], NLP (Natural Language Processing) [1], and computer version [25]. Bahdanau et al. [2] attempt to build a Large Vocabulary Continuous Speech Recognition (LVCSR) Systems using attention-based RNN and demonstrate that their approach, compared with traditional methods, requires fewer training stages, less auxiliary data, and less domain expertise. Luong et al. [1] explore the architecture of attention-based neural machine translation and examine the effects of two attentional mechanisms (one that focuses on all source words and and the other which focuses on a subset of words) on the WMT translation tasks between English and German in both directions. Ba et al. [25] present an attention-based RNN for recognizing multiple objects in images, while only being provided with class labels during training. The results show that the attention-based RNN is more accurate and less computation than the state-of-the-art. To our best knowledge, we are the very first work employing attention-based RNN for EEG-based user identification.

3 EEG PATTERN ANALYSIS

In this section, we first introduce some background about EEG patterns followed by a topographical analysis of real-world EEG data to discover which specific constituent patterns capture the most distinctive features that

allow us to distinguish the subject's identity. Next, we analyze why Delta pattern works best both qualitatively and quantitatively.

The EEG signals collected from any typical EEG hardware can can be divided into several non-overlapping frequency bands (Delta, Theta, Alpha, Beta, and Gamma) based on the strong intra-band correlation with a distinct behavioral state [3, 24, 36]. Each decomposed EEG pattern contains signals associated with particular brain information. The EEG frequency patterns and the corresponding characteristics are listed in Table 1. The awareness degree in this paper denotes the perception of individuals while facing outside stimuli. Each frequency band represents a specific active situation of brain state and a qualitative assessment of awareness. More specifically,

- **Delta pattern** ($0.5 - 4$ Hz) is associated with deep sleep while the subject has lower awareness.
- **Theta pattern** ($4 - 8$ Hz) corresponds to light sleep in the realm of low awareness.
- **Alpha pattern** ($8 - 12$ Hz) mainly occurs during eyes closed and deeply relaxed state, and corresponds to the medium awareness.
- **Beta pattern** ($12 - 30$ Hz) is the dominant rhythm while the subject's eyes are open and is associated with high awareness. Most of our daily activities (such as eating, walking, and talking) are captured by Beta patterns.
- **Gamma pattern** ($30 - 100$ Hz) represents the joint interaction of several brain areas to carry out a specific motor and cognitive function. This pattern is associated with highest awareness.

In order to investigate which EEG pattern is most intrinsic and rich of distinctive information for user identification, we study the EEG topography of different frequency patterns. Figure 1 shows the EEG topography of various subjects on full bands, Delta, Theta, Alpha, Beta, and Gamma patterns, respectively. Moreover, we calculated the cosine-similarity between EEG signals belonging to different subjects in a pairwise manner. The averaged cosine-similarity are as follows: 0.1313 (full patterns), 0.0722 (Delta pattern), 0.1672 (Theta pattern), 0.2819 (Alpha pattern), 0.0888 (Beta pattern), and 0.082 (Gamma pattern). This illustrates that the delta pattern has the lowest inter-subject similarity compared to other patterns and thus is likely to offer the most distinguishable features for person identification. In the following, we present two arguments to explain why Delta patterns are suited for user identification. Prior studies have shown that the functional significance of delta oscillations is not yet fully understood[20]. Our arguments below are based on the current knowledge of Delta patterns.

On one hand, qualitatively, Delta pattern is universal and stable. A widely accepted view about Delta pattern is that it only occurs in deep sleep state. This is a significant reason why most researchers neglect Delta frequency in user identification. However, recent research in neurophysiology claims that the Delta rhythm is often evident during 'quiet' wakefulness in rodents and nonhuman primates [31]. This suggests that the delta patterns can dominate the background activity of some neocortical circuits in awake individuals. In addition, Delta pattern is observed to be related to cognitive processing [14]. It's easy to infer that Delta pattern exists while the subject is awake (processing cognitive tasks). Compared with baseline (a state with no delta waves), delta waves are associated with increase of activity in many brain regions, which suggests that Delta pattern is not associated with a state of brain quiescence, but rather associated with an active state during which brain activity is consistently synchronized to the slow oscillation in specific cerebral regions [8]. Moreover, there is evidence that suggests that Delta patterns are primarily created in the hypothalamus [26] which is associated with a series of life-support body functions such as autonomic regulation (e.g.,blood pressure, heart rate, thermoregulation) and neuroendocrine control [41]. Considerable evidence on the association between delta waves and autonomic and metabolic processes shows that integration of cerebral activity with homeostatic processes might be one of the Delta wave's functions [20]. Since the life-support functions are operational all the time, we can argue that regardless of the state of the individual, Delta oscillations will always be produced.

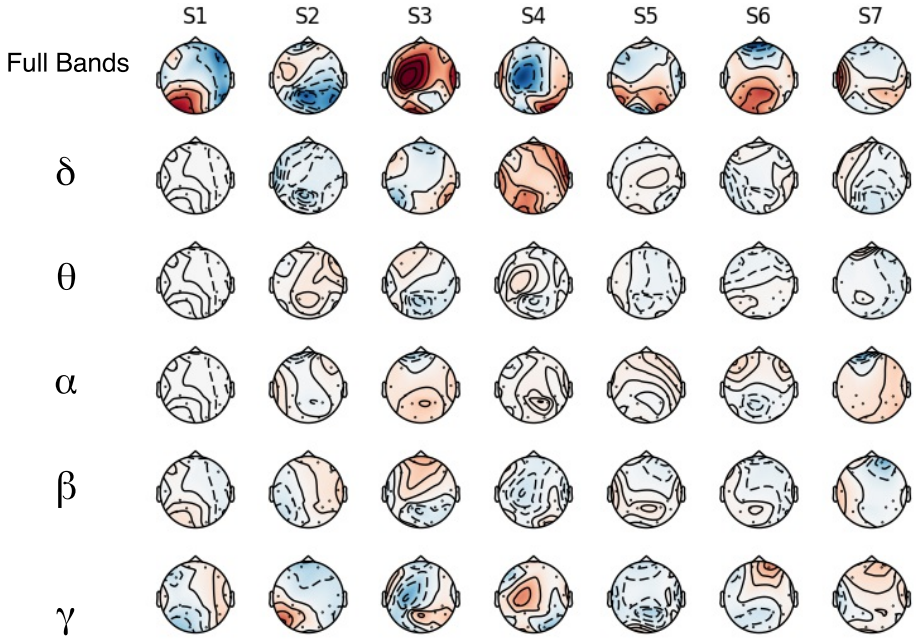

Fig. 1. EEG topography of various subjects under different frequency patterns. The inter-subject EEG signal cosine-similarity is calculated under each pattern and the results are reported as 0.1313 (full patterns), 0.0722 (Delta pattern), 0.1672 (Theta pattern), 0.2819 (Alpha pattern), 0.0888 (Beta pattern), and 0.082 (Gamma pattern). This illustrates that the delta pattern has the lowest inter-subject similarity compared to other patterns and thus is likely to offer the most distinguishable features for person identification.

Table 2. The inter-subject correlation coefficients. Full denotes the un-decomposed full-frequency band data. The lower coefficients indicate that the subject's EEG data is easier to be distinguished. We used data from the EID-M dataset (detailed in Section 5.1).

Subject		Subject 1	Subject 2	Subject 3	Subject 4	Subject 5	Subject 6	Subject 7	Subject 8	STD	Average
Patterns	Delta	0.137	0.428	0.246	0.179	0.221	0.119	0.187	0.239	0.089554	**0.219**
	Theta	0.447	0.671	0.552	0.31	0.387	0.207	0.199	0.386	0.151929	0.395
	Alpha	0.387	0.629	0.615	0.377	0.299	0.306	0.283	0.457	0.128653	0.419
	Beta	0.249	0.487	0.329	0.308	0.281	0.307	0.238	0.441	0.083224	0.33
	Gamma	0.528	0.692	0.538	0.362	0.521	0.667	0.428	0.537	0.102288	0.534
	Full	0.333	0.329	0.408	0.304	0.297	0.621	0.302	0.447	0.104231	0.38

Next, we present some qualitative arguments to demonstrate that Delta patterns contain the most distinguishable information. We analyze inter-subject correlations of the decomposed EEG patterns, which measure the similarity of two samples belonging to different subjects. For example, the inter-subject correlation of subject 1 is calculated by the following steps: 1) randomly select 10 samples from subject 1; 2) randomly select 10 samples from each of other subjects (subject 2-8) to get 70 samples; 3) calculate the pair wise similarity between the first 10 samples and the latter 70 samples to get 700 similarities; 4) average the 700 similarities to produce the finally inter-subject correlation coefficient of subject 1. We measure the inter-subject correlations for all the frequency patterns in order to discover the most effective pattern. We used data from the EID-M dataset (detailed

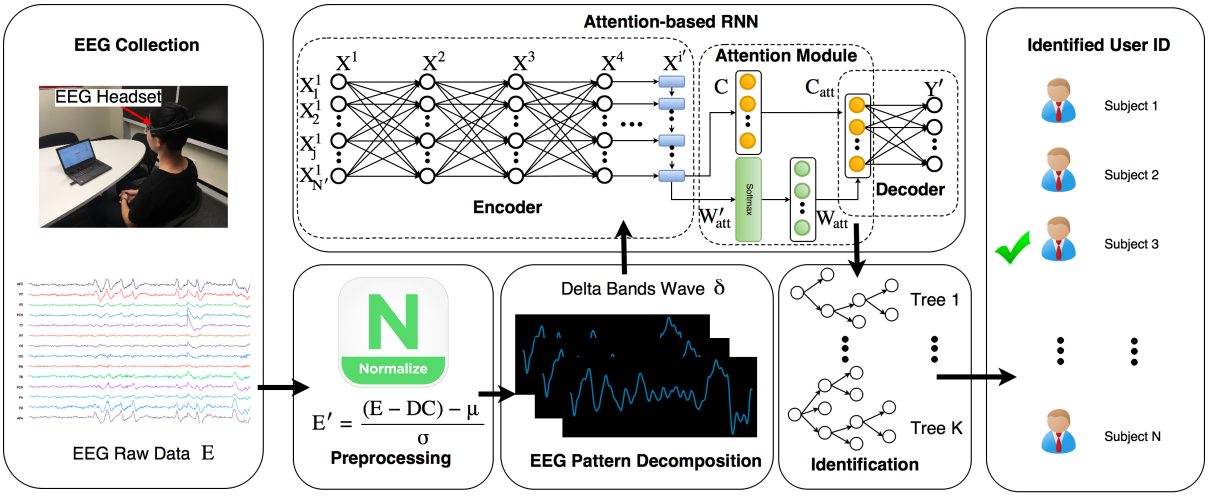

Fig. 2. Flowchart of the proposed approach. At the beginning of identification, raw EEG data E is collected from the user and then fed to the preprocessing stage. The preprocessed data E' is decomposed to Delta pattern δ which serves as the input to the attention-based RNN. The encoder compresses the input sequence X^1 into an intermediate code C and produces the weights W'_{att} simultaneously. The attention-based module accepts both C and W'_{att} from the LSTM layer $X^{i'}$, processes W'_{att} through a softmax layer, and calculates the attention-based code C_{att}. Finally, a statistical boosting classifier is employed to identify the user.

in Section 5.1). The correlation coefficient analysis results are shown in Table 2. We can observe that the Delta pattern has the lowest inter-subject correlation coefficients compared with other patterns. This indicates that the Delta patterns are most dissimilar to other samples, and thus most distinctive. Therefore, Delta patterns show promise for user identification. The dedicated comparative experiment between different EEG patterns will be reported in Section 5.7.

4 METHODOLOGY

In this section, we first give an overview of the proposed MindID system and then present the technical details for each component, namely, *Preprocessing*, *EEG pattern decomposition*, *Attention-based RNN*, and *Classification*.

4.1 Overview

Figure 2 outlines the specific steps of the proposed MindID system. The brainwaves are collected by the portable EEG acquisition equipment while the user is in a relaxed state with his/her eyes closed (our preliminary experiment results illustrate that the Delta wave is more domination in relaxed state although still exists in all states). Each EEG sample is a numerical feature vector with N dimensions which correspond to the number of channels of the wearable EEG headset. The EEG samples are first preprocessed to remove the Direct Current (DC) offset and followed by normalization (Section 4.2). Next, we employ EEG pattern decomposition to isolate the Delta waves since they contain the most distinctive information which can be used to identify the subject (as outlined in Section 3). The delta waves are fed to an attention-based Encoder-Decoder RNN, which identifies the most distinctive channels and adjusts the weights accordingly. This model learns the deep correlations between the delta patterns which are then fed to a statistical boosting classifier (Section 4.5) to identify individual users.

4.2 Preprocessing

The raw EEG samples are pre-processed to remove the DC offset and normalize the signals. Eliminating DC offset is necessary because EEG headsets invariably introduce a constant noise component in the recorded signals. The specific headset used in our experiments (details in Section 5) introduces a DC offset of 4200 muV[6]. In the preprocessing stage, this constant DC offset is first subtracted from the raw signal E.

Normalization also plays a crucial role in a knowledge discovery process for handling different units and scales of features. For example, if two raw data sources, one ranging from 0 to 1 and another ranging from 0 to 100 are together used for analysis then the results will be dominated by the latter if normalization is not employed. Generally, there are three widely used normalization methods: Min-Max Normalization, Unity Normalization, and Z-score Scaling Normalization [43]. Our experiments (not shown for brevity) indicated that Z-score scaling is the most suited for the EEG data. In summary, the preprocessed data E' can be calculated by

$$E' = \frac{(E - DC) - \mu}{\sigma}$$

where DC denotes the Direct Current which is 4200 muV, μ denotes the mean of $E - DC$ and σ denotes the standard deviation.

4.3 EEG Pattern Decomposition

In Section 3, we used empirical EEG data to show that the part of the EEG signals that belong to the Delta frequency band ($0.5 - 4Hz$) is particularly well-suited for accurate and robust user identification. To isolate the signals in the Delta band, we use a Butterworth band-pass filter of order 3 with the frequency range of 0.5Hz to 4Hz. The designed filter has the following specifications: the order is three, the low cut is $0.5Hz$, and the high cut is set as $4Hz$. The preprocessed signal E' is fed as input to this filter which provides the decomposed Delta pattern δ as output.

4.4 Attention-based RNN

Next, the Delta pattern δ is fed into an attention-based Encoder-Decoder RNN structure [40] which aims to learn the most representable features for user identification. The general Encoder-Decoder RNN framework assumes that all feature dimensions of the input sequence are equally important and assigns them equal weights. In the context of EEG data, each dimension refers to a different electrode of the EEG equipment. For example, the first dimension (first channel) collects the EEG data from the $AF3$[7] electrode which is located at the frontal lobe of the scalp while the 7-th dimension is gathered from $O1$ electrode at the occipital lobe.

Since different EEG channels record different aspects of the brain signals, some of which are more representative of the individual, an approach that assumes all dimensions to be equal may not be suitable. On the other words, various EEG channels have different contribution to the person identification task and should be corresponding to different weights. The effectiveness of attention-based RNN has been demonstrated in various domains including wearable sensor based activity recognition [6, 42], natural language processing [1, 23, 39], computer version [25] and speech recognition [2, 5]. Inspired by the wide success of this approach, we introduce the attention mechanism to the Encoder-Decoder RNN model to assign varying weights to different dimensions of the EEG data. The proposed attention-based Encoder-Decoder RNN consists of three components (as shown in Figure 2): the encoder, the attention module, and the decoder. The encoder is designed to compress the input Delta δ wave into a single intermediate code C; the attention module calculates a better intermediate code C_{att} by generating a sequence of distinct weights W_{att} for the different dimensions; the decoder accepts the attention-based code

[6] https://www.bci2000.org/mediawiki/index.php/Contributions:Emotiv

[7] Both $AF3$ and $O2$ are EEG measurement positions in the International 10-20 Systems.

Table 3. Notation

Parameters	Explanation
E	EEG raw data
E'	Preprocessed EEG data
δ	Delta pattern of E'
X^i	Data in the i-th layer in attention-based RNN
I	The number of layers in attention-based RNN
N^i	The number of dimensions of X^i
Y	The one-hot label of user ID
Y'	The attention-based RNN predicts user ID
K	The number of user ID categories
$\mathcal{T}(\cdot)$	The linear function
C	The intermediate code
$\mathcal{L}(\cdot)$	The output calculation procedure of LSTM cell
$\mathcal{L}'(\cdot)$	The final hidden state calculation procedure of LSTM cell
f_i, f_f, f_o, f_m	The input, forget, output, and input modulation gate
W'_{att}	The unnormalized attention weights
W_{att}	The normalized attention weights
C_{att}	The attention-based intermediate code
n_{iter}	The iteration threshold of attention-based RNN
X_D	The learned deep feature from attention-based RNN
x_d	A single sample in X_D
m	The m-th tree
M	The number of XGB trees
I_D	The final identified user ID of MindID approach

C_{att} and decodes it to the user ID. Note, this user ID is predicted by the attention-based RNN instead of MindID, and the final identified ID of MindID approach will be introduced in Section 4.5.

Suppose the data in i-th layer could be denoted by $X^i = (X^i_j; i \in [1, 2, \cdots, I], j \in [1, 2, \cdots, N^i])$ where j denotes the j-th dimension of X^i. I represents the number of neural network layers in the proposed attention based RNN model while N^i denotes the number of dimensions in X^i. Take the first layer as an example, we have $X^1 = \delta$ which indicates the input sequence is the Delta pattern. Let the output sequence be $Y = (Y_k; k \in [1, 2, \cdots, K])$ where K denotes the number of user ID categories. In this paper, the user ID is represented by the one-hot label with length K. For simplicity, let's define the operation $\mathcal{T}(\cdot)$ as:

$$\mathcal{T}(X^i) = X^i W + b$$

Further more, we have

$$\mathcal{T}(X^{i-1}_j, X^i_{j-1}) = X^{i-1}_j * W' + X^i_{j-1} * W'' + b'$$

where W, b, W', W'', b' denote the corresponding weights and biases parameters.

The encoder component contains several non-recurrent fully-connected neural network layers and one recurrent Long Short-Term Memory (LSTM) layer. The non-recurrent layers are employed to construct and fit a non-linear function to purify the input Delta pattern. The necessity of which is demonstrated by our preliminary

experiments[8]. The data flow in these non-recurrent layers are calculated as follows,

$$X^{i+1} = \mathcal{T}(X^i)$$

The LSTM layer is adopted to compress the output of non-recurrent layers to a length-fixed sequence which is regarded as the intermediate code C. Suppose LSTM is the i'-th layer, the code equals to the output of LSTM, which is $C = X_j^{i'}$. The $X_j^{i'}$ can be measured by

$$X_j^{i'} = \mathcal{L}(c_{j-1}^{i'}, X_j^{i-1}, X_{j-1}^{i'}) \tag{1}$$

where $c_{j-1}^{i'}$ denotes the hidden state of the $(j-1)$-th LSTM cell. The operation $\mathcal{L}(\cdot)$ denotes the calculation process of the LSTM structure, which can be inferred from the following equations

$$X_j^{i'} = f_o \odot tanh(c_j^{i'})$$
$$c_j^{i'} = f_f \odot c_{j-1}^{i'} + f_i \odot f_m$$
$$f_o = sigmoid(\mathcal{T}(X_j^{i'-1}, X_{j-1}^{i'}))$$
$$f_f = sigmoid(\mathcal{T}(X_j^{i'-1}, X_{j-1}^{i'}))$$
$$f_i = sigmoid(\mathcal{T}(X_j^{i'-1}, X_{j-1}^{i'}))$$
$$f_m = tanh(\mathcal{T}(X_j^{i'-1}, X_{j-1}^{i'}))$$

where f_o, f_f, f_i and f_m represent the output gate, forget gate, input gate and input modulation gate[9], separately, and $\odot$ denotes the element-wise multiplication.

The attention module accepts the final hidden states as the unnormalized attention weights W'_{att} which can be measured by the mapping operation $\mathcal{L}'(\cdot)$ (similar with Equation 1)

$$W'_{att} = \mathcal{L}'(c_{j-1}^{i'}, X_j^{i-1}, X_{j-1}^{i'})$$

and calculate the normalized attention weights W_{att}

$$W_{att} = softmax(W'_{att})$$

The softmax function is employed to normalize the attention weights into the range of $[0, 1]$. Therefore, the weights can be explained as the probability that how the code C is relevant to the output results. Under the attention mechanism, the code C is weighted to C_{att}

$$C_{att} = C \odot W_{att}$$

Note, C and W_{att} are trained instantaneously. The decoder receives the attention-based code C_{att} and decodes it to predict the user ID Y'[10] . Since Y' is predicted at the output layer of the attention based RNN model ($Y' = X^I$), we have

$$Y' = \mathcal{T}(C_{att})$$

At last, we employ the cross-entropy function to calculate the prediction cost between the predicted ID Y' and the ground truth Y. ℓ_2-norm (with parameter λ) is selected to prevent overfitting. The cost is optimized by the AdamOptimizer algorithm [18]. The threshold for the number of iterations of the attention-based RNN is set as n_{iter}. The weighted code C_{att} has a linear relationship with the output layer and the predicted results. If the model is trained well then the weighted code C_{att} could be regarded as the weighted code as a high-quality

[8]Some optimal designs like the neural network layers are validated by the preliminary experiments but the validation procedure will not be reported in this paper for space limitation

[9]http://colah.github.io/posts/2015-08-Understanding-LSTMs/

[10]Note, Y' is not the identification results of MindID model. The final identified user ID is I_D calculated in Section 4.5

ALGORITHM 1: The MindID User Identification Algorithm

Input: EEG raw data E
Output: Identification results I_D

Initialization;
Preprocessing: $E' \leftarrow E$;
EEG pattern decomposition: $\delta \leftarrow E'$;
if $iteration < n_{iter}$ **then**
  for $i = 1, 2, \cdots, I$ **do**
    $X^1 = \delta$
    $C \leftarrow X^1, \mathcal{L}(c_{j-1}^{i'}, X_j^{i-1}, X_{j-1}^{i'})$
    $W_{att} \leftarrow C, \mathcal{L}'(c_{j-1}^{i'}, X_j^{i-1}, X_{j-1}^{i'})$
    $C_{att} = C \odot W_{att}$
    $X_D = C_{att}$
  end for
else
  Return X_D
end if
for X_D **do**
  $I_D \leftarrow X_D$
end for
return I_D

representation of the identity of the user. We set the learned deep feature X_D equals to C_{att}, $X_D = C_{att}$, and use it to recognize the user in the identification stage.

4.5 Identification

In this section, we employ Extreme Gradient Boosting classifier (XGB) [7] to classify the learned deep feature X_D for user identification. The XGB classifier fuses a set of classification and regression trees (CART) and exploits as detailed information as possible from the input features X_D. It builds multiple trees and each tree has its leaves and corresponding scores. Moreover, it proposes a regularized model formalization to prevent over-fitting and it is widely used for its accurate prediction power.

The learned deep feature X_D is used to train a number of the CART (there are M trees) and predict a set of user's IDs. Suppose $x_d \in X_D$ is a single sample of the deep feature. The finally identification result of the input x_d is calculated as

$$y_m = f(x_d)$$
$$I_D = F(\sum_{1}^{M} y_m), m = 1, 2, \cdots, M$$

where f denotes the classification function of a single tree, y_m denotes the predicted ID of the m-th tree and F denotes the mapping from single tree prediction space to the final prediction space. The I_D is the final identified user ID. The overall procedure is summarized in Algorithm 1. All the parameters mentioned in this section are listed in Table 3.

5 EXPERIMENTS AND RESULTS

We first outline the experimental settings in Section 5.1. Next, we systematically investigate the following questions:

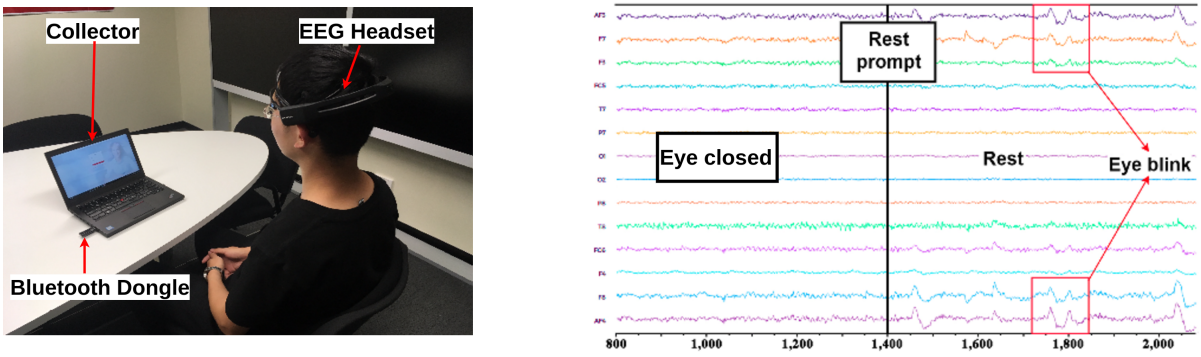

Fig. 3. EEG collection experiment and the collected raw data. The EEG raw data is gathered by the EEG headset and transmitted to server storing the data through bluetooth. The EEG data is recorded while the user is relaxed and keeps his eyes closed.

Table 4. Datasets details. In Trial column, M denotes multi-trials and S denotes single-trial. **EID-M** is used to compare the proposed approach with the state-of-the-art and baselines; the comparison between **EID-M** and **EID-S** are used to verify the robustness; the comparison between **EID-S** and **EEG-S** are used to verify the adaptability. **EED-S-L** is used to evaluate the influence of the number of participants and **EEG-S** is a subset of **EEG-S-L**.

Name	Source	Channels	Trial	Frequency	Subjects	Comparison	Robustness	Adaptability
EID-M	Local	14	M	128 *Hz*	8	✓	✓	-
EID-S	Local	14	S	128 *Hz*	8	-	✓	✓
EEG-S-L	Public	64	S	160 *Hz*	20	-	-	-
EEG-S	Public	64	S	160 *Hz*	8	-	-	✓

- How does MindID compare with state-of-the-art methods and other baselines (Section 5.2)?
- How efficient is MindID (Section 5.3)?
- Is MindID robust under a multi-trial setting (Section 5.4)?
- Does MindID exhibit consistence results when tested with different datasets (Section 5.5)?
- Do the number of subjects impact the results (Section 5.6)?
- How do other decomposed EEG signals compare with the Delta signals (Section 5.7)?

5.1 Experimental Settings

5.1.1 Datasets. The proposed MindID system is evaluated by three datasets: a multi-trial local dataset (*EID-M*), a single-trial dataset (*EID-S*), and a public dataset (*eegmmidb*). The details of datasets are introduced in Table 4. All the datasets measure the EEG raw data from the subject's scalp while the subject is relaxed.

EID-M denotes EEG based ID recognition with the training set coming from the different trials in the same day. Since a multi-trial scenario is more representative of a practical setting, EID-M dataset is used to compare MindID with the state-of-the-art methods and baselines. The EID-M dataset is collected locally in our lab from 8 subjects (5 males and 3 females) aged from 24 to 28. We use the *Emotiv Epoc+*[11] headset and the experiment setting is depicted in Figure 3.

[11] https://www.emotiv.com/product/emotiv-epoc-14-channel-mobile-eeg/

Table 5. Evaluation report of EID-M dataset. The overall accuracy achieves 0.982 of 21000 testing samples. The support is the number of samples of each class.

	0	1	2	3	4	5	6	7	Average/Total
Precision	0.9723	0.9789	0.9777	0.9894	0.989	0.9814	0.9898	0.9774	**0.982**
Recall	0.9822	0.9885	0.9945	0.9711	0.9808	0.9821	0.9742	0.9834	0.9821
F1-score	0.9772	0.9837	0.9860	0.9802	0.9849	0.9818	0.9820	0.9804	0.982
Support	2674	2554	2601	2650	2639	2634	2636	2612	21000

The Emotiv Epoc+ contains 14 channels and the sampling rate is set as 128 *Hz*. In the experiment, each subject undertakes three trials and each trial produces 7,000 EEG samples. Summarily, each subject has 21,000 samples and the whole EID-M dataset contains 168,000 samples.

EID-S is collected under the same situation with EID-M (5 males, 3 females, 14 channels, and 128 Hz). The main difference between them is the former dataset is collected in the single trial. EID-S in total contains 56,000 samples belonging to 8 subjects (7,000 samples per subject).

EEG-S-L is a subset of the widely used online public dataset *eegmmidb* (*EEG motor movement/imagery database*)[12]. It is collected with the BCI2000 (Brain Computer Interface) instrumentation system [13] [34] (64 channels and 160 *Hz* sampling rate). EEG-S contains 20 subjects with 7000 samples collected from each subject in a single trial setting.

EEG-S is a subset of EEG-S-L, which only contains 8 subjects. To compare the adaptability of the proposed approach (Section 5.5), we randomly select 8 participants from EEG-S-L to compare with EID-S. This allows us to undertake a like-by-like comparison with the only variable being the type of EEG headset used.

To assess the performance of the proposed MindID model, we employ several widely-used evaluation metrics such as accuracy, precision, recall, F1 score, ROC (Receiver Operating Characteristic) curve, support, and AUC (Area Under the Curve).

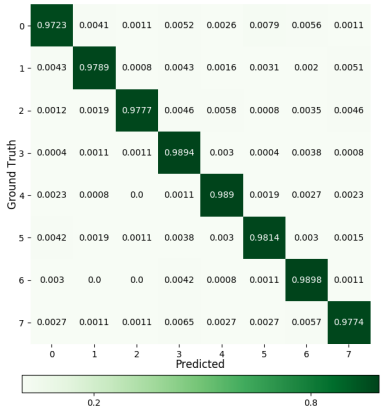

Fig. 4. Confusion matrix of EID-M

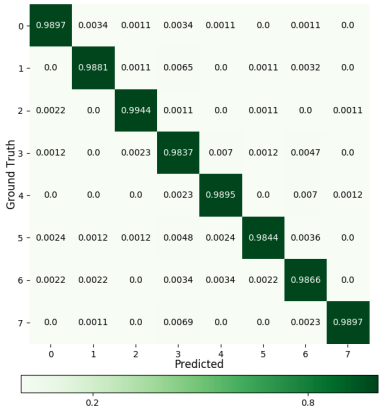

Fig. 5. Confusion matrix of EID-S

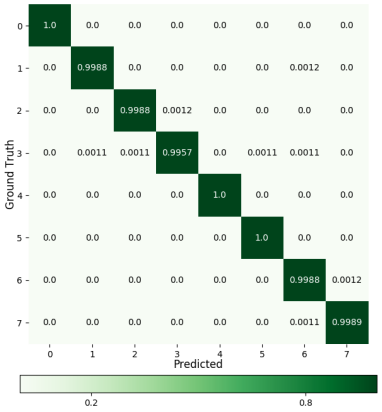

Fig. 6. Confusion matrix of EEG-S

[12] https://www.physionet.org/pn4/eegmmidb/
[13] http://www.schalklab.org/research/bci2000

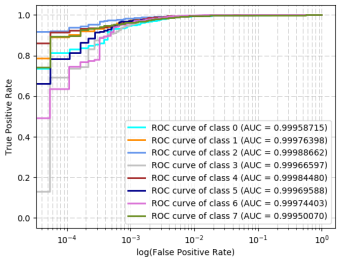

Fig. 7. ROC and AUC of EID-M

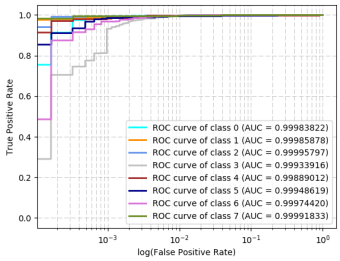

Fig. 8. ROC and AUC of EID-S

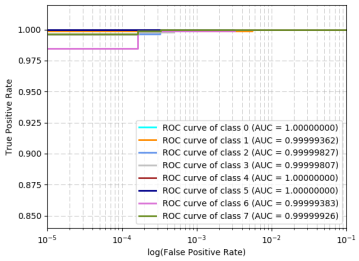

Fig. 9. ROC and AUC of EEG-S

Table 6. The accuracy comparison with baselines and the state-of-the-art methods over EID-M dataset. The result shows that our approach achieves the highest accuracy of 0.982.

Index	Method	Acc	Recall	F1-Sore	AUC
1	Jayarathne[15]	0.919	0.914	0.9165	0.946
2	Bashar et al. [4]	0.873	0.898	0.8853	0.907
3	Keshishzadeh et al. [17]	0.815	0.843	0.8288	0.859
4	Gui et al.[12]	0.833	0.811	0.8219	0.842
5	Thomas and Vinod [37]	0.859	0.869	0.8640	0.888
6	Kumari and Vaish [21]	0.875	0.872	0.8735	0.901
7	RF	0.795	0.813	0.8039	0.827
8	KNN	0.849	0.836	0.8424	0.847
9	RNN	0.815	0.803	0.8090	0.821
10	RNN+XGB	0.808	0.789	0.7984	0.803
11	PD+RNN	0.853	0.821	0.8367	0.844
12	AR+RNN	0.811	0.798	0.8044	0.831
13	XGB	0.815	0.811	0.8130	0.853
14	PD+XGB	0.965	0.959	0.9620	0.977
15	Ours (EID-M)	**0.982**	**0.9821**	**0.9820**	**0.999**

5.2 Overall Comparison

In this section, we firstly report the performance of MindID using the EID-M dataset and then compare the proposed approach with the state-of-the-art approaches and baselines. We randomly select 147,000 samples from EID-M to train the model and the residual 21,000 samples are used to test the performance. Through tuning, the hyper-parameters used in our approach are listed following. In EEG pattern decomposition, we employ a 3 order butter-worth band-pass filter and the passband is $[0.5Hz, 4Hz]$. In the attention-based RNN structure, the encoder consists of 1 input layer (14 nodes), 3 non-recurrent fully-connected hidden layers (164 nodes) and 1 recurrent LSTM layer (164 cells); the decoder includes 1 fully-connected hidden layer (164 nodes) and 1 output layer (8 nodes). The learning rate is 0.001; the parameter of $\ell - 2$ norm is set as 0.001; the encoder and decoder separately have 6 and 2 layers; training dataset is divided into 7 batches with the batch size of 21,000; the number of training iterations is 2000. In the classifier: the learning rate is 0.7; the sub-sampling rate is 0.9; the max depth is set as 6; the training iterations is 500. The ground truth (from 0 to 7) is represented as a one-hot label which corresponding to the ID of subjects.

The proposed approach achieves the highest identification accuracy of **0.982**. The detailed confusion matrix, evaluation report, and ROC curves (with AUC scores) are illustrated in Figure 4, Table 5, and Figure 7, respectively. Observe that our approach obtains higher than 0.97 precision for each class.

In addition, we compare the accuracy of our method and other state-of-the-art and baselines in Table 6. RF denotes Random Forest, AdaBoost denotes Adaptive Boosting, LDA denotes Linear Discriminant Analysis, PD denotes for Pattern Decomposition, AR denotes AutoRegressive method, and XGB denotes for X-Gradient Boosting classifier (the classifier used in our approach). In addition, the key parameters of the baselines are listed here: Linear SVM ($C = 1$), RF ($n = 200$), KNN (k=3), and AR (13 order autoregressive from 40 samples). The setting up of PD, RNN and XGB classifier are same as the hyper-parameters mentioned above. The methods used in the state-of-the-art are introduced as follows:

- Jayarathne et al. [15] focus on the 8 to 30 Hz Alpha and Beta combined frequency band across all EEG channels and extract the Common Spatial Patterns (CSP) values as classification features. LDA is employed as the classifier.
- Bashar et al. [4] first remove noise and artifacts using Bandpass FIR filter. Then learn the features through multi-scale shape description (MSD), multi-scale wavelet packet statistics (WPS) and multi-scale wavelet packet energy statistics (WPES). These features are finally used to train a support vector machine (SVM) classifier.
- Keshishzadeh et al. [17] investigates the Autoregressive (AR) coefficients as the feature set which is identified by an SVM classifier.
- Gui et al.[12] propose to reduce the noise level through a low-pass filter, extract frequency features using wavelet packet decomposition, and perform classification based on a deep neural network.
- Thomas and Vinod [37] combine subject-specific Alpha peak frequency, peak power, and Delta band power values to form discriminative feature vectors and templates.
- Kumari and Vaish [21] apply discrete wavelet analysis to decompose the raw EEG signals corresponding to sub-band frequency (0-59Hz). The extracted statistical measures and energy calculation of each decomposed wave are classified by a neural network structure.

As noted earlier, we use the EID-M dataset for the comparison. As observed from Table 6, our method significantly outperforms all other methods in all metrics.

5.3 Efficiency Evaluation

In this section, the efficiency refers to the latency incurred to perform the identification.High latency may limit the suitability for practical deployment. We compare MindID with the same baselines and classification methods as in Section 5.2. In this paper, we run the experiments on a GPU-accelerated machine with Nvidia Titan X Pascal GPU, 768G memory, and 145 TB PCIe based SSD.

The time required to train the identification model is illustrated in Figure 10(the X-axis label denotes the index of algorithms shown in Table 6). Observe that our approach (PD+RNN+XGB) and RNN+XGB require longer to train the model that other methods. There are two reasons behind this. First, these algorithms iterate over a large number of rounds. RNN and XGB executes 2000 and 500 iterations, respectively. Second, the deep learning structure and the boosting trees have an inherent complex structure and require many more parameters than other classification models. Compared to the training time, however, for practical considerations, the execution time of an algorithm during testing is more important than training which is a one-time operation. Figure 11 shows that the testing time of our model is less than 1 second, which is shorter than most of the state-of-the-art methods and baselines. Summarily, while MindID requires longer to train, the actual execution is near real-time (< 1 sec), thus making it attractive for real-world deployment.

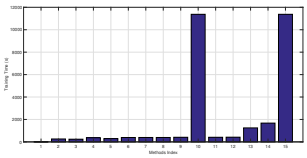

Fig. 10. Training time. The index corresponding the index in Table 6.

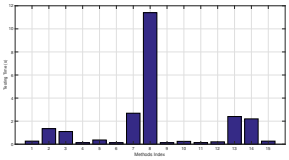

Fig. 11. Testing time. The index corresponding the index in Table 6.

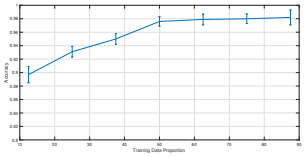

Fig. 12. The accuracy change trend with training data size

Table 7. Evaluation report of EID-S dataset. The overall accuracy achieves 0.9882 of 7000 testing samples.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Average/Total**
Precision	0.9897	0.9881	0.9944	0.9837	0.9895	0.9844	0.9866	0.9897	**0.9882**
Recall	0.992	0.9924	0.9944	0.9712	0.986	0.9939	0.9789	0.9977	0.9883
F1-score	0.9908	0.9903	0.9944	0.9774	0.9878	0.9891	0.9827	0.9937	0.9883
Support	872	927	892	857	857	831	893	871	7000

In practice, the amount of data needed to train the model is also an important consideration as gathering training data is not so easy. We conduct a set of experiments to investigate the influence of training data size on the accuracy. We run the experiments for 5 times and report the error-bar of results in Figure 12. Our approach achieves an accuracy of 0.9% even when only 12.5% of the available data set is used for the training. This is rather promising and suggests that our model has a low dependency on the size of the training data.

5.4 Robustness Evaluation

When an EEG-based system is deployed in the real world, the typical usage would always be in a multi-trail setting. That is the data used to train the system is collected in one trial (ie. one set of circumstances) which would be different form the conditions in which the system is employed for user identification. Note that the placement of the EEG headset on the user's skull may vary slightly for each usage. For example, the user wears the EEG headset and collects the first trial data; then collects the second trial data after he/she removes the headset and puts it back again. There may be some difference between two trials data, which is caused by the different placement position or other internal equipment reasons. Therefore, The divergence of the training data and testing data should be considered when the identification system is designed.

In this section, we evaluate the robustness of the proposed approach by analyzing whether the trial setting (single vs multi-trial) affects the identification accuracy. Two datasets, which respectively contain single-trial identification data (EID-S) and multi-trial identification data (EID-M), are employed.

The evaluation of EID-S is shown in Table 7, we can observe that our approach achieves the overall accuracy of **0.9882%** and the precision for all classes is greater 0.98. To gain further insight, the confusion matrix (Table 5) and ROC curves (Figure 8) are provided. The performance of MindID with EID-M was reported in Section 5.2 (Figure 4, Table 5, and Figure 7). The multi-trial setting results in a very slight decrease (0.9882 to 0.982) in the accuracy. However, the impact of inter-trial divergence is rather minimal (0.062). This suggests that MindID has the potential to be deployed in the real-world and achieve repeatable and accurate results in diverse conditions.

5.5 Adaptability Evaluation

To examine the adaptability and consistency, our model is evaluated using another dataset (EEG-S) which is collected from a more precise EEG equipment, BCI 2000 which has 64 channels and collects signals at 160Hz.

Table 8. Evaluation report of EEG-S dataset. The overall accuracy achieves 0.9989 of 7000 testing samples.

	0	1	2	3	4	5	6	7	Average/Total
Precision	1	0.9988	0.9988	0.9957	1	1	0.9988	0.9989	**0.9989**
Recall	1	0.9988	0.9988	0.9989	1	0.9988	0.9964	0.9989	0.9988
F1-score	1	0.9988	0.9988	0.9973	1	0.9994	0.9976	0.9989	0.9989
Support	872	869	848	939	880	864	842	886	7000

However, this headset is rather inconvenient to the subject. We selected a subset of this publicly available headset such that it matches the sample size of user population of our local dataset (EID-S), i.e., 56,000 samples from 8 subjects.

The results presented in Table 8 illustrate that our model achieves an accuracy of **0.9989** while all other metrics (precision, recall, and F1-score) are greater than 0.995. The confusion matrix and ROC curves are given in Figure 6 and Figure 9, respectively. The accurate classification of EEG-S demonstrates that our approach has good adaptability and able to handle different situations (such as different types of EEG equipments).

Comparing with the results for EID-S (Figure 5, Table 7, and Figure 8), we observe a slight improvement with EEG-S of about 0.01. We attribute this to the improved precision of the EEG headset in the number of channels (64 vs 14) and a higher sampling rate (160Hz vs 128Hz).

Section 5.4 and 5.5 illustrate that our approach is robust and adaptable and thus has the potential for practical deployment in many different environments.

5.6 Effect of User Population Size

The user population size is an important factor that can influence the performance of the identification system. Intuitively, as the target user population size increases, there is less distinction between the EEG signals of the individual subjects, which is thus likely to impact the identification accuracy. In this section, we design extensive experiments in order to explore the influence of the user population size. The dataset EEG-S-L contains EEG data collected from 20 subjects. We vary the total number of users in the target population group from 8 to 20 (in increments of 2) and plot the accuracy results in Figure 13. It is evident that there is a slight decrease in the accuracy from 0.9989 for 8 subjects to 0.9937 for 20 subjects. However, the accuracy is still over 99% and thus rather competitive. Furthermore, from Figure 13, we can observe that the derivative of the relationship curve is negative, which suggests that the proposed approach is likely to be effective for even larger population sizes. To provide further insight, the confusion matrix for the experiment with 20 subjects is reported in Figure 14.

5.7 Comparison of Different EEG Frequency Patterns

This section presents experiments to validate the hypothesis proposed in Section 3, which claims that the Delta pattern signals contain most distinguishable information for identification. In this experiment, we use the 3 dataset (EID-M, EID-S, and EEG-S) and decompose EEG signals into 6 frequency patterns, namely: Delta, Theta, Alpha, Beta, Gamma, and Full-frequency. The last set contains the entire frequency band of the EEG signals from 0 to $128Hz$. Since the sampling rate of the EEG signals is $128Hz$, the Butterworth filter employs a frequency range of 0 - 64 Hz.

We compare MindID with a subset of state-of-the-art methods and baselines as in Section 5.2. In particular, we select [4, 15, 17] as these methods do not rely on signals belonging to specific frequency bands but can rather use all 6 patterns under consideration. The results are shown in Table 9. The primary conclusions are listed as follows:

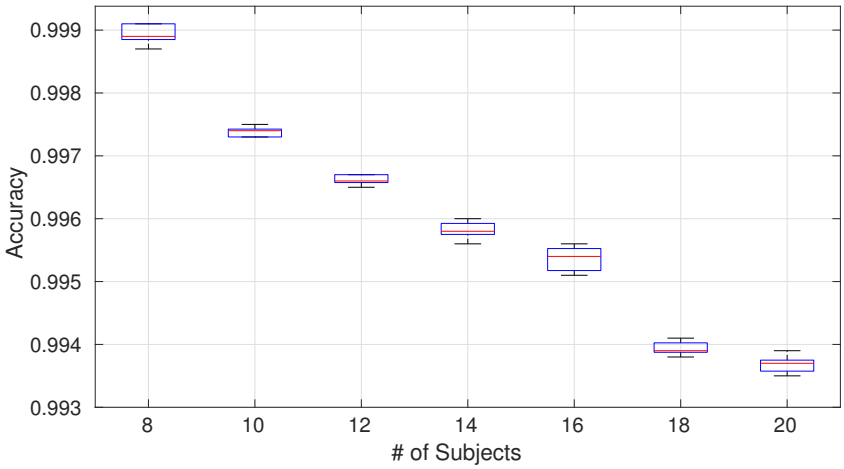

Fig. 13. The relationship between training subject number and identify accuracy

- Our approaches achieves the highest accuracy on all of the three datasets (with different trials, collection equipment, and sampling precision), which shows that our model has outstanding robustness and adaptability.
- The 11 methods including MindID achieve their best results with the Delta patterns. This result provides strong evidence to suggest that Delta pattern contain the most distinctive information for human identification and thus proves the hypothesis proposed in Section 3.
- Several statistical classification models (such as RF, KNN, and XGB) work well on the low-frequency patterns (Delta and Theta) but do not achieve good results with high-frequency band signals (Alpha, Beta, and Gamma).
- Deep learning methods are particularly good at extracting deep relationships between the samples which are inherently noisy and fluctuating. This conclusion can be inferred from the observations that RNN has lower accuracy than RF/KNN/XGB with Delta and Theta patterns but performs better with other patterns. These observations inspire the combination of the attention-based RNN structure and the tree-boosting classifier.
- The baselines and the state-of-the-art methods can achieve acceptable identification accuracy with high-quality EEG dataset (EEG-S) but performs poorly with the low-quality datasets (EID-M and EID-S). Consider the Full-frequency pattern as an example, RF/XGB/RNN achieves an accuracy of more than 0.95 on EEG-S but lower than 0.82 on EID-M. *However, our approach consistently achieves high accuracy no matter the data quality.* This suggests that MindID has the potential to deal with various real-world effects and thus a prime candidate for practical deployment.

6 DISCUSSION AND FUTURE WORK

In this paper, we propose an EEG-based identification approach and evaluate the robustness and adaptability over three datasets. In this section, we discuss the challenges and potential directions for future research.

- First, EEG-based identification system is less vulnerable to attacks compared to existing biometric identification systems. In order to evaluate the attack-resilience of MindID, We test our approach to dealing with the threat from unauthorized subjects among a number of attack categories [29]. We randomly select 10 subjects

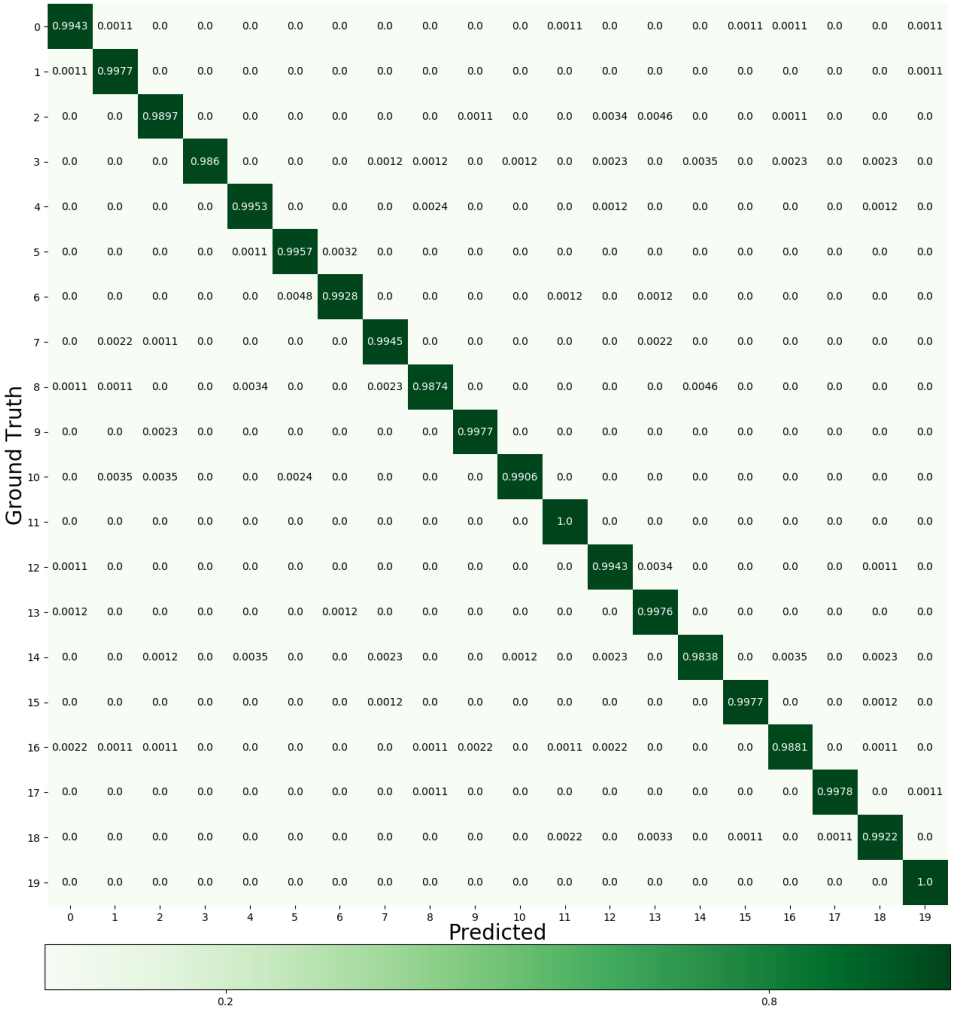

Fig. 14. Confusion matrix of EEG-S-L dataset

from EEG-S-L dataset as authorized users while the rest of users are as unauthorized subjects. During the testing, given the unauthorized users' EEG signals, MindID predicts the probability indicating how likely the samples belong to an authorized subject or not. The specific user will be regarded as unauthorized if the predict probability is under a threshold. Our experimental results demonstrate that MindID is able to precisely detect the authorized users with around 99% accuracy under an appropriate threshold setting. This suggests that our approach has the potential to distinguish the attack from unauthorized subject.

- Second, the impact of variations in the EEG signals over longitudinal scales on the performance of such identification systems needs to be studied. For a thorough investigation, it would be necessary to collect EEG data over multiple trials spread across several days. We have taken some preliminary steps in this

Table 9. EEG Pattern Decomposition Analysis

Dataset	Methods	EEG Patterns						Best Result
		Delta	Theta	Alpha	Beta	Gamma	Full	
EID-M	**Jayarathne [15]**	0.919	0.701	0.725	0.598	0.602	0.785	**0.982 (Delta)**
	Bashar et al. [4]	0.873	0.716	0.425	0.393	0.412	0.571	
	Keshishzadeh et al. [17]	0.815	0.672	0.536	0.273	0.409	0.511	
	SVM	0.143	0.157	0.137	0.135	0.138	0.2745	
	RF	0.936	0.707	0.677	0.489	**0.435**	0.7935	
	KNN	0.941	**0.804**	0.618	0.35	0.313	0.819	
	AdaBoost	0.251	0.13	0.15	0.15	0.171	0.24	
	LDA	0.148	0.154	0.135	0.135	0.129	0.28	
	XGB	0.965	0.665	0.69	0.495	0.414	0.815	
	RNN	0.917	0.709	0.708	0.518	0.411	0.813	
	Ours	**0.982**	0.713	**0.73**	**0.513**	0.423	**0.822**	
EID-S	**Jayarathne [15]**	0.938	0.799	0.764	0.602	0.663	0.828	**0.9882 (Delta)**
	Bashar et al. [4]	0.884	0.760	0.437	0.413	0.452	0.597	
	Keshishzadeh et al. [17]	0.846	0.699	0.672	0.413	0.498	0.628	
	SVM	0.135	0.162	0.181	0.152	0.132	0.408	
	RF	0.947	0.771	0.719	0.587	0.377	0.863	
	KNN	0.953	**0.824**	0.714	0.472	0.495	0.853	
	AdaBoost	0.278	0.29	0.162	0.2	0.16	0.3	
	LDA	0.14	0.16	0.183	0.152	0.122	0.41	
	XGB	0.981	0.785	0.791	0.599	0.489	0.893	
	RNN	0.9425	0.7568	0.8175	**0.6331**	0.5141	0.9045	
	Ours	**0.9882**	0.821	**0.8259**	0.612	**0.517**	**0.913**	
EEG-S	**Jayarathne [15]**	0.967	0.891	0.855	0.678	0.693	0.898	**0.9989 (Delta)**
	Bashar et al. [4]	0.903	0.836	0.537	0.559	0.612	0.775	
	Keshishzadeh et al. [17]	0.928	0.832	0.732	0.611	0.589	0.801	
	SVM	0.216	0.167	0.148	0.169	0.186	0.652	
	RF	0.972	0.885	0.819	0.823	0.87	0.957	
	KNN	0.974	0.865	0.781	0.559	0.743	0.936	
	AdaBoost	0.32	0.32	0.27	0.23	0.22	0.34	
	LDA	0.186	0.17	0.28	0.168	0.162	0.6618	
	XGB	0.9972	**0.982**	0.967	0.959	0.953	0.989	
	RNN	0.9981	0.9667	0.964	0.947	0.952	0.9886	
	Ours	**0.9989**	0.972	**0.968**	**0.961**	**0.955**	**0.99**	

regards by collecting EEG data from 8 subjects across 3 separate trials. However, there is scope to undertake more extensive evaluations in this regard.

- EEG signals are known to be sensitive to various factors such as the mood of the subject, intake of foods, drugs and alcohol. Knyazev [20] infers that EEG signals are affected by inherent factors such as panic, sustained pain, sexual arousal, etc. Dubbelink et al. [9] conduct experiments in obese and lean female adolescents and record the magnetoencephalographic (MEG) signal of participants' brain. The obese adolescents had increased synchronization in delta and beta frequency bands compared to lean controls.

Reid et al. [30] claim that the increase of delta power during the first 5 min following cocaine was correlated with increased ratings of cocaine craving. Reward-related decrease of delta activity has been observed after administration of legal psycho-active drugs, such as alcohol [33], tobacco [19], and caffeine [13]. One future scope of our future work is to study how the identification system is influenced by the aforementioned factors and enhance the current approach to be more adaptive.

- The impact of population size on the performance needs further investigation. In this paper, explore this effect to some extent but considering a corpus of 20 subjects. However, further investigations with larger groups, for example, 100 subjects, are necessary. That said, our results already demonstrate that MindID can be used in settings such as small offices which are accessed by a small group of people.
- The EEG data of an individual is known to change gradually with environmental factors such as age, mental state and lifestyle. For example, Delta patterns are known to decrease with age in older individuals [10]. This suggests that the pre-trained model used in MindID should be updated when such changes are detected. In our future work, we aim to develop an online learning system which can automatically retrain the model using the data collected during the operational phase.
- While we provide some explanations in Section 3 for why Delta patterns may be most informative for user identification, the underlying mechanism is still not well known. Further investigation is necessary.
- The privacy of pervasive EEG technology is not concerned in this paper. The collected EEG data may not only contain subject ID related information but also infers other privacy of the subject (e.g., emotion and fatigue state). In our future work, we attempt to propose an algorithm to eliminate other private information in the collected EEG data.

7 CONCLUSION

We proposed a biometric EEG-based identification approach called MindID and argue that its inherent resilience against attacks makes it an attractive approach compared to traditional biometric identification methods. We decomposed EEG signal into various constituent frequency bands and demonstrate that the Delta patterns capture the most distinguishable features for user identification. MindID incorporates four key steps. Following pre-processing, the EEG data is decomposed into Delta patterns, which are fed to an attention-based RNN structure for extracting deeper representations of the identifiable features. Finally, a statistical boosting classifier is used to identify the individual. The proposed approach is evaluated over 3 datasets (two local and one public dataset). The experiments results illustrate that our model achieves accuracy of 0.982, 0.9882, and 0.9989, respectively. The results also infer the robustness and adaptability of our model. We also outline several directions for future research.

Taking the advantages of EEG-based techniques for attack-resilient, we propose a biometric EEG-based identification approach to overcome the limitations of traditional biometric identification methods. We analyzed the EEG data pattern characteristics and capture the Delta pattern which takes the most distinguishable features for user identification. Based on the pattern decomposition analysis, we report the structure of the proposed approach. In the first step of identification, the preprocessed EEG data is decomposed into Delta pattern. Then an attention-based RNN structure is employed to extract deep representations of Delta wave. At last, the deep representations are used to directly identify the user' ID. The proposed approach is evaluated over 3 datasets (two local and one public dataset). The experiments results illustrate that our model achieves the accuracy of 0.982, 0.9882, and 0.9989 over three datasets, separately. The results also infer the robustness and adaptability of our model. We also outline several directions for future research.

REFERENCES

[1] Jimmy Ba, Volodymyr Mnih, and Koray Kavukcuoglu. 2014. Multiple object recognition with visual attention. *arXiv preprint arXiv:1412.7755* (2014).

[2] Dzmitry Bahdanau, Jan Chorowski, Dmitriy Serdyuk, Philemon Brakel, and Yoshua Bengio. 2016. End-to-end attention-based large vocabulary speech recognition. In *Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on*. IEEE, 4945–4949.

[3] Erol Başar. 1980. *EEG-brain dynamics: relation between EEG and brain evoked potentials*. Elsevier-North-Holland Biomedical Press.

[4] Md Khayrul Bashar, Ishio Chiaki, and Hiroaki Yoshida. 2016. Human identification from brain EEG signals using advanced machine learning method EEG-based biometrics. In *Biomedical Engineering and Sciences (IECBES), 2016 IEEE EMBS Conference on*. IEEE, 475–479.

[5] William Chan, Navdeep Jaitly, Quoc V Le, Oriol Vinyals, and Noam M Shazeer. 2017. Speech recognition with attention-based recurrent neural networks. US Patent 9,799,327.

[6] Kaixuan Chen, Lina Yao, Xianzhi Wang, Dalin Zhang, Tao Gu, Zhiwen Yu, and Zheng Yang. 2018. Interpretable Parallel Recurrent Neural Networks with Convolutional Attentions for Multi-Modality Activity Modeling. *The International Joint Conference on Neural Networks (IJCNN)* (2018).

[7] Tianqi Chen and Carlos Guestrin. 2016. Xgboost: A scalable tree boosting system. In *Proceedings of the 22Nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 785–794.

[8] Thien Thanh Dang-Vu, Manuel Schabus, Martin Desseilles, Genevieve Albouy, Mélanie Boly, Annabelle Darsaud, Steffen Gais, Géraldine Rauchs, Virginie Sterpenich, Gilles Vandewalle, et al. 2008. Spontaneous neural activity during human slow wave sleep. *Proceedings of the National Academy of Sciences* 105, 39 (2008), 15160–15165.

[9] Kim TE Olde Dubbelink, Abraham Felius, Jeroen PA Verbunt, Bob W Van Dijk, Henk W Berendse, Cornelis J Stam, and Henriette A Delemarre-van de Waal. 2008. Increased resting-state functional connectivity in obese adolescents; a magnetoencephalographic pilot study. *PLoS One* 3, 7 (2008), e2827.

[10] Derya Durusu Emek-Savaş, Bahar Güntekin, Görsev G Yener, and Erol Başar. 2016. Decrease of delta oscillatory responses is associated with increased age in healthy elderly. *International Journal of Psychophysiology* 103 (2016), 103–109.

[11] Geof H Givens, J Ross Beveridge, Yui Man Lui, David S Bolme, Bruce A Draper, and P Jonathon Phillips. 2013. Biometric face recognition: from classical statistics to future challenges. *Wiley Interdisciplinary Reviews: Computational Statistics* 5, 4 (2013), 288–308.

[12] Qiong Gui, Zhanpeng Jin, and Wenyao Xu. 2014. Exploring EEG-based biometrics for user identification and authentication. In *Signal Processing in Medicine and Biology Symposium (SPMB), 2014 IEEE*. IEEE, 1–6.

[13] D Corydon Hammond. 2003. The Effects of Caffeine on the Brain: A Review. *Journal of Neurotherapy* 7, 2 (2003), 79–89.

[14] Thalía Harmony. 2013. The functional significance of delta oscillations in cognitive processing. *Frontiers in integrative neuroscience* 7 (2013), 83.

[15] Isuru Jayarathne, Michael Cohen, and Senaka Amarakeerthi. 2016. BrainID: Development of an EEG-based biometric authentication system. In *Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual*. IEEE, 1–6.

[16] Dan H Kerem and Amir B Geva. 2017. Brain state identification and forecasting of acute pathology using unsupervised fuzzy clustering of EEG temporal patterns. In *Fuzzy and neuro-fuzzy systems in medicine*. CRC Press, 19–68.

[17] Sarineh Keshishzadeh, Ali Fallah, and Saeid Rashidi. 2016. Improved EEG based human authentication system on large dataset. In *Electrical Engineering (ICEE), 2016 24th Iranian Conference on*. IEEE, 1165–1169.

[18] Diederik Kingma and Jimmy Ba. 2014. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980* (2014).

[19] Verner Knott, Meaghan Cosgrove, Crystal Villeneuve, Derek Fisher, Anne Millar, and Judy McIntosh. 2008. EEG correlates of imagery-induced cigarette craving in male and female smokers. *Addictive behaviors* 33, 4 (2008), 616–621.

[20] Gennady G Knyazev. 2012. EEG delta oscillations as a correlate of basic homeostatic and motivational processes. *Neuroscience & Biobehavioral Reviews* 36, 1 (2012), 677–695.

[21] Pinki Kumari and Abhishek Vaish. 2015. Brainwave based user identification system: A pilot study in robotics environment. *Robotics and Autonomous Systems* 65 (2015), 15–23.

[22] Neal S Latman and Emily Herb. 2013. A field study of the accuracy and reliability of a biometric iris recognition system. *Science & Justice* 53, 2 (2013), 98–102.

[23] Pengchao Li, Liangrui Peng, Junyang Cai, Xiaoqing Ding, and Shuangkui Ge. 2017. Attention Based RNN Model for Document Image Quality Assessment. In *Document Analysis and Recognition (ICDAR), 2017 14th IAPR International Conference on*, Vol. 1. IEEE, 819–825.

[24] xiaoli Li. 2016. Signal Processing in Neuroscience. Springer, 8–12.

[25] Minh-Thang Luong, Hieu Pham, and Christopher D Manning. 2015. Effective approaches to attention-based neural machine translation. *arXiv preprint arXiv:1508.04025* (2015).

[26] Dennis McGinty, Ronald Szymusiak, and Darrell Thomson. 1994. Preoptic/anterior hypothalamic warming increases EEG delta frequency activity within non-rapid eye movement sleep. *Brain research* 667, 2 (1994), 273–277.

[27] Johannes Müller-Gerking, Gert Pfurtscheller, and Henrik Flyvbjerg. 1999. Designing optimal spatial filters for single-trial EEG classification in a movement task. *Clinical neurophysiology* 110, 5 (1999), 787–798.

[28] David Ormerod. 2017. Sounding out expert voice identification. *Expert Evidence and Scientific Proof in Criminal Trials* (2017).

[29] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. 2013. Attack detection and identification in cyber-physical systems. *IEEE Trans. Automat. Control* 58, 11 (2013), 2715–2729.

[30] Malcolm S Reid, Frank Flammino, Bryant Howard, Diana Nilsen, and Leslie S Prichep. 2006. Topographic imaging of quantitative EEG in response to smoked cocaine self-administration in humans. *Neuropsychopharmacology* 31, 4 (2006), 872.
[31] Robert NS Sachdev, Nicolas Gaspard, Jason L Gerrard, Lawrence J Hirsch, Dennis D Spencer, and Hitten P Zaveri. 2015. Delta rhythm in wakefulness: evidence from intracranial recordings in human beings. *Journal of neurophysiology* 114, 2 (2015), 1248–1254.
[32] Fahreddin Sadikoglu and Selin Uzelaltinbulat. 2016. Biometric Retina Identification Based on Neural Network. *Procedia Computer Science* 102 (2016), 26–33.
[33] Araceli Sanz-Martin, Miguel Ángel Guevara, Claudia Amezcua, Gloria Santana, and Marisela Hernández-González. 2011. Effects of red wine on the electrical activity and functional coupling between prefrontal–parietal cortices in young men. *Appetite* 57, 1 (2011), 84–93.
[34] Gerwin Schalk, Dennis J McFarland, Thilo Hinterberger, Niels Birbaumer, and Jonathan R Wolpaw. 2004. BCI2000: a general-purpose brain-computer interface (BCI) system. *IEEE Transactions on biomedical engineering* 51, 6 (2004), 1034–1043.
[35] Javad Sohankar, Koosha Sadeghi, Ayan Banerjee, and Sandeep KS Gupta. 2015. E-bias: A pervasive eeg-based identification and authentication system. In *Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks*. ACM, 165–172.
[36] Mircea Steriade. 1991. Alertness, quiet sleep, dreaming. In *Normal and Altered States of Function*. Springer, 279–357.
[37] Kavitha P Thomas and A Prasad Vinod. 2016. Utilizing individual alpha frequency and delta band power in EEG based biometric recognition. In *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*. IEEE, 004787–004791.
[38] JA Unar, Woo Chaw Seng, and Almas Abbasi. 2014. A review of biometric technology along with trends and prospects. *Pattern recognition* 47, 8 (2014), 2673–2688.
[39] Bingning Wang, Kang Liu, and Jun Zhao. 2016. Inner attention based recurrent neural networks for answer selection. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, Vol. 1. 1288–1297.
[40] Feng Wang and David MJ Tax. 2016. Survey on the attention based RNN model and its applications in computer vision. *arXiv preprint arXiv:1601.06823* (2016).
[41] Kyoko Yoshida, Xiaodong Li, Georgina Cano, Michael Lazarus, and Clifford B Saper. 2009. Parallel preoptic pathways for thermoregulation. *Journal of Neuroscience* 29, 38 (2009), 11954–11964.
[42] Xiang Zhang, Lina Yao, Chaoran Huang, Sen Wang, Mingkui Tan, Guodong Long, and Can Wang. 2018. Multi-modality Sensor Data Classification with Selective Attention. In *The 27th International Joint Conference on Artificial Intelligence, IJCAI-18*. 3111–3117.
[43] Xiang Zhang, Lina Yao, Dalin Zhang, Xianzhi Wang, Quan Z Sheng, and Tao Gu. 2017. Multi-person brain activity recognition via comprehensive eeg signal analysis. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (Mobiquitous,2017)*. ACM.

Received November 2017; revised May 2018; accepted September 2018