Computers & Security 93 (2020) 101788

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A survey on methods and challenges in EEG based authentication

Amir Jalaly Bidgoly[a,*], Hamed Jalaly Bidgoly[b], Zeynab Arezoumand[a]

[a] Department of Information Technology and Computer Engineering, University of Qom, Iran
[b] School of Electrical and Computer Engineering, University of Tehran, Iran

ARTICLE INFO

Article history:
Received 13 October 2019
Revised 21 January 2020
Accepted 10 March 2020
Available online 11 March 2020

Keywords:
EEG
Biometric factor
Authentication
User identification
Pattern recognition
Survey

ABSTRACT

EEG is the recording of electrical activities of the brain, usually along the scalp surface, which are the results of synaptic activations of the brain's neurons. In recent years, it has been shown that EEG is an appropriate signal for the biometric authentication and has important features such as resistance to spoofing attacks and impossibility to use under pressure and coercion states. In this paper, the state-of-the-art methods in EEG based authentication are reviewed. This review includes a number of aspects such as the various tasks that the user required to perform during the authentication, devices and available datasets, the preprocessing procedures and the classification methods used in the EEG biometric authentication. Both shallow and deep classification methods are reviewed in this paper. The study shows that the deep learning approaches which are used in the past few years, although still require further research, have shown great results. Moreover, the paper summarizes the works to address the open challenges of this area. The EEG authentication challenges have been discussed from a variety of points of view, including privacy, user-friendliness, attacks, and authentication requirements such as universality, permanency, uniqueness, and collectability. This paper can be used as a preliminary plan and a roadmap for researchers interested in EEG biometric.

1. Introduction

In computer science and cryptography protocols, authentication is defined as the act of confirming the claimed identity of a subject. Authentication is a critical tool to manage access to physical or digital resources such as buildings, rooms or computing devices. One of the most important approaches for user authentication is the use of unique biological characteristics of the human being. Different biometric factors are provided for this purpose, which encompass almost many aspects of human being which can be monitored and processed by the computer systems, such as fingerprint, palm, iris, voice, etc. In particular, researchers have special attention to the use of biometric signals such as EEG, ECG, and EMG as an appropriate tool of biometric authentication (Abbas et al., 2015; Blasco et al., 2016). These signals have distinguished advantages over other biometrics; for example, they are more robust against spoof attacks.

Among the biometric signals, "*electroencephalogram*" (EEG) has gained more interest. EEG biometric has unique advantages which make it prominent between other biometric factors, such as:

- Biometric factors such as fingerprints or iris may be forged or imitated. For instance, researchers show that an intruder can simply make a fake fingerprint by just having a picture of one's finger (Galbally et al., 2013). However, unlike the other biometric factors, EGG is not exposed to the intruder which makes it uncapturable and thus, hard to be forged (Ruiz-Blondet et al., 2016).
- EEGs are emotional state dependent and stress or fear changes the normal brain waves' patterns regardless of the activity. As a result, EGG biometric cannot be invoked under force and coercion situations, while in the other authentication methods, even in the challenge-based response ones, an adversary may access to a system by force or threatening the user.
- In the other biometrics, one may use a dead (and warm) body to authorize his/her access to the system. However, for EGG biometric, a dead brain does not produce EEG signals. Hence, EEG itself guarantees that the user is alive and authenticating by his own.

EEG based authentication has many applications in many fields of computer science (Yang et al., 2018) and it can be used as a tool to enhance the security of computer systems. For instance, Klonovs et al. reported the development of a mobile application that increases the security of smartphones through implementing two-step authentication, by combining traditional methods of au-

[*] Corresponding author.
E-mail address: jalaly@qom.ac.ir (A. Jalaly Bidgoly).

https://doi.org/10.1016/j.cose.2020.101788
0167-4048/© 2020 Elsevier Ltd. All rights reserved.

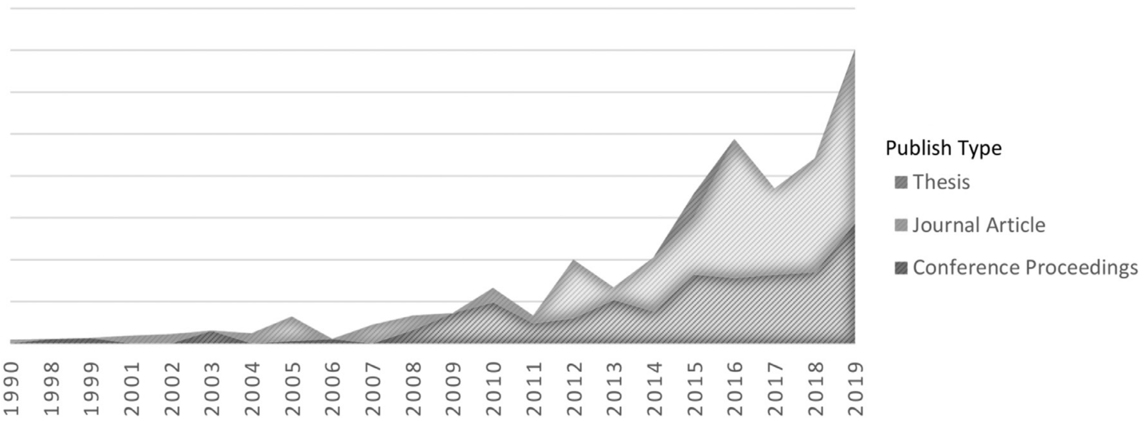

Fig. 1. Number of documents published about EEG based authentication.

thentication and an EEG based one (Klonovs et al., 2013). Apart from conventional authentication applications, some applications have gained particular interest to use this biometric factor. "*Brain computer interface*" (BCI) is an outstanding example here (Lin et al., 2017; Ramzan and Shidlovskiy, 2018). BCI is a try to make direct communication gateway between a human brain and a device. The human may control an electronic device not only by sending explicit commands but also by his or her brainwaves. Integrating BCI and EEG based authentication makes these applications not only execute the user commands but also recognize his/her identity before executing. Since BCI is based on brainwaves, EEG biometric is the best candidate as an authentication factor in this application. EEG may also have other security usages than authentication. As an example, researchers have shown that these signals can be used to generate a cryptographic key (Nguyen et al., 2017; Ravi et al., 2008). The generated key is unique for each person and task and is more robust to attacks as compared to other encryption systems (Ravi et al., 2008).

Considering the advances in the development of portable medical devices, including EEG headset, as well as the unique advantages of EEG, this biometric gains significant interest in recent years. Fig. 1 represents documents published in the context of EEG based authentication. Rapidly growing publications in recent years show the increasing interest of the researchers in this field. Besides, the industries have shown their interest in using it in their products. For instance, trending companies, like NeuroSky, are doing research (Eeg headsets and the rise of passthoughts, 2017) and designing sensors Eeg - electroencephalogram - bci in this field. Moreover, researchers are working on EEG wearable systems using gears from Emotiv and NeuroSky, and even Google Glass (Moore, 2016).

An EEG based authentication system requires several steps. At first, the user should perform a specific task while the system records his/her EEG signals. The signals then have to be prepossessed to enhance its quality. After preprocessing, the enhanced signals are used to train a classifier. Traditionally, shallow classifiers such as "*Support Vector Machine*" (SVM) and "*k-nearest neighbors*" (KNN) have been used for this aim, but in recent years many of them are replaced by deep learning approaches. To use shallow models, it is necessary to extract different features of the signals, and then the model can be trained on them; while in deep learning approach, the feature extraction is not required as an extra step and the model can be directly trained on the preprocessed data.

In this paper, the state-of-the-art research in different aspects of biometric authentication systems has been reviewed. The paper continues as follows. In the next section, the characteristics of brain signals and also methods of data acquisition are presented. In Section 3, the properties of the EEG as an authentication tool are studied. The available datasets in this field are reviewed in Section 4. The Section 5 represents the various tasks that can be performed during EEG recording. Section 6 looks at how the signals can be enhanced by preprocessing. Shallow and deep models in EEG biometric are discussed in Sections 7 and 8, respectively. Section 9 discusses about the security and privacy of EEG biometric. Finally, the paper ends with a review of the open challenges and the conclusion accordingly in Sections 10 and 11.

2. Background of EEG

EEG is the recording of electrical activities of the brain, usually along the scalp surface. These electrical activities are results of ionic current flows caused by the synchronized synaptic activation of the brain's neurons (Niedermeyer and da Silva, 2005) and reveal as rhythmic voltage fluctuations that range from 5 to 100μV in amplitude and between 0.5 and 40 Hz in frequency. Analyzing the dominant frequencies and amplitude of EEG waveforms in the different parts of brains can provide some clues about the physical or the mental state of the person(Bickford, 1987; Sanei, 2013). Based on the frequency, brain waves are classified into the five frequency bands as follows(Sanei and Chambers, 2013):

Delta ($1-4$**Hz**) is the slowest and usually the highest waveform in amplitude. The delta band is observed in babies and during deep sleep in adults;

Theta ($4-8$**Hz**) is observed in the children, drowsy adults and during memory recalling(Klimesch, 1996). The amplitude of Theta waves is normally less than 100μV;

Alpha ($8-12$**Hz**) is usually the dominant frequency band and appears during relaxed awareness or when eyes are closed. Focused attention or relaxation with opening eyes reduces the amplitude of the Alpha band. These waves are normally less than 50μ V;

Beta ($12-25$**Hz**) is associated with thinking, active concentration and focused attention. Also, executing body movements or seeing other's body movements increases Beta power(Zhang et al., 2008). The amplitude of Beta waves is normally less than 30μV;

Gamma (**over** 25**Hz**) is observed during multiple sensory processing(Read and Innis, 2017). Gamma patterns have the lowest amplitude.

In addition to the function-frequency relations, it is also believed that each part of the brain is responsible for doing a specific physical or mental function. Consequently, for studying brain waves of each desired task, not only analyzing the dominant frequency but also recording from the corresponding part of the brain

Table 1
Functions associated to different parts of the brain(Demos, 2005).

Region	Local channels	Functions
Frontal Lobe	Fp1, FP2, FPz, Pz, F3, F7, F4, F8	Memory, concentration, emotions.
Parietal Lobe	P3, P4, Pz	Problem Solving, attention, grammar, sense of touch.
Temporal Lobe	T3, T5, T4, T6	Memory, face recognition, hearing, word recognition, social clues.
Occipital Lobe	O1, O2, Oz	Reading, vision.
Cerebellum	–	Motor control, balance.
Sensorimotor Cortex	C3, C4, Cz	Attention, mental processing, fine motor control, sensory integration.

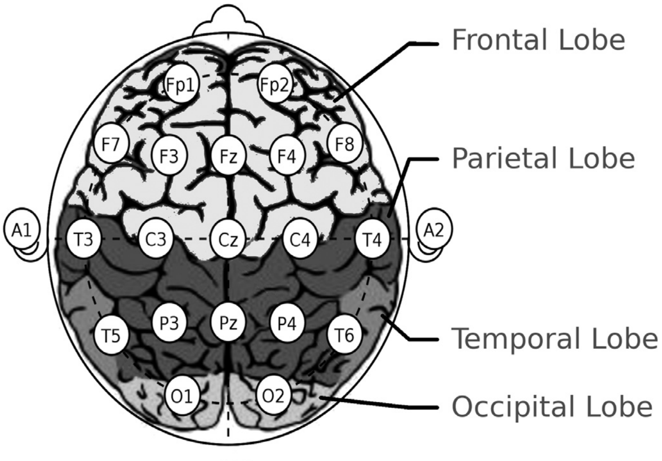

Fig. 2. Electrode placement in the 10–20 standard and the corresponding brain lobes under each electrode.

should be more attended. Functions that are associated to each part of brain, are summarized in Table 1 (Demos, 2005).

To capture the EEG signals, low impedance electrodes are attached to the scalp to pick up electric potentials generated by the brain activities. The electrodes can be placed via conductive gel, namely *wet electrode*, or be directly contacted with skin, namely *dry electrode*. Typically, dry electrodes are easier to attach, however, they are more sensitive to the motion artifacts. There are some standards to locate and label the electrodes on the scalp; e.g., 10–20 standard(Demos, 2005). In the 10–20 standard, the electrodes are placed at 10% and 20% points along lines of longitude and latitude, respectively, and labeled according to the attached lobe. Besides, odd numbers are assigned to the electrodes on the left hemisphere, and even numbers are assigned to the electrodes on the right one; see Fig. 2.

There are both off-the-shelf clinical and commercial products in the market for recording EEG signals. The commercial products are often designed as a headset for ease of use. These EEG headsets are not only capable of capturing user's EGG, but also offering developer toolkits that can detect emotions, attention or simple BCI commands which makes them much easier to use in practice. Emotiv and Neurosky companies are the leading ones in these products. As an example, “Emotiv Epoc+” headset (Fig. 3a) can capture AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8 and AF4 channels using 14 embedded wet electrodes with 2048Hz sampling rate. “Mindwave” headset (Fig. 3b) is another sample provided by Neurosky. These devices have been used in various papers to manually collect the required EEG data.

3. EEG as a biometric authentication factor

The authentication process is usually performed based on some previously known and unique information about the user which are named as “*authentication factors*”. Generally, there are three types of authentication factors:

1. **Knowledge factor**: the information which just the user *knows*,
2. **Ownership factor**: the object which just the user *has/owns*, and
3. **Biometric factor**: the physiological or behavioral characteristics which just the user *is*.

The last one includes the biological aspects of a human, covering a wide range of elements from fingerprint to biometric signals and DNA. The biometric factors have many unique advantages over the other authentication factors. For instance, they are not required to carry with, they cannot be stolen like the ownership factors, and they are not required to be memorized like the knowledge factors. Hence, the biometric factors bring the most comfort authentication methods for the users.

Every biometric factor should have a set of requirements to be appropriate for the authentication purpose. These requirements are 1) universality, 2) permanency, 3) uniqueness, and 4) collectability (Armstrong et al., 2015; Jain et al., 2004). Universality means that each biometric feature, which is considered as an authentication factor, should be capable of being used for every person (not only for a group of people with a specified set of assumptions). Permanency indicates that the biometric factor should be stable over time. Uniqueness requires that the biometric factor be distinguishable for every different user. Finally, collectability refers to the requirement that each biometric factor should be easily collected from the user. In literature, it seems that EEG satisfies all the requirements. It could easily be collected from everyone by a low-cost EEG headset, and a set of features can be extracted from it which is unique for each individual. Also, papers show that the features are quite stable over time. In the Section 10, we will revisit these requirements and discuss the state-of-the-art and challenges of the research in achieving them.

As mentioned before, constructing an EEG based authentication system requires several steps. Usually, the user should be calm and perform a pre-defined task with a specific protocol. These tasks are defined in such a way that bring the brain into action, but do not require movement of the other parts of the body. Instances of these tasks are singing a song in mind, imagining exercise of a sport, thinking of a particular keyword, or simply resting. The authentication system records the user EEG signals through a portable and commercially available EEG headset. These signals are initially pre-processed to enhance their quality and then used to train a classifier. Please note that we should distinguish between “*user identification*” and “*user authentication*” (which often the papers mistakenly used them instead of each other). The identification process deals with the question of who the user is, but the authentication method is to prove or disprove the user's claimed identity by considering a given statistical property. In the former, each user is modeled as a separate class and the model tries to identify the user's class by receiving his/her EEG records. In the latter, a binary classifier is used only for admission or rejection of the claimed identity. In this case, the model receives an individual identity and the recorded EEG signals and then predicts if the records belong to the given identity. In both cases, an initial recording of the EEG should be used to train the classifier, namely “*registration phase*”. After the initial training of the model, the user will be able to authenticate/identify himself to the system in the

(a) Emotiv Epoc+ headset, (b) Neurosky Mindwave headset,

Fig. 3. Commercial EEG headsets.

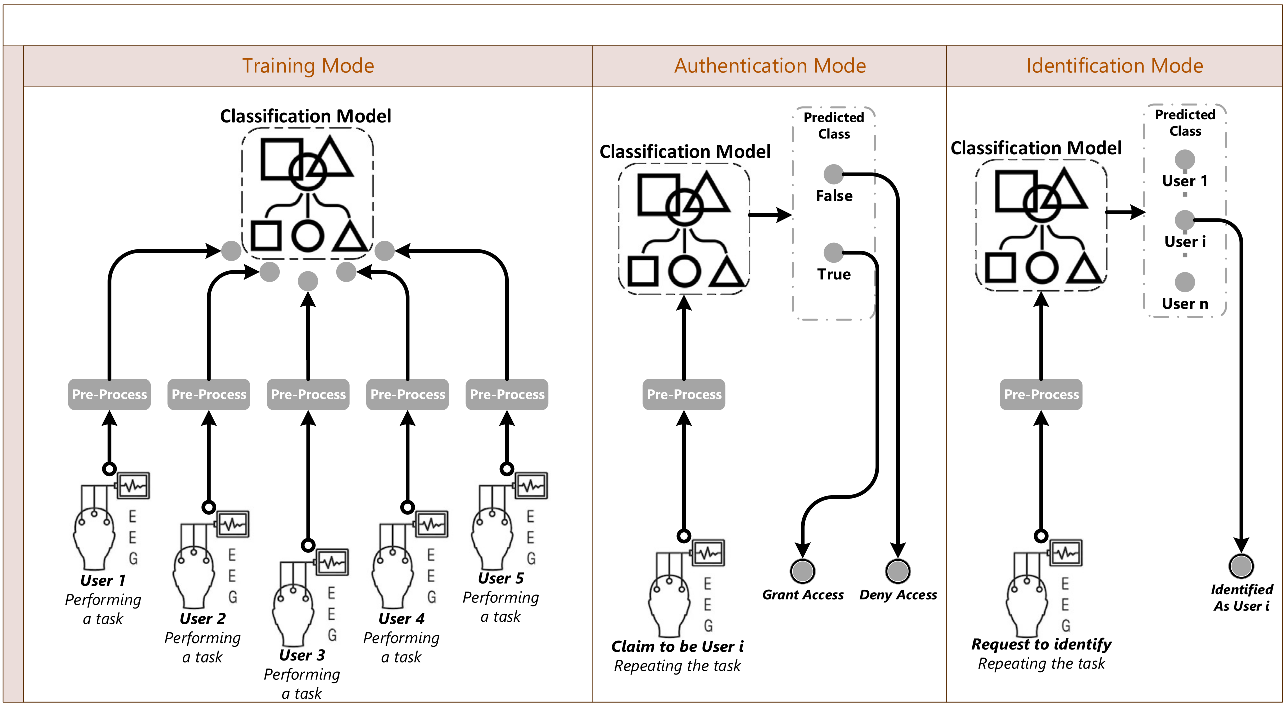

Fig. 4. The process of EEG-based authentication.

"*enrollment phase*". To this end, he must repeat exactly the task that he performed during the initial recording. This new record is then processed and classified by the model and based on the classifier type, the identity of the user is detected in the identification or confirmed in the authentication. In other words,the model determines that *who* is enrolled in the identification or *who that gives statistical property* is the same as the claimed identity in the authentication. The overall process of authenticating using EEG is presented in Fig. 4.

4. Available datasets

In this section, the public datasets that are mostly used in the EEG authentication are reviewed.

4.1. Physionet EEG motor movement/imagery dataset

Physionet EEG Motor Movement/Imagery dataset (Goldberger et al., 2000) is one of the most popular and publicly available datasets produced by the BCI2000 system (Schalk et al., 2004). This dataset includes EEG records from 109 healthy volunteers who performed various Motor/Imagery tasks. EEG signals were recorded by using 64 channels with the sampling rate of 160Hz. Each subject performed 14 experimental runs: two one-minute baseline runs (one with eyes opened, one with eyes closed), and three two-minute runs of each of the four following tasks: open and close left or right fist, imagine opening and closing left or right fist, open and close both fists or both feet, and imagine opening and closing both fists or both feet.

Due to the number of subjects and sampling channels, as well as the diversity of tasks, this dataset attracts the attention of researchers and has been used in many works including (Delpozo-Banos et al., 2015; Kang et al., 2018; Keshishzadeh et al., 2016; Kim and Kim, 2019; Lan Ma et al., 2015; Sun et al., 2019; Thomas and Vinod, 2018; Wang and Najafizadeh, 2016), to name but a few.

4.2. BCI competition III dataset

This dataset, which itself is made up of a set of different datasets, is provided by the cooperation of a team of universities and laboratories such as Graz University of Technology, University OF TÜBINGEN and Berlin BCI group. Datasets include EEG records of one to five subjects performing different tasks. For instance, IIIa as one of these datasets is the EEG records of 3 subjects (named K3b, K6b, and L1b) that were recorded with 250Hz sampling rate using the Neuroscan amplifier with 62 EEG channels (60 electrodes + 2 reference electrodes). In the experiments, the subjects performed 60 trails of the imagination of the movement of 4 body parts according to a cue, including left hand, right hand, foot, and tongue. These datasets are used by various research (Bao et al., 2009; Hu, 2009; 2010; Jian-feng, 2009; Nguyen et al., 2017; Xiao and Hu, 2010).

4.3. BCI competition IV datasets

In continue to BCI competitions, the fourth BCI competition was held in 2008 with 5 different datasets. These datasets include more subjects and tasks. For example, Dataset 2a (Brunner et al., 2008), as one of these datasets, contains EEG signals from 9 subjects recorded using 22 EEG channels and 3 EOG channels with the sampling rate of 250Hz. Subjects performed four different tasks including the imagination of the movements of the left hand, the right hand, both the legs and the tongue. The experiments were recorded in two sessions on different days for each subject. Each session contains 6 runs that were separated by short breaks. These datasets have also been used by various papers (Lawhern et al., 2018; Schirrmeister et al., 2017).

4.4. UCI KDD EEG database

The records of this dataset (Begleiter et al., 2002) are obtained by 64 electrodes at a sampling rate of 256 Hz. The number of subjects was 122 including normal and alcoholic males. In experiments, each person was exposed to visual stimuli, including black and white images from the Snodgrass and Vanderwart collection (Snodgrass and Vanderwart, 1980). The experiments included two stimulants S1 and S2, each showing for 300 ms and separating within 1.6 seconds. The subjects were asked to determine if S1 complies with S2 or not. In some cases, only one trigger was provided. Liew et al. (2015) and Delpozo-Banos et al. (2015) are some examples of papers which are used this dataset in their works.

4.5. Australian EEG database

Australian EEG database (Hunter et al., 2005) is a result of an 11-year study (1991–2002) on EEG signals of 40 patients (20 males and 20 females) at John Hunter Hospital. The EEG was recorded with open eyes and closed eyes for about 20 min, using 23 electrodes at a sampling rate of 167 Hz. This dataset is used in several research (Hunter et al., 2005; Nguyen et al., 2012; 2013; Phung et al., 2014).

4.6. DEAP

The DEAP dataset (Koelstra et al., 2012) is a famous and well-known dataset in emotion detection studies, however, it is also used for EEG authentication in some works (Delpozo-Banos et al., 2015; Pham et al., 2015; Vahid and Arbabi, 2016; Wilaiprasitporn et al., 2019). EEG samples were collected from 32 healthy subjects using 32 channels with 512 Hz sampling rate. For each one, 40 one-minute videos were played, where each one rises a specific emotion of the subject such as pride, joy, satisfaction, hope, sadness, and fear.

4.7. Other datasets

Aside from the datasets mentioned above, there are other available data collections in this field that are less well-known. Keirn and Aunon dataset (Keirn and Aunon, 1990) is a small and old database containing EEG from 5 individuals (4 males and 1 female between the ages of 21 and 48), which is recorded by 6 channels and the sampling rate of 250 Hz. The tasks defined in this dataset are interesting and unique. Each user had to do five mental tasks, including silently rest, solving a complex multiplication without physical motion, silently imagining the rotation of a three-dimensional object around an arbitrary axis, visualizing numbers on an imaginary backboard, and writing a mail to a friend in mind.

Several datasets have also been introduced in recent years. Sockeel et al. (2016) published a dataset including 11 subjects' EEG recorded by a 62 channels BrainAmp cap in 2016. In 2017, Kaur et al. (2017) have published a dataset containing brain signals of 60 different subjects while listening to four different types of music including devotional, electronic, classical and rock. Their main goal was to examine the impact of different emotions on EEG based identification systems.

5. EEG acquisition protocols

In general, protocols used in the EEG recording can be categorized into three groups: resting states, mental tasks, and tasks with an external stimulus. The selected protocol can affect the procedure or the accuracy of authentication. For instance, the resting states or the mental tasks do not require any extra equipment but EEG recording devices; while, tasks followed by external stimuli

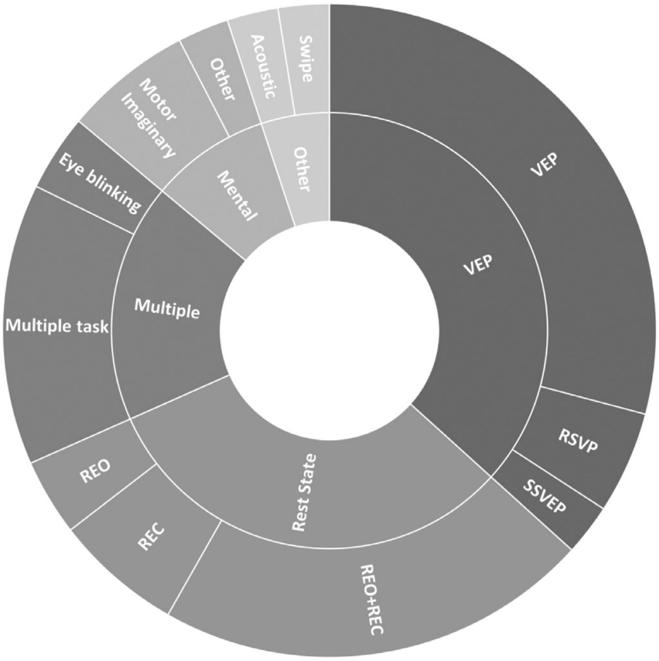

Fig. 5. Distribution of different EEG acquisition protocols in the EEG authentication.

require some devices to create the appropriate stimulation. On the other hand, simple tasks like resting states are easily affected by environment noise and artifacts, whereas mental tasks and tasks followed by external stimuli create a higher "*signal-to-noise ratio*" (SNR). This can be achieved by distinguishing "*Event Related Potential*" (ERP) which is an electrical potential generated in the brain in response to any kind of sensori-motor event, external stimulus or mental task(Luck, 2014). Besides, the ERP is time synchronized to the event and lasts to one second. In comparison to other non-biometric authentication methods, ERPs can be categorized into "*challenge-based response*" methods in which user is asked to respond to a system command(Idrus et al., 2013). The other factor that should be considered in the EEG acquisition protocol is that, which part of the brain engages more to execute the desired task. For instance, ERP responses to the visual stimuli are mostly observed in the occipital lobe, visual cortex, and central region. As a result, with some compromising, the electrodes can be reduced to Oz, O1, and O2. In the following, the protocols mainly used in the EEG authentication are described.

5.1. Resting states

Resting states are the most popular protocol in acquiring EEG signals(Di et al., 2019; Kim and Kim, 2019; La Rocca et al., 2014; Nakamura et al., 2017; Poulos et al., 1998; Schons et al., 2018; Waili et al., 2019; Wang and Najafizadeh, 2016). In this protocol, the individual is asked to be completely relaxed, normally sit on a chair, in a quiet environment and then EEG signal is recorded. Although both closed eyes, namely "*REC*", and opened eyes, namely "*REO*", are used in this protocol, there are differences in the dominant frequency band and the more efficient EEG channels. In REO, the best results are achieved from the central region, while with REC, the parietal region does. Besides, α band is dominant band(Barry et al., 2007; La Rocca et al., 2014) during REC. The popularity of this protocol lies in its simplicity. Besides, it does not require any extra requirements or instructions, however, the environment should be quiet and the individual should have no mental activity or preoccupation; otherwise, the results are deflected. Nevertheless, the resting state can be used as a baseline EEG activity for the other tasks in the preprocessing stage.

5.2. Visual stimuli

Visual stimuli, which are also known as "*Visual Evoked Potential*" (VEP), is a group of ERPs that are caused by external visual stimuli. VEPs, in turn, cover a wide range of visual stimuli. In Ruiz-blondet et al. (2014) and Gui et al. (2015), the individual is asked to silently read some unconnected texts including words (e.g. BAG, FISH), pseudo-words (e.g. MOG, TRAT), acronyms (e.g., MTV, TNT), illegal strings (e.g., BPW, PPS) or instances of their own names. In Zuquete et al. (2010) and Abo-Zahhad et al. (2016), a sequence of pictures, which each one is followed by a blank screen, are displayed on a screen for 1–2 s and the individuals are asked to recognize the pictures as soon as they are presented. In some cases, individuals are additionally asked to respond to a rare target picture, by concentrating on or pressing a button, among a large sequence of non-target pictures. The target picture can be a special geometric shape(Das et al., 2015; 2016b), numbers among all characters(Das et al., 2016a; 2016b), moving objects versus stationary objects(Zhang et al., 2018), or a picture already selected by own individual as a password(Liew et al., 2018). "*Rapid Serial Visual Presentation*" (RSVP) is another protocol in which the sequence of infrequent target/frequent non-target pictures are shown sequentially with a high rate, e.g., 2–10 Hz, to minimize the training duration (Chen et al., 2016; Zeng et al., 2019; Zhang et al., 2018). RSVP, in particular, elicits *P300* ERP, that is a special positive peak that appears between 200 – 700ms after an infrequent stimulus(Polich, 2007). It's worth mentioning that the RSVP protocol is also a very common paradigm in the BCI applications(Wang et al., 2018). The other common paradigm between the BCI and the authentication protocols, is periodic visual stimuli leading to "*Steady-State Visual Evoked Potentials*" (SSVEP) that is, a periodic visual stimulus, in the frequency range of 4 to 60 Hz, can induce enhanced stationary periodic oscillations with the same frequency and its higher harmonics in the brain waves recorded over visual areas(Phothisonothai, 2015; Piciucco et al., 2017). This stimulus may be generated by a panel of flickering LEDs. Rate of increasing in the power spectrum of brain frequencies is not only corresponding with stimulation frequency, intensity and duty cycle of flickering, but also varies in different individuals. Despite the simplicity, SSVEPs are useful tools because of the excellent SNR and robustness against artifacts.

The drawback of all VEPs is the need for external devices to create the stimuli and the time synchronization between the stimuli and the EEG recording. However, it is shown that VEP components are very stable over time(Gaspar et al., 2011) and they can satisfy the permanency condition of biometric authentications. Besides, in SSVEP, there is no need to synchronize recording.

5.3. Acoustic stimuli

Acoustic Stimulus is another type of ERP that is emerged by listening to a piece of music or a special tone; though, it is not as common as VEP. In Kaur et al. (2017), four different genres of music were played for individuals in which they induce different emotions and interests. The individuals were also asked to provide music preference which acts as a personal identification mechanism. In Frank et al. (2017), individuals were asked to determine three of their favorite songs. Then, these songs were used to create clips to represent an audio pass-thought.

5.4. Mental task

In the mental tasks, the individual is asked to imagine some physical body movements or do mental activities. For instance, in Marcel and Millan (2007), Hu (2010), Chuang et al. (2013) and Das et al. (2018), the individual should move hand or foot imaginarily or do both imaginary and physical body movement(Alyasseri et al., 2018; Sharma and Vaish, 2016). It is shown that imaginary tasks lead to better results than similar physical ones. In Chuang et al. (2013) and Johnson et al. (2014), the individual was asked to silently sing a favorite song, counting numbers in mind and concentrate on a desired thought as a "*pass-thought*". Doing mental multiplication, visualizing the rotation of a given geometric figure around an axis, counting numbers in mind and composing a letter to a friend are the other instances of mental tasks considered in Kumari and Vaish (2016). Imagine a person, a gesture or taste of a food(Frank et al., 2017) and generation of words beginning with randomly selected letter(Marcel and Millan, 2007) are other sets of mental tasks that individuals are asked to perform.

In comparison to the visual stimuli, although mental tasks do not require special devices for stimulation, they still need some simple equipment to generate a clue for the individual to initialize the task.

5.5. Multi-Tasks

There are some protocols that the EEG is recorded with more than one type of stimulus. For instance, individuals are asked to watch short music videos that induce different emotional states(Chen et al., 2019; Pham et al., 2015; Vahid and Arbabi, 2016). The fusion of both EEG and EOG signals is another multi-model protocol that is used to improve the accuracy of classification(Bhateja et al., 2019).

6. Preprocessing

Similar to any other classifications, the EEG authentication requires some preprocessing on the raw EEG signals to enhance the quality. Preprocessing methods can be categorized into three groups described in the following.

6.1. Frequency domain filtering

As mentioned in Section 2, the brain wave frequencies range from 0.5 to 40Hz. As a result, a band-pass filter is usually applied to the raw signals to filter the lower and higher frequencies. To aim this, "*Butterworth*", as an anti-aliasing infinite impulse response filter, is the most common band-pass filter used in the EEG preprocessing(Alyasseri et al., 2018; Frank et al., 2017; Singh et al., 2015; Thomas et al., 2017). "*Chebyshev*" filter is the other common filter used in the literature(Chen et al., 2016; Zeng et al., 2019). In comparison to Butterworth, Chebyshev filter has sharper cut-off frequency with more ripples. It's worth mentioning that, Butterworth is also used to separate different EEG bands in the feature extraction stage. In some cases, that one desires to keep higher frequencies, a "*Notch*" filter, with stopband frequency of 50 or 60Hz, is applied to the signals to remove the power line artifacts(Abdullah et al., 2010a; Delpozo-Banos et al., 2015); however, it may add some phase distortion.

6.2. Spatial domain filtering

When sufficiently large numbers of electrodes are employed, spatial filters can be used to reduce noise, detect and remove body artifacts, and enhance localized activities. The most common spatial filters used in the EEG biometric are "*Common Average Referencing*" (CAR)(Das et al., 2016a; 2015; Maiorana and Campisi, 2018; Maiorana et al., 2016b; Piciucco et al., 2017), "*Independent Component Analysis*" (ICA) (Arnau-Gonzalez et al., 2017; Maiorana et al., 2016b; Tangkraingkij et al., 2010; Wang and Najafizadeh, 2016), and Laplacian filter (Kostílek and Št'astnỳ, 2012; Marcel and Millan, 2007).

In CAR, the measured potential at each electrode is subjected to the mean of the entire electrodes (McFarland et al., 1997):

$$c^u = v^u - \frac{1}{M}\sum_{i=1}^{M} v^i, \tag{1}$$

where v^u is the raw measured potential of electrode u and M is the number of all electrodes. It makes the signal robust to inappropriate reference choices in mono-polar recordings or unexpected reference variations

ICA is one of the blind source separation techniques in which components identified as eye movements/blinking, background noise, and muscle artifacts can be removed. Indeed, the raw EEG data is considered as a linear combination of multiple sources, including both brain and non-brain activities and external noises, and is modeled as follows(Maiorana et al., 2016b):

$$s = Wx, \tag{2}$$

where x is the measured vector, s is separated sources and W is the transformation matrix. "*Canonical Correlation Analysis*"(Koike-Akino et al., 2016) and "*Empirical Mode Decomposition*" (EMD) (Kumari and Vaish, 2016) are the other source separation techniques.

Laplacian filter is used as a spatial high pass filter that enhances localized activities while suppressing the diffusion ones. Laplacian is calculated by subtracting the sum of weighted potential of the neighborhood electrodes from the current electrode potential as the following(McFarland et al., 1997):

$$v_i^l = v_i^r - \frac{\sum_{j\in S_i} \frac{v_j^r}{d_{ij}}}{\sum_{j\in S_i} \frac{1}{d_{ij}}}, \tag{3}$$

where S_i is set of neighborhood electrodes of i*th* electrode and d_{ij} is the distance between the electrodes of i and j.

6.3. Time domain filtering

We categorize some preprocessing methods that are applied directly on the time series of EEG, as the time domain filters; though, they may have common characteristics with other domains. In the following, these preprocessing methods are briefly introduced.

Ensemble averaging is a simple, but effective, technique that is applied to EEG to not only reduce the noise measurements but also to enhance ERP signals. In general, averaging of multiple trials, recorded with the same protocol, reduces the noise power. In particular, if EEG is recorded after a stimulus presentation, averaging of multiple time-locked ERP responses attenuates the baseline brain activities whereas the peaks of ERPs are amplified. This is a common preprocess to increase the SNR in the ERP-based authentications(Das et al., 2016b; Frank et al., 2017; Gui et al., 2015). Another method to enhance ERPs is baseline removal. Here, the EEG signals are initially measured in the rest state, before presenting stimulus. Then, the mean of this measurement is used to remove baseline activities from the ERPs in either time domain(Chen et al., 2019) or frequency domain(Koelstra et al., 2012). Removing the baseline by considering EEG by its own is also common in the literature. In this type, the EEG is normalized to a dimensionless zero-mean signal with variance one(Das et al., 2016b; Ruiz-Blondet et al., 2016; Zhang et al., 2018). Thresholding is another preprocess method in which spikes above a certain threshold, usually $50\mu V$, are bypassed. Thresholding is used to remove eye-blinking or muscle reflex artifacts (Frank et al., 2017; Sundararajan et al., 2015).

7. Shallow classification

Shallow methods can be considered as two-level processing; extracting some distinguishing features and then applying a classification method on the extracted features. However, by considering the type of signal, the features and classifiers can be completely different in various applications. In the EEG biometric, the input signals are the time series of electrical potential fluctuations recorded from different locations of brain. As a result, features that can be extracted in any of time domain, frequency domain or spatial domains, are mainly useful; e.g., coefficients of *Auto Regressive Model* in the time domain, *Power Spectral Density* in the frequency domain, *Wavelet* coefficients in the time-frequency domain or *common spatial coherence* in the spatial-frequency domain. Similarly, the applied methods should be able to classify these types of features. In the following, the most common feature extraction and classification methods in the EEG authentication are reviewed. It is worth mentioning that in any level, the available methods can be utilized singly or fused together to improve the results. In the feature-level, the features extracted from different methods are fused together directly or by means of some feature reduction tools such as *Canonical Correlation analysis*. In the decision-level, the matching score of different classification methods are fused together to enhance confidence level.

Table 2
Shallow classification works on the EEG Authentication.

Study	Task	Number of subjects	Number of channels	Features	Method	Accuracy (%)
Marcel and Millan (2007)	Imaginary Task	10	8	PSD	Guassian Mixture Model	92.9
Gui et al. (2014)	VEP	32	6	Wavelet	ANN	99.87
Abo-Zahhad et al. (2015)	Eye blinking	10	1	AR	LDA	99.8
Ruiz-Blondet et al. (2016)	VEP	50	26	Template	cross correlation	100
Sharma and Vaish (2016)	Imaginary/ Physical movement	5	1	Gamma band Wavelet	ANN	88
Gui et al. (2015)	VEP	37	4	Template	Euclidean distance	90
Maiorana et al. (2016a)	REO, REC	50	19	AR, PSD, Spectral coherence	Fusion of Manhattan, Euclidean and cosine distances	95
Ruiz-Blondet et al. (2017)	VEP	20	26	template	cross correlation	100
Kaur et al. (2017)	Acoustic ERP	60	14	wavelet	HMM/SVM	97
Maiorana and Campisi (2018)	REC, REO, mental computation	45	19	AR, MFCC, bump representation	HMM	98
Di et al. (2019)	REO,REC	17	20	PSD	Fusion of Euclidean distance, SVM and LDA.	95
Waili et al. (2019)	REO,REC	6	3	Wavelet	ANN	78

7.1. Feature extraction

"*Autoregressive Model*" (AR) is one of the most common methods to extract features in the EEG authentication. In AR model, a time series is modeled as a weighted summation of previous Q samples(La Rocca et al., 2014):

$$x[n] = -\sum_{q=1}^{Q} a_q x[n-q] + w[n], \quad (4)$$

where $w[n]$ is the white noise and $\{a_q\}$ is set of AR coefficients. Consequently, by considering the EEG signal as a dynamic time series, the measured potential activity of each channel can be modeled by an AR. Then, set of coefficients of all channels is used as the feature vector(Abo-Zahhad et al., 2015; Bhateja et al., 2019; Keshishzadeh et al., 2016; La Rocca et al., 2014; Maiorana and Campisi, 2018; Maiorana et al., 2016a; Pham et al., 2014; 2015). AR coefficients can be classified by "*Support Vector Machine*" (SVM) (Keshishzadeh et al., 2016), "*Artificial Neural Networks*" (ANN) (Bhateja et al., 2019), "*Linear Decremental Analysis*" (LDA) (Abo-Zahhad et al., 2015) or similarity based classifiers (Maiorana et al., 2016a). AR extracts EEG features in the time domain.

In some cases, the time series of EEG signals are directly used to generate a "*template*", rather than modeling by AR. The template contains a short period of the processed signal of one or multiple channels(Chuang et al., 2013; Das et al., 2016a; Gui et al., 2015; Kumar et al., 2017; Ruiz-Blondet et al., 2016). The processing includes averaging over trials or filtering frequency bands. Although template generation is significantly less complex than AR modeling, it requires more storage space and consequently, it may not be practical on a large scale dataset or people. Template can be classified by "*Hidden Markov Model*" (HMM) (Kumar et al., 2017), *cosine distance* (Das et al., 2016a) or *cross correlation*(Ruiz-Blondet et al., 2016). Obviously, the template represents the EEGs in the time domain. Another simple, but compact, representation of time domain is the statical characteristics of the time series; e.g., mean, standard deviation or RMS of EEG signal per channel(Kaur et al., 2017; Kumar et al., 2017).

"*Power Spectral Density*" (PSD) is another common feature describing the EEG signals in the frequency domain. Indeed, PSD is the power distribution of different frequencies or different bands. PSD is usually estimated by means of *Discrete Fourier Transform* and *Welch Method*(Di et al., 2019) or *Bartlett Method*(Pham et al., 2014). Here, the feature vector is the augmentation of PSD of all selected channels(Ashby et al., 2011; Di et al., 2019; Maiorana et al., 2016a; Pham et al., 2015) and it can be classified by SVM(Ashby et al., 2011), similarity-based methods(Maiorana et al., 2016a) or LDA(Di et al., 2019).

Regarding the non-stationary nature of EEG signals, "*Wavelet Transform*" (WT) is also widely used as a powerful feature extractor in both time-frequency domains. WT decomposes a signal to a weighted summation of functions, namely *wavelet*, that each one is a shifted and scaled copy of a basic function, namely *mother wavelet*. Each wavelet approximates the signal with a lower resolution. By using Wavelet decomposition, the set of wavelets' coefficients per channel is defined as the feature vector(Alyasseri et al., 2018; Kaur et al., 2017; Sharma and Vaish, 2016) and it can be classified by HMM(Kaur et al., 2017), ANN(Alyasseri et al., 2018) or SVM(Kaur and Singh, 2017). In rather cases, the statical properties of wavelets' coefficients are also used as features; e.g. mean, standard deviation, RMS and entropy(Abdullah et al., 2010b; Kaur and Singh, 2017).

The other less common features introduced in the literature are "*mel-frequency cepstrum coefficients*" (MFCCs) (Maiorana and Campisi, 2018; Piciucco et al., 2017) in the frequency domain, "*sort time*

Fourier transform (STFT) (Phothisonothai, 2015) in the time-spatial domain and "*common spatial coherence*"(Singh et al., 2015) in the spatial-frequency domain.

Finally it's worth mentioning that in many studies, multiple methods are used simultaneously to extract features in different domains; e.g. combination of AR and PSD in Ashby et al. (2011), AR and statical properties in Kumar et al. (2017), AR, PSD, entropy and mutual information in Hu (2010), entropy, mutual information and statical properties in Kumari and Vaish (2016), and AR and MFCC in Maiorana and Campisi (2018). In these cases, the different type of features are fused directly or processed by some features' reduction tools such as "*Principle Component Analysis*" (PCA)(Kaur and Singh, 2017; Palaniappan, 2006) or "*Canonical Correlation Analysis*" (CCA) (Bhateja et al., 2019; Kumari and Vaish, 2016).

7.2. Classification methods

Similarity-based methods are the simplest and the least complex classification approach in which two vectors are compared and labeled as the same class if their similarity score is greater than a pre-defined threshold. Indeed, a feature vector generated in the enrollment phase is compared with the feature vectors generated in the registration phase. Besides, it's mainly used in the authentication, rather than identification. The more common similarity-based methods include "*Euclidean distance*"(Fraschini et al., 2015; Gui et al., 2015), "*cross correlation*"(Ruiz-Blondet et al., 2016; Thomas et al., 2017), "*cosine distance*"(Das et al., 2015), "*Manhattan distance*"(Maiorana et al., 2016a), and "*Dynamic Time Wrapping*" (Das et al., 2016b). These methods can be used to directly compare two templates(Das et al., 2015; Ruiz-Blondet et al., 2016) or the features extracted from different domains(Maiorana et al., 2016a; Piciucco et al., 2017).

"*Support Vector Machine*" is a linear classifier that defines a hyper-plane to separate features of different classes, mostly binary ones, in such a way that maximizes the distances of each class from the hyper-plane. Regarding the binary nature of the authentication, SVM is widely used in the literature as both linear (Ashby et al., 2011; Di et al., 2019; Kaur and Singh, 2017; Keshishzadeh et al., 2016; Kumar et al., 2017) and nonlinear classifier(Vahid and Arbabi, 2016). SVM can be used to classify features extracted from the time domain(Kumar et al., 2017) or the frequency domain(Di et al., 2019).

"*Linear Decremental Analysis*" (LDA) is another linear classifier that can reduce feature dimensions as well by accounting class labels. Therefore, LDA is used where there are so many features with possibility of correlation(Di et al., 2019; Jayarathne et al., 2016) or the features are extracted from different sources(Abo-Zahhad et al., 2015; 2016). LDA can be used to classify AR features(Abo-Zahhad et al., 2015) or PSD features(Di et al., 2019).

"*Hidden Markov model*" (HMM) is widely used to model signals with a temporal dynamic nature, like as EEG. The HMM can be simply defined as a finite set of hidden states with transition probabilities from each state to another one. It is used to directly model time series(Kumar et al., 2017) or to classify features extracted in the time-frequency domains(Kaur et al., 2017; Maiorana and Campisi, 2018).

"*Artificial Neural Network*" (ANN) is a nonlinear classifier that tries to mimic the structures of the human neural system. ANN contains a hidden layer with a nonlinear characteristic that lets it model nonlinear data with more degrees of freedom. Therefore, it can be used not only for the authentication, but also for the classification(Abdullah et al., 2010a; Alyasseri et al., 2018; Bhateja et al., 2019; Hu, 2010; Sharma and Vaish, 2016; Waili et al., 2019).

"*K-Nearest Neighbors*" (KNN) (Chuang et al., 2013; Singh et al., 2015), "*Support Vector Data Description*" (SVDD) (Pham et al., 2015), "*Random Forest*" (RF)(Kaur and Singh, 2017), and "*Gaussian Mixture Model*" (GMM)(Marcel and Millan, 2007) are the other classification methods that are used in the EEG authentication.

Similar to the feature extraction step, again, the classification results of different methods can also be fused to increase confidence level(Abo-Zahhad et al., 2016; Kaur and Singh, 2017; Maiorana et al., 2016a).

8. Deep classification

With the rapidly increasing interest and development of deep learning, many fields of computer science have evolved. The deep learning methods are capable of feature extraction from the raw data. Along with other areas, deep learning has been gained significant interest in many various aspects of EEG processing such as motor imagery classification (Tabar and Halici, 2016), EEG decoding and visualization (Schirrmeister et al., 2017), EEG-based emotion recognition (Yin et al., 2017), and last but not the least EEG-based authentication. Deep learning approaches have significantly increased the accuracy of EEG biometric authentication systems to over 99% even for a set of over 100 people (Sun et al., 2019).

Most of the deep EEG biometric methods proposed in the papers are on the bases of "*Convolutional Neural Networks*" (CNN) models. Das et al. (2018), for example, showed that CNN models are able to reach 99.3% accuracy in the EGG user identification. They used a CNN model with four convolutional layers and two max-pooling layers. Wu et al. (2018) similarly, reached the precision of 97% for EGG collected during a 30-day interval (which is one of the EEG biometric challenges). To overcome the need of deep learning approaches to a huge amount of data, Schons et al. (2018) used data augmentation. By creating overlapped time windows, they were able to increase the training samples to several hundred times. Their proposed method significantly decreased EER compared with the previous works (Fraschini et al., 2015; Yang et al., 2018). Using the adversarial invariant representation learning approach, Zhang et al. (2018) proposed an adversarial convolutional network for the EEG biometric, which can distinguish individual characteristics from the signals recorded during different sessions. In their proposed model, a CNN with four convolutional layers for representing data and two fully connected networks as identifier and adversary were used. Chen et al. (2019) proposed a new convolutional neural network with global spatial and local temporal filters called GSLT-CNN. These works are just some instances to name, and there exist other similar works in the literature. For example, Lan Ma et al. (2015), Schons et al. (2018), and Wu et al. (2018) proposed CNN models, respectively, with two, three, and two different convolutional layers in their works.

The important point in using CNN models is how to model the input data. In most cases, the input is considered as a two-dimensional matrix, one dimension is the sampling channels, and the other dimension is samples collected per channel. Some methods, such as Wu et al. (2018), have chosen a different approach. He defined the input as the matrix of $C \times F$ where C is the channels and F is the voltages averaging in non-overlapping time-windows.

Convolutional neural networks have very good performance with static data, such as photos or a part of the signal, but are not designed to extract information and time features in the time series such as the EEG signals. Hence, various works have been done to use other deep learning methods including "*Recursive Neural Networks*" (RNNs) models for the EEG biometric authentication. RNNs and their family, "*Long Short-Term Memory*" (LSTM) and "*Gated Recurrent Unit*" (GRU), are good tools for extracting time attributes in sequences. Sun et al. (2019) proposed a new neural network based approach combining CNNs and LSTMs, called "*1D-Convolutional Long Short-Term Memory*" (1D-Convolutional-LSTM) for the EEG authentication. This model is more accurate than either CNN or LSTM and is also able to maintain its performance even with the reduction of channels. The authors showed that 1D-Convolutional-LSTM with 16 channels gives 0.71% higher accuracy than the CNN system with 64 channels. Wilaiprasitporn et al. (2019) have also proposed a combination of CNN and RNN networks. Moreover, they reviewed two types of RNN networks, including LSTMs and GRUs. Compared to LSTMs, GRUs are faster to train and require fewer data to generalize, even though they have comparable performance and accuracy. The accuracy obtained in this paper for the CNN-GRU and CNN-LSTM is 99.17% and 98.23%, respectively, on the DEAP dataset.

The works on the EEG authentication based on the deep learning approaches are summarized in Table 3. It should be mentioned that despite the excellent performance of deep learning approaches in the EEG biometric, these methods are not free of problems. For example, Ozdenizci Özdenizci et al. (2019) showed that these methods do not yet have acceptable performance across different sessions.

9. Security and privacy of the EEG biometric

Although EEG based authentication is perceived as a leading technique, it still faces several security and privacy challenges. An EEG biometric can be broken down by an adversary if attacker could generate an input EEG signal which its features are close enough to a target user. The attacker has three different ways of doing this: 1) imitate the victim's brain, 2) brute force the system, 3) sniffing the victim's EEG signals and try to reproduce it. Imitating the victim's brain means that the attacker somehow becomes aware of the victim's thoughts during the registration phase (for example, in the task of imagining the body movement, he knows which part of the body, the user imagines to move) and tries to imitate those thoughts to fool the system and bypass the authentication mechanism. Johnson et al. (2014) had shown that the existence of an imitating attacker in an environment increases the false acceptance rate of the system from 2% to 5%. The error rate might still seem low enough at the first glance, but considering the very limited population size of the study (only 15 subjects), this arises a warning that error may increase unacceptably in larger populations. In another study, it was shown that in the authenticating by the imaginary sport task, the system error would increase from 0% to 17%, if an imitating attacker exists in the environment who is aware of the users' selected sport. This research clearly demonstrates the sensitivity of the imitation attacks' success rate to the chosen task.

Although the studies have not yet proved the high probability of imitation attacks succeeding, by considering the very few studies investigating the imitating attacks (including Johnson et al., 2014; Sohankar et al., 2015), it is still too early to claim the robustness of EEG biometric against these type of attacks. In the current situation, solutions such as locking the user account after several failed attempts are sufficient to prevent the imitating attacker.

The second method that an adversary may use to break the system, is the brute-force attack which is testing every possible EEG as the input with the hope of eventually finding the correct one. The probability of an authentication factor breaking through the brute-force is usually measured by the "*entropy*" metric. Suppose the adversary has a method to generate as many fake EEG signals as required, the entropy of EEG biometric is defined as the binary logarithm ($\log_2 n$) of the average number of the required EEG generated by the adversary to break the authentication system. Sadeghi et al. (2017) showed that EEG biometric entropy is at best 83-bits. This entropy is obtained extracting features using PSD and classifying by a *Naive Bayes Classifier*. The entropy of other methods was significantly lower in their study. For example, the entropy of AR feature extractor and SVM classifier were estimated

Table 3
Deep classification works on the EEG authentication.

Study	Task	No. of subjects	No. of channels	Sample duration	Base model	Layers	Augmentation	Accuracy (%)
Özdenizci et al. (2019)	RSVP	10	16	0.5 s	CNN	4 conv. 2 FC	No	99.30
Wilaiprasitporn et al. (2019)	VEP	32	5	10 s	CNN+LSTM +GRU	3 conv. 2 FC LSTM/GRU	No	99.17
Wu et al. (2018)	RSVP	15	16	3 s	CNN	2 conv. 3 FC	No	97.60
Schons et al. (2018)	REC, REO	109	64	12 s	CNN	3 conv. 4 FC	Yes	99.62
Zhang et al. (2018)	RSVP	15	64	1 s	CNN	2 conv. 1 FC	No	89
Chen et al. (2019)	RSVP	157	28	1 s	CNN	3 conv. 2 FC	No	96
Mao et al. (2017)	Virtual Driving	100	64	1 s	CNN	3 conv. 2 FC	No	97
Arnau-Gonzalez et al. (2017)	VEP	23	14	6 s	CNN	5 conv. 3 FC	No	94
Lan Ma et al. (2015)	REC/REO	10	64	1 s	CNN	2 conv. 1 FC	No	88
Das et al. (2018)	Imaginary Body movement	40	17	0.6 s	CNN	4 conv. 1 FC	No	99.30
Sun et al. (2019)	Imaginary/Physical movement	109	16	1 s	CNN+LSTM	4 conv. 5 FC	No	99.58

Table 4
Entropy of different biometrics.

Biometric	Study	Entropy (bits)
Finger vein	Krivokuća et al. (2020)	4.2–19.5
Retina	Arakala et al. (2009)	16.7
Voice	K. Inthavisas (2012)	18–30
Iris	Hao et al. (2006)	44
Fingerprint	Li et al. (2012)	48
Face	Feng and Yuen (2012)	75
Iris	Kanade et al. (2009)	94
Gait	Hoang et al. (2015)	50–139
EEG	Sadeghi et al. (2017)	83
EEG	Bajwa and Dantu (2016)	82

to be only 36 bits. In another similar research (Nguyen et al., 2019), the EEG entropy is approximated by 82 bits based on 18 selected channels. To have a better view of the superiority of EEG biometric over some well-known biometric, the entropy of some common biometrics are summarized in Table 4. It is worth mentioning that the entropy of human chosen passwords is 20–22 bits(Wang et al., 2017). The studies on EEG entrophy considered only shallow classification methods. Given that recent works have paid much more attention to deep learning approaches, the claims of these studies need to be further explored in the future research considering the deep learning methods.

Besides the entropy of the EEG biometric, there are two other points considering with brute-forcing EEG biometric: 1) how an adversary can generate artificial EEG signals, 2) how the system can differentiate artificial machine generated signals and human recorded signals. Generating artificial EEG is a subclass of artificial signal generation. Traditionally, it can be achieved by some methods such as autoregression, or statistical simulation or physiological modeling of EEG, however, they often demonstrate poor generalization performance (Nik Aznan et al., 2019). With the development of machine learning methods and in particular deep learning approaches in recent years, special attention has been paid to the use of these methods for artificial data generation. The most important of these methods are "*Generative Adversarial Networks*" (GANs) (Creswell et al., 2018). GANs provide a way to generate new data with the same statistics as the training set. A variety of works have been done in recent years to produce fake EEG signals with GAN (for instance, (Hartmann et al., 2018; Nik Aznan et al., 2019; Panwar et al., 2019; Piplani et al., 2018)) that have shown a very good performance. These tools have made it easier for the adversary to attack EEG based authentication systems. In return, the authentication systems should provide a way to distinguish machine-made and human-generated signals. The solution is the liveness test method which ensures that input data is originating from a live human being, and it is not artificial data. Unfortunately, the EEG signals are believed to have an intrinsic liveness property due to the point that they can only be obtained when a live human subject is present. Clearly, given the success of recent methods such as GAN for generating fake EEG signals, this assumption is not realistic (Sohankar et al., 2017). Some liveness test methods such as reflection or response to an external stimulus may be applicable here, but as far as we know there is no liveness test designed specifically for the specification of EEG signals.

Last but not the least attacking method, is attempting to reuse a sniffed target's EEG signals to log in the system as the target. Replay attack by using the exact sniffed EEG can be easily prevented by rejecting a duplicated signal since it is not plausible that the recorded biometric signals of a person are exactly the same at two different sessions. Even adding white noise to the sniffed signal can be detected using a similarity check in which each signal should have a threshold of difference with the previous ones (Roberts, 2007; Sadeghi et al., 2017; Sohankar et al., 2015). But the advent of recent methods such as GANs in synthetic data generation has made similarity check alone not enough to prevent these attacks. Piplani et al. (2018) showed that the EEG based authentication system might be easily tricked into accepting the synthetic data generated by a GAN model. These weaknesses in EEG biometric require serious consideration and proposing defensive methods to strengthen authentication.

Given the weakness of the liveness and similarity testing methods, it seems that the only way to prevent these attacks is to prevent intruders from sniffing the users' EEG signals by approaches such as encryption transmitting channels and EEG records. However, reviews of the apps on the market show that they do not only meet these security recommendations, but also the program reveals many security vulnerabilities, even more than those discussed above. Xiao et al. (2019) explored the possibility of 5 attacks on the apps in NeuroSky App store. The attacks include the sniffing and recording the signals emitted from the victim's headset device. The analysis showed that from 156 apps publicly available in the store, all are vulnerable to this attack. The apps transmit the EGG signals through the "*over-the-air*" (OTA) transmission protocol between the brainwave headset and an RF dongle which can be sniffed by a proximate adversary. Moreover, from 31 free apps on the store, all are vulnerable to at least one type of remote attacks.

Sniffing and accessing the users' recorded EEGs do not only threaten system security but can also violate user privacy. EEG records, especially in resting states, reveal much information about the user. The current research shows that EEG can be used to predict viewed images, transfer brain waves to texts, monitor sleep, and reveal personal information such as sex, age, and user's illnesses or addictions (Bickford, 1987; Gondesen et al., 2019; Höller and Uhl, 2018; Xiao et al., 2019). It can even be used to inference the user's current emotion (Aggarwal et al., 2018) or activities such as reading, blinking, solving math problems, listening to music, relaxing, thinking of an item, and watching videos (Ni et al., 2017; Xiao et al., 2019). Given these challenges, prior to the commercial use of EEG biometric, a solution must be found to prevent the disclosure of personal information through the brain's signals while allowing the user to be authenticated. This issue will be discussed further in the next section as one of the challenges.

10. Open challenges

Many researchers have used EEG as a biometric authentication method so far, though these methods are often implemented only in the controlled environment, and there are still several challenges ahead of their applications in real-life scenarios (Yang and Deravi, 2017). For instance, the biometric authentication factor requirements such as universality and uniqueness are still not fully satisfied. This section reviews these challenges from different points of view including biometric factor requirements (i.e. universality, permanency, uniqueness, and collectability), user-friendly and user privacy.

10.1. Universality

A universal EGG based authentication system should be capable of being used for almost all people. Current research have studied either a limited set of individuals with predefined assumptions or a publicly available dataset that is believed to be biased (Gondesen et al., 2019). The subjects considered in these works were all healthy and almost young. The evaluation of existing unhealthy or affected subjects in the EEG authentication systems is still an important and open discussion (Del Pozo-Banos et al., 2014). Currently, there exist few works which have studied a dataset including healthy and alcoholic users (e.g.

Nguyen et al., 2012), but as far as we know, these works arenot only very limited, but also has not gone beyond alcoholic users. Hence, it can be argued that the EEG biometric has not met universality, yet.

Another issue that must be considered for universality is the use of feature extractor models instead of classifiers. In all research, a classifier is learned on the recorded EEG of a set of subjects, and then this model is used to distinguish between those subjects. This approach is not suited to have a global EEG biometric model since in this approach, at least one EEG sample of involved subjects is needed to train the model, and when a new person is added to the system, the whole model should be re-trained from scratch. In deep learning approaches, a deep model can act as a feature extractor instead of a classifier. A feature extractor model can be used to extract the feature vector of any subject (even those who are not visited in the learning phase), and then the subject is identified to the corresponding class by vector similarity-based algorithms (e.g. cosine similarity). Among the papers, only Schons et al. (2018) have tried to propose an EEG feature extractor model using a CNN, although they did not employ the feature vectors directly, and used it as the input of a fully connected neural network which ultimately makes their approach similar to a classification model. The authors believe that the existence of a feature extraction model that does not need to be re-trained for each person's entry is essential for the universal use of EEG biometric.

Another issue should be considered in the universality, is language dependencies in ERPs with linguistic stimuli, e.g. visualized a word of play a song. Up to the best knowledge of the authors, there is no research directly investigating the effects of different languages on the EEG authentication. However, there are clues that processing another language, especially in low proficiency users, engages different and more parts of the brain and with higher coherence than the first language. In adults, the left hemisphere is mostly involved in the native language processing, whereas in processing the second/foreign language, the right one is. Besides, it is shown that in the users with higher proficiency in the second language, linguistic processing is shifted to the left hemisphere and with a lower coherence in both hemispheres(Reiterer et al., 2009; 2011). Furthermore, it seems that harder language leads to more coherence(Cheung et al., 2009). As a result, the authors believe that if words or song are going to be used in the ERPs, it should be in the native language; otherwise, EEG pattern over scalp may change by aging or improving proficiency.

10.2. Permanency

Early studies on the EEG biometric authentication have only been performed on recorded data from a series of consecutive sessions, thus this question has still not been well answered whether the patterns of the EEG change over the long term. The permanency of EEG biometric has been challenged just in recent papers (La Rocca et al., 2014; 2014; Maiorana and Campisi, 2018; Maiorana et al., 2016a). Maiorana et al. (2016a) has argued that there are very few studies in which the data were acquired during different sessions on different days, and for those who have been recording data over different days, often the distance between sessions were only a few weeks. He later in his recent work (Maiorana and Campisi, 2018) examined the EEG records which have been acquired during a three-year period. This paper is the best on the permanency of EEG biometric, however, this field is still in the early stage and needs further research.

10.3. Uniqueness

In order to ensure that the biometrics are unique, it must be shown that they can uniquely identify an individual in a large set of individuals. However, current studies often consider a very limited and small set of populations between 4 and 50 subjects which cannot prove the uniqueness of the EEG biometric in practice. The distribution of participant size in the literature is represented in Fig. 6. As it is represented, more than 80% of works are on less than 50 subjects, and just a few works have studied their proposed methods for more than 100 subjects. Also, it has been argued that the identification ability of EEG biometric would be decreased by increasing the number of participants (Boubakeur et al., 2017; Tangkraingkij et al., 2010). Tangkraingkij et al. (2010) showed that the accuracy of the system may even be reduced up to 9% only by increasing participants by ten. We believe that EEG biometric cannot be yet claimed to be a universally unique biometric factor such as fingerprint.

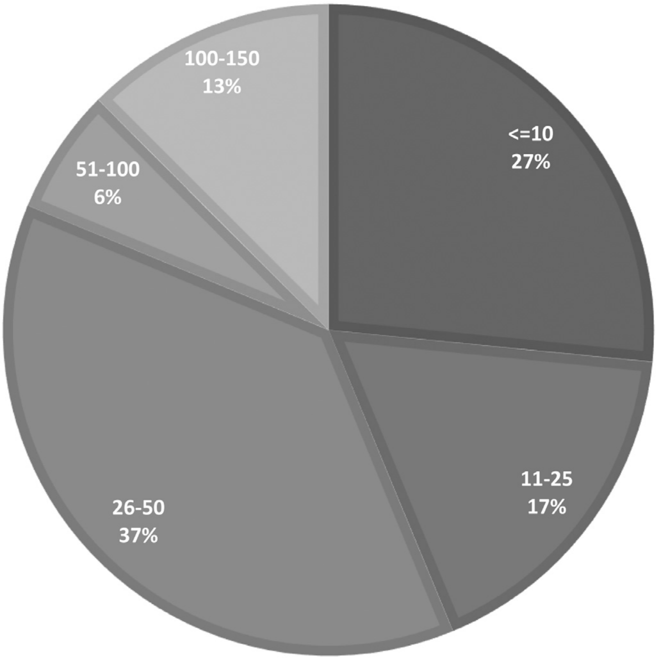

Fig. 6. Distribution of participant size in the EEG based authentication research.

10.4. Collectability

From the collectibility point of view, many of the challenges have been solved; however, this ability has not yet reached maturity. Current works generally require specific conditions during recording EEG and it should be done in a relaxed and cooperative manner. For example, in the sampling of the resting state with closed eyes, any sound in the environment will disrupt the functioning of the system. These conditions are not available in the uncontrollable environment. As a result, the use of EEG biometric authentication systems in practice is still with challenges.

On the other hand, the channels required for sampling should be reduced to the extent possible. The number of channels required in the papers is about 20 on average, which is more than the number of electrodes in most commercially available devices. Just a 17% of works have used less than 5 channels. This challenge is particularly true in the deep learning approaches, which currently have the best possible accuracy. The number of channels required in these works is 33 channels on average, which seems to be difficult to be used in practice. Hence, more research is yet required to be made to reduce the number of channels.

10.5. User privacy

As mentioned before, EEG records may be used to predict the private information of the users. To protect the users' privacy, unnecessary access to stored EEG records should be restricted. One may suggest to protect the storage of recorded EEG through encryption with data cryptography algorithms. There exist some papers on EEG encryption (e.g. Lin et al., 2014; Nguyen et al., 2017), however, we believe encryption does not solve this challenge, since if an attacker gains the control of the system and thus the key of encryption, he can recover encrypted EEG records. These systems should employ a similar approach to password-based authentication. These systems never store the passwords itself but the hash of passwords. The hashes could only be used for proving the claimed identity, but does not reveal any more information. Conventional hashing functions cannot be used in the EEG-based authentication since one person's EEG cannot be exactly the same on two different sessions, and even a small change in the input of these hash functions will result in completely different outputs. This leads to losing the ability to verify the claimed information at the time of authentication. For this aim, there are other protection methods for biometrics which are known as biometric template protection methods including feature transformation, key binding (such as fuzzy vault and fuzzy commitment), and key generation (such as secure sketch and fuzzy extractor) (Jain et al., 2008). These methods make it computationally impossible for an adversary to obtain the original biometric feature values, while the system is still able to verify the claimed biometric at the time of authentication. However, as far as we know, no research has done yet on the using of these methods in the EEG biometric. The only related paper is the work done by Singandhupe et al. (2017) in which the fuzzy extractor is used to extract a key to secure communication between a person and the drone under control. The paper only focused on the security of communication and it has not discussed the feasibility of using the proposed method in the general EEG based authentication and larger populations.

Similar to other biometrics, the EEG biometric features also need to be protected from revealing personal information, although this has not yet been addressed in the literature. There are plenty of formal works support the template protection methods for biometric authentication factors. For example, He and Wang (2014) proposed a biometrics-based authentication scheme using elliptic curve cryptography and fuzzy extractor. They also proved the completeness of the proposed scheme using the BAN logic. In addition, there are several mature works that suggest using multi-factor authentication for increasing both user security and privacy. For instance, Wang and Wang (2016) defined the security model of a two-factor authentication and then formally verified its required properties. This work provides a good theoretical background for this topic. In other works (Wang et al., 2015), an enhanced scheme with both user anonymity and provable security is suggested. The strength of this work is that it tries to achieve perfect security and privacy with the least additional communication or computation cost.

10.6. Security

As mentioned in Section 9, the spoofing attack is the main security challenge of EEG biometirc. Currently, the most important method of spoofing attack against EEG biometric is to use machine learning approach to generate synthetic EEG signals. The advances in the GAN models make it easy for the attackers to generate fake EEG signals similar to a victim's EEG, with the sufficient numbers EEG samples. There are main defense techniques: 1) prevent the attackers from accessing the users' EEG, 2) providing a liveness test. For preventing the attacker to access the target's EEG, the EEG records should be protected using methods such as encrypting the transmission channel or hashing the stored data. Liveness test is another way to deal with these attacks. Despite the importance of liveness test, it is rarely discussed in the literature, and since a dead person lacks biometric signals, it is assumed that brain signals can only be received from a living person. As mentioned in the previous section, this assumption is not true. We believe that currently one of the most important security challenges of EEG biometric is to provide a liveness test method.

10.7. User-friendly

While recording brain signals, users need to perform a specific task under defined conditions. The tasks may not be a pleasure for some users. Chuang et al. (2013) suggested that an EEG biometric system can be built independently of tasks. They have shown that tasks do not have much impact on the system accuracy, thus the system does not require to be dependent on a specific task. Moreover, they provided the users with a questionnaire that revealed some tasks are difficult or not pleasing to the users. Consequently, the authors suggested that, in order to increase the user-friendliness of the system, each user may separately choose the task of interest. Apart from this, this topic has not been addressed by other research so far and should be looked at in the future.

11. Conclusion

This paper provides an overview of authentication and identification methods using brain signals. The paper first reviews the characteristics of brain signals and their requirements as an authentication tool. In continue, available public datasets and different protocols for data acquisition are studied. Among the selected datasets, Physionet and DEAP are the most common and useful datasets due to the number of subjects, channels, and diversity of the tasks. Also, these datasets, in total, covered a wide range of EEG acquisition protocols, including rest states, music videos (both visual/acoustic ERPs) and physical/mental tasks. Although the rest states are simpler and more common in practice, ERP based tasks create higher SNR. However, they require some equipment for time synchronization between initiation of stimulus and EEG recording.

The next reviewed topic is the most common preprocessing methods of EEG signals. The appropriate preprocessing methods are not only dependent on the type and trials of tasks, but also on the selected feature extraction method. For instance, ensemble averaging can only be applied in ERP based tasks. Or, frequency filtering is required whenever time-domain features or templates are going to be extracted. Removing artifacts is another common preprocess, however, some researches have kept bio-artifacts, i.e. eye blinking, since they contain biometric data as well(Bhateja et al., 2019). Moreover, in this paper, different models of classifications that are used in literature for EEG authentication are also reviewed. These methods are divided into two categories of shallow and deep classifications. However, the use of the deep learning approach in this area has begun in recent years and there are still not many papers on that, but this approach has well-proven in this field and surpasses shallow methods. Shallow classification is a two-stage process in which the features should be extracted from preprocessed EEG data in the first stage and then, they can be classified in the second stage. The correct selection of feature extractor and classifier affects the result accuracy, directly. Although AR and PSD, as the extracted features, and similarity-based and SVM methods, as classifiers, are more common than the others, due to the lack of a standard benchmark, one cannot explicitly determine which methods are better in overall. Deep learning approaches, on the other hand, the model can be directly trained on the preprocessed data, and indeed, it, in turn, extracts distinguishable features during the training phase. Therefore, in the deep approaches, only selecting the appropriate network, the number of layers and their types matters. Currently, CNN is the most network used in the deep EEG authentication. It's worth mentioning that this paper is the first work that reviewed deep learning methods in EEG authentication. Furthermore, the paper discussed the open challenges in this field by summarizing existing work. These challenges are addressed in different categories including universality, permanency, uniqueness, collectability, privacy, security, and user-friendliness. The challenges are required to be addressed in future works.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abbas, S.N., Abo-Zahhad, M., Ahmed, S.M., Abbas, S.N., Abo-Zahhad, M., Ahmed, S.M., 2015. State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. IET Biom. 4 (3), 179–190.

Abdullah, M.K., Subari, K.S., Loong, J.L.C., Ahmad, N.N., 2010. Analysis of effective channel placement for an eeg-based biometric system. In: 2010 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES). IEEE, pp. 303–306.

Abdullah, M.K., Subari, K.S., Loong, J.L.C., Ahmad, N.N., 2010. Analysis of the eeg signal for a practical biometric system. World Acad. Sci. Eng. Technol. 68, 1123–1127.

Abo-Zahhad, M., Ahmed, S.M., Abbas, S.N., 2015. A new EEG acquisition protocol for biometric identification using eye blinking signals. Int. J. Intell. Syst.Appl. 7 (6), 48–54.

Abo-Zahhad, M., Ahmed, S.M., Abbas, S.N., 2016. A new multi-level approach to EEG based human authentication using eye blinking. Pattern Recognit. Lett. 82, 216–225.

Aggarwal, S., Aggarwal, L., Rihal, M.S., Aggarwal, S., 2018. Eeg based participant independent emotion classification using gradient boosting machines. In: 2018 IEEE 8th International Advance Computing Conference (IACC), pp. 266–271.

Alyasseri, Z.A.A., Khader, A.T., Al-Betar, M.A., Papa, J.P., ahmad Alomari, O., 2018. Eeg-based person authentication using multi-objective flower pollination algorithm. In: 2018 IEEE Congress on Evolutionary Computation (CEC). IEEE, pp. 1–8.

Arakala, A., Culpepper, J.S., Jeffers, J., Turpin, A., Boztaş, S., Horadam, K.J., McKendrick, A.M., 2009. Entropy of the retina template. In: International Conference on Biometrics. Springer, pp. 1250–1259.

Armstrong, B.C., Ruiz-Blondet, M.V., Khalifian, N., Kurtz, K.J., Jin, Z., Laszlo, S., 2015. Brainprint: assessing the uniqueness, collectability, and permanence of a novel method for erp biometrics. Neurocomputing 166, 59–67.

Arnau-Gonzalez, P., Katsigiannis, S., Ramzan, N., Tolson, D., Arevalillo-Herrez, M., 2017. Es1d: a deep network for eeg-based subject identification. In: 2017 IEEE 17th International Conference on Bioinformatics and Bioengineering (BIBE). IEEE, pp. 81–85.

Ashby, C., Bhatia, A., Tenore, F., Vogelstein, J., 2011. Low-cost electroencephalogram (EEG) based authentication. In: 2011 5th International IEEE/EMBS Conference on Neural Engineering. IEEE, pp. 442–445.

Bajwa, G., Dantu, R., 2016. Neurokey: towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Comput. Secur. 62, 95–113.

Bao, X., Wang, J., Hu, J., 2009. Method of individual identification based on electroencephalogram analysis. In: Proceedings – 2009 International Conference on New Trends in Information and Service Science, NISS 2009, pp. 390–393.

Barry, R.J., Clarke, A.R., Johnstone, S.J., Magee, C.A., Rushby, J.A., 2007. Eeg differences between eyes-closed and eyes-open resting conditions. Clin. Neurophysiol. 118 (12), 2765–2773.

Begleiter, H., Porjesz, B., Litke, A., Zhang, X.L., Wang, W., 2002. Event related potentials during object recognition tasks. Brain Res. Bull. 38 (6), 531–538.

Bhateja, V., Gupta, A., Mishra, A., Mishra, A., 2019. Artificial Neural Networks Based Fusion and Classification of Eeg/eog Signals. In: Information Systems Design and Intelligent Applications. Springer, pp. 141–148.

Bickford, R., 1987. Electroencephalography. In: Adelman, G. (Ed.), Encyclopedia of Neuroscience. Cambridge, pp. 371–373.

Blasco, J., Chen, T.M., Tapiador, J., Peris-Lopez, P., 2016. A survey of wearable biometric recognition systems. ACM Comput. Surv. 49 (3), 43.

Boubakeur, M.R., Wang, G., Zhang, C., Liu, K., 2017. Eeg-based person recognition analysis and criticism. In: 2017 IEEE International Conference on Big Knowledge (ICBK). IEEE, pp. 155–160.

Brunner, C., Leeb, R., Müller-Putz, G., Schlögl, A., Pfurtscheller, G., 2008. BCI Competition 2008–Graz Data Sset A. Technical Report.

Chen, J.X., Mao, Z.J., Yao, W.X., Huang, Y.F., 2019. EEG-Based biometric identification with convolutional neural network. Multimed. Tools Appl..

Chen, Y., Atnafu, A.D., Schlattner, I., Weldtsadik, W.T., Roh, M.C., Kim, H.J., Lee, S.W., Blankertz, B., Fazli, S., 2016. A high-security EEG-based login system with RSVP stimuli and dry electrodes. IEEE Trans. Inf. Forensics Secur. 11 (12), 2635–2647.

Cheung, M.-c., Chan, A.S., Sze, S.L., 2009. Increased theta coherence during chinese reading. Int. J. Psychophysiol. 74 (2), 132–138.

Chuang, J., Nguyen, H., Wang, C., Johnson, B., 2013. I think, therefore I am: Usability and security of authentication using brainwaves. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7862, pp. 1–16. LNCS

Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., Bharath, A.A., 2018. Generative adversarial networks: an overview. IEEE Signal Process. Mag. 35 (1), 53–65.

Das, R., Maiorana, E., Campisi, P., 2016. EEG biometrics using visual stimuli: a longitudinal study. IEEE Signal Process. Lett. 23 (3), 341–345.

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

Das, R., Maiorana, E., La Rocca, D., Campisi, P., 2015. EEG biometrics for user recognition using visually evoked potentials. In: Lecture Notes in Informatics (LNI), Proceedings –Series of the Gesellschaft fur Informatik (GI) P-245, pp. 303–310.

Das, R., Piciucco, E., Maiorana, E., Campisi, P., 2016. Visually evoked potentials for EEG biometrie recognition. In: 2016 1st International Workshop on Sensing, Processing and Learning for Intelligent Machines, SPLINE 2016 – Proceedings.

Del Pozo-Banos, M., Alonso, J.B., Ticay-Rivas, J.R., Travieso, C.M., 2014. Electroencephalogram subject identification: areview. Expert Syst. Appl. 41 (15), 6537–6554.

Delpozo-Banos, M., Travieso, C.M., Weidemann, C.T., Alonso, J.B., 2015. EEG biometric identification: a thorough exploration of the time-frequency domain. J. Neural Eng. 12 (5).

Demos, J.N., 2005. Getting Started With Neurofeedback. WW Norton & Company.

Di, Y., An, X., He, F., Liu, S., Ke, Y., Ming, D., 2019. Robustness analysis of identification using resting-state EEG signals. IEEE Access 7 (c), 42113–42122.

Eeg - electroencephalogram - bci. http://neurosky.com/biosensors/eeg-sensor/. Accessed: 14 June 2019.

Eeg headsets and the rise of passthoughts, 2017, http://neurosky.com/2017/02/eeg-headsets-and-the-rise-of-passthoughts/ (Accessed 14 June 2019).

Feng, Y.C., Yuen, P.C., 2012. Binary discriminant analysis for generating binary face template. IEEE Trans. Inf. Forensics Secur. 7 (2), 613–624.

Frank, D., Mabrey, J., Yoshigoe, K., 2017. Personalizable neurological user authentication framework. In: 2017 International Conference on Computing, Networking and Communications, ICNC 2017, pp. 932–936.

Fraschini, M., Hillebrand, A., Demuru, M., Didaci, L., Marcialis, G.L., 2015. An EEG-based biometric system using eigenvector centrality in resting state brain networks. IEEE Signal Process. Lett. 22 (6), 666–670.

Galbally, J., Marcel, S., Fierrez, J., 2013. Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition. IEEE Trans. Image Process. 23 (2), 710–724.

Gaspar, C.M., Rousselet, G.A., Pernet, C.R., 2011. Reliability of ERP and single-trial analyses. Neuroimage 58 (2), 620–629.

Goldberger, A.L., Amaral, L.A., Glass, L., Hausdorff, J.M., Ivanov, P.C., Mark, R.G., Mietus, J.E., Moody, G.B., Peng, C.K., Stanley, H.E., 2000. Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals.. Circulation 101 (23), e215–e220.

Gondesen, F., Marx, M., Gollmann, D., 2019. Eeg-based biometrics. In: Biometric-Based Physical and Cybersecurity Systems. Springer, pp. 287–318.

Gui, Q., Jin, Z., Xu, W., 2014. Exploring eeg-based biometrics for user identification and authentication. In: 2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB). IEEE, pp. 1–6.

Gui, Q., Jin, Z., Xu, W., Ruiz-Blondet, M.V., Laszlo, S., 2015. Multichannel eeg-based biometric using improved RBFneural networks. In: 2015 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), pp. 1–6.

Hao, F., Anderson, R., Daugman, J., 2006. Combining crypto with biometrics effectively. IEEE Trans. Comput. 55 (9), 1081–1088.

Hartmann, K. G., Schirrmeister, R. T., Ball, T., 2018. EEG-GAN: generative adversarial networks for electroencephalograhic (EEG) brain signals. arXiv:1806.01875.

He, D., Wang, D., 2014. Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst. J. 9 (3), 816–823.

Hoang, T., Choi, D., Nguyen, T., 2015. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. Int. J. Inf. Secur. 14 (6), 549–560.

Höller, Y., Uhl, A., 2018. Do eeg-biometric templates threaten user privacy? In: Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security. ACM, pp. 31–42.

Hu, J.F., 2009. New biometric approach based on motor imagery EEG signals. In: FBIE 2009 – 2009 International Conference on Future BioMedical Information Engineering, pp. 94–97.

Hu, J.F., 2010. Biometric system based on EEG signals by feature combination. In: 2010 International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2010, 1, pp. 752–755.

Hunter, M., Smith, R.L., Hyslop, W., Rosso, O.A., Gerlach, R., Rostas, J.A., Williams, D.B., Henskens, F., 2005. The Australian EEG database. Clin. EEG Neurosci. 36 (2), 76–81.

Idrus, S.Z.S., Cherrier, E., Rosenberger, C., Schwartzmann, J.-J., 2013. A review on authentication methods. Aust. J. Basic Appl. Sci. 7 (5), 95–107.

Jain, A.K., Nandakumar, K., Nagar, A., 2008. Biometric template security. EURASIP J. Adv. Signal Process. 2008, 113.

Jain, A.K., Ross, A., Prabhakar, S., 2004. An introduction to biometric recognition. IEEE Trans. Circt. Syst. Video Technol. 14 (1), 4–20. doi:10.1109/TCSVT.2003.818349.

Jayarathne, I., Cohen, M., Amarakeerthi, S., 2016. Brainid: development of an eeg-based biometric authentication system. In: 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, pp. 1–6.

Jian-feng, H., 2009. Multifeature biometric system based on EEG signals. In: Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human. ACM, pp. 1341–1345.

Johnson, B., Maillart, T., Chuang, J., 2014. My thoughts are not your thoughts. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication. ACM, pp. 1329–1338.

K. Inthavisas, D.L., 2012. Secure speech biometric templates for user authentication. IET Biom. 1. 46–54(8)

Kanade, S., Camara, D., Petrovska-Delacrtaz, D., Dorizzi, B., 2009. Application of biometrics to obtain high entropy cryptographic keys. World Acad. Sci. Eng. Technol. 52, 330.

Kang, J.-h., Chang, Y., Kim, S.-p., 2018. Neurocomputing electroencephalographic feature evaluation for improving personal authentication performance. Neurocomputing 287, 93–101.

Kaur, B., Singh, D., 2017. Neuro signals: a future biomertic approach towards user identification. In: 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence. IEEE, pp. 112–117.

Kaur, B., Singh, D., Roy, P.P., 2017. A novel framework of EEG-based user identification by analyzing music-listening behavior. Multimed. Tools Appl. 76 (24), 25581–25602.

Keirn, Z.A., Aunon, J.I., 1990. A new mode of communication between man and his surroundings. IEEE Trans. Biomed. Eng. 37 (12), 1209–1214.

Keshishzadeh, S., Fallah, A., Rashidi, S., 2016. Improved EEG based human authentication system on large dataset. In: 2016 24th Iranian Conference on Electrical Engineering, ICEE 2016, pp. 1165–1169.

Kim, D., Kim, K., 2019. Resting state eeg-based biometric system using concatenation of quadrantal functional networks. IEEE Access 7, 65745–65756.

Klimesch, W., 1996. Memory processes, brain oscillations and EEGsynchronization. Int. J. Psychophysiol. 24 (1), 61–100.

Klonovs, J., Petersen, C.K., Olesen, H., Hammershøj, A., Hammershoj, A., 2013. ID proof on the go: development of a mobile EEG-based biometric authentication system. IEEE Spectr. 8 (February), 81–89.

Koelstra, S., Mühl, C., Soleymani, M., Lee, J.S., Yazdani, A., Ebrahimi, T., Pun, T., Nijholt, A., Patras, I., 2012. DEAP: a database for emotion analysis; using physiological signals. IEEE Trans. Affect. Comput. 3 (1), 18–31.

Koike-Akino, T., Mahajan, R., Marks, T.K., Wang, Y., Watanabe, S., Tuzel, O., Orlik, P., 2016. High-accuracy user identification using eeg biometrics. In: 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). IEEE, pp. 854–858.

Kostílek, M., Št'astnỳ, J., 2012. Eeg biometric identification: repeatability and influence of movement-related eeg. In: 2012 International Conference on Applied Electronics. IEEE, pp. 147–150.

Krivokuća, V., Gomez-Barrero, M., Marcel, S., Rathgeb, C., Busch, C., 2020. Towards measuring the amount of discriminatory information in finger vein biometric characteristics using a relative entropy estimator. In: Handbook of Vascular Biometrics. Springer, pp. 507–525.

Kumar, P., Saini, R., Pratim Roy, P., Prosad Dogra, D., 2017. A bio-signal based framework to secure mobile devices. J. Netw. Comput. Appl. 89 (January), 62–71.

Kumari, P., Vaish, A., 2016. Feature-level fusion of mental task's brain signal for an efficient identification system. Neural Comput. Appl. 27 (3), 659–669.

La Rocca, D., Campisi, P., Scarano, G., 2014. Stable EEG features for biometric recognition in resting state conditions. Commun. Comput. Inf. Sci. 452, 313–330.

Lan Ma, Minett, J.W., Blu, T., Wang, W.S.-Y., 2015. Resting state EEG-based biometrics for individual identification using convolutional neural networks. In: 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 2848–2851.

Lawhern, V.J., Solon, A.J., Waytowich, N.R., Gordon, S.M., Hung, C.P., Lance, B.J., 2018. Eegnet: a compact convolutional neural network for eeg-based brain–computer interfaces. J. Neural Eng. 15 (5), 056013.

Li, P., Yang, X., Qiao, H., Cao, K., Liu, E., Tian, J., 2012. An effective biometric cryptosystem combining fingerprints with error correction codes. Expert Syst. Appl. 39 (7), 6562–6574.

Liew, S.-H., Choo, Y.-H., Low, Y.F., Mohd Yusoh, Z.I., 2018. EEG-based biometric authentication modelling using incremental fuzzy-rough nearest neighbour technique. IET Biom. 7 (2), 145–152.

Liew, S.-H., Choo, Y.-H., Low, Y.F., Yusoh, Z.I.M., 2015. Identifying visual evoked potential (vep) electrodes setting for person authentication. Int. J. Adv. Soft Comput. Appl. 7 (3), 85–99.

Lin, C.-F., Shih, S.-H., Zhu, J.-D., 2014. Chaos based encryption system for encrypting electroencephalogram signals. J. Med. Syst. 38 (5), 49.

Lin, C.-T., Liu, Y.-T., Wu, S.-L., Cao, Z., Wang, Y.-K., Huang, C.-S., King, J.-T., Chen, S.-A., Lu, S.-W., Chuang, C.-H., 2017. Eeg-based brain-computer interfaces: a novel neurotechnology and computational intelligence method. IEEE Syst. Man Cybern. Mag. 3 (4), 16–26.

Luck, S.J., 2014. An Introduction to the Event-Related Potential Technique. MIT Press, Cambridge, MA, USA.

Maiorana, E., Campisi, P., 2018. Longitudinal evaluation of EEG-Based biometric recognition. IEEE Trans. Inf. Forensics Secur. 13 (5), 1123–1138.

Maiorana, E., La Rocca, D., Campisi, P., 2016. On the permanence of EEG signals for biometric recognition. IEEE Trans. Inf. Forensics Secur. 11 (1), 163–175.

Maiorana, E., Solé-Casals, J., Campisi, P., 2016. EEG signal preprocessing for biometric recognition. Mach. Vis. Appl. 27 (8), 1351–1360.

Mao, Z., Yao, W.X., Huang, Y., 2017. Eeg-based biometric identification with deep learning. In: 2017 8th International IEEE/EMBS Conference on Neural Engineering (NER), pp. 609–612.

Marcel, S., Millan, J.d.R., 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Trans. Pattern Anal. Mach. Intell. 29 (4), 743–748.

McFarland, D.J., McCane, L.M., David, S.V., Wolpaw, J.R., 1997. Spatial filter selection for eeg-based communication. Electroencephalogr. Clin. Neurophysiol. 103 (3), 386–394.

Moore, S.K., 2016. "Brainprint" biometric id hits 100% accuracy [news]. IEEE Spectr. 53 (6). 14–14

Nakamura, T., Goverdovsky, V., Mandic, D.P., 2017. In-ear eeg biometrics for feasible and readily collectable real-world person authentication. IEEE Trans. Inf. Forensics Secur. 13 (3), 648–661.

Nguyen, D., Tran, D., Ma, W., 2019. A study on combing EEG signals and crytography for bitcoin security. Aust. J. Intell. Inf.Process. Syst. 34.

Nguyen, D., Tran, D., Sharma, D., Ma, W., 2017. On the study of EEG-based cryptographic key generation. In: Procedia Computer Science. Elsevier B.V., pp. 936–945.

Nguyen, P., Tran, D., Huang, X., Sharma, D., 2012. A proposed feature extraction method for EEG-based person identification. Int. Conf. Artif.Intell..

Nguyen, P., Tran, D., Le, T., Huang, X., Ma, W., 2013. Eeg-based person verification using multi-sphere SVDDand UBM. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, pp. 289–300.

Ni, Z., Yuksel, A.C., Ni, X., Mandel, M.I., Xie, L., 2017. Confused or not confused?: Disentangling brain activity from eeg data using bidirectional LSTM recurrent neural networks. In: Proceedings of the 8th ACM International Conference on Bioinformatics, Computational Biology,and Health Informatics. ACM, New York, NY, USA, pp. 241–246.

Niedermeyer, E., da Silva, F.L., 2005. Electroencephalography: Basic Principles, Clinical Applications, and Related Fields. Lippincott Williams & Wilkins.

Nik Aznan, N.K., Atapour-Abarghouei, A., Bonner, S., Connolly, J.D., Al Moubayed, N., Breckon, T.P., 2019. Simulating brain signals: creating synthetic eeg data via neural-based generative models for improved SSVEP classification. In: 2019 International Joint Conference on Neural Networks (IJCNN), pp. 1–8.

Özdenizci, O., Wang, Y., Koike-Akino, T., Erdoğmuş, D., 2019. Adversarial deep learning in eeg biometrics. IEEE Signal Process. Lett. 26 (5), 710–714.

Palaniappan, R., 2006. Electroencephalogram signals from imagined activities: a novel biometric identifier for a small population. In: International Conference on Intelligent Data Engineering and Automated Learning. Springer, pp. 604–611.

Panwar, S., Rad, P., Quarles, J., Huang, Y., 2019. Generating eeg signals of an RSVP experiment by a class conditioned Wasserstein generative adversarial network. In: 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). IEEE, pp. 1304–1310.

Pham, T., Ma, W., Tran, D., Nguyen, P., Phung, D., 2014. Multi-factor EEG-based user authentication. Proc. Int. Jt. Conf. Neural Netw. 4029–4034.

Pham, T., Ma, W., Tran, D., Tran, D.S., Phung, D., 2015. A study on the stability of eeg signals for user authentication. In: 2015 7th International IEEE/EMBS Conference on Neural Engineering (NER). IEEE, pp. 122–125.

Phothisonothai, M., 2015. An investigation of using SSVEP for EEG-based user authentication system. In: 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA). IEEE, pp. 923–926.

Phung, D.Q., Tran, D., Ma, W., Nguyen, P., Pham, T., 2014. Using Shannon entropy as eeg signal feature for fast person identification.. In: ESANN, 4, pp. 413–418.

Piciucco, E., Maiorana, E., Falzon, O., Camilleri, K.P., Campisi, P., 2017. Steady-state visual evoked potentials for eeg-based biometric identification. In: 2017 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE, pp. 1–5.

Piplani, T., Merill, N., Chuang, J., 2018. Faking it, making it: fooling and improving brain-based authentication with generative adversarial networks. In: 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–7.

Polich, J., 2007. Updating p300: an integrative theory of p3a and p3b. Clin. Neurophysiol. 118 (10), 2128–2148.

Poulos, M., Rangoussi, M., Kafetzopoulos, E., 1998. Person identification via the eeg using computational geometry algorithms. In: 9th European Signal Processing Conference (EUSIPCO 1998). IEEE, pp. 1–4.

Ramzan, Q., Shidlovskiy, S., 2018. Evolution of the Brain Computing Interface (BCI) and proposed electroencephalography (EEG) signals based authentication model. MATEC Web Conf. 155, 01006.

Ravi, K.V.R., Palaniappan, R., Eswaran, C., Phon-Amnuaisuk, S., 2008. Data encryption using event-related brain signals. In: Proceedings - International Conference on Computational Intelligence and Multimedia Applications, ICCIMA 2007, 1, pp. 540–544.

Read, G.L., Innis, I.J., 2017. Electroencephalography (EEG). Am. Cancer Soc., pp. 1–18.

Reiterer, S., Pereda, E., Bhattacharya, J., 2009. Measuring second language proficiency with eeg synchronization: how functional cortical networks and hemispheric involvement differ as a function of proficiency level in second language speakers. Second Lang. Res. 25 (1), 77–106.

Reiterer, S.M., Pereda, E., Bhattacharya, J., 2011. On a possible relationship between linguistic expertise and EEG gamma band phase synchrony. Front. Psychol. 2, 334.

Roberts, C., 2007. Biometric attack vectors and defences. Comput. Secur. 26 (1), 14–25.

Ruiz-blondet, M., Khalifian, N., Armstrong, B.C., Jin, Z., Kurtz, K.J., Laszlo, S., 2014. Brainprint: identifying unique features of neural activity with machine learning. In: Proc. 36th Annual Conf. of the Cognitive Science Society, pp. 827–832.

Ruiz-Blondet, M.V., Jin, Z., Laszlo, S., 2016. Cerebre: a novel method for very high accuracy event-related potential biometric identification. IEEE Trans. Inf. Forensics Secur. 11 (7), 1618–1629.

Ruiz-Blondet, M.V., Jin, Z., Laszlo, S., 2017. Permanence of the cerebre brain biometric protocol. Pattern Recognit. Lett. 95, 37–43.

Sadeghi, K., Banerjee, A., Sohankar, J., K. S. Gupta, S., 2017. Geometrical analysis of machine learning security in biometric authentication systems. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 309–314.

Sadeghi, K., Sohankar, J., Banerjee, A., Gupta, S.K., 2017. A novel spoofing attack against electroencephalogram-based security systems. In: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, pp. 1–6.

Sanei, S., 2013. Adaptive Processing of Brain Signals. John Wiley & Sons.

Sanei, S., Chambers, J., 2013. EEG Signal Processing. Wiley.

Schalk, G., McFarland, D.J., Hinterberger, T., Birbaumer, N., Wolpaw, J.R., 2004. Bci2000: a general-purpose brain-computer interface (BCI) system. IEEE Trans. Biomed. Eng. 51 (6), 1034–1043.

Schirrmeister, R.T., Springenberg, J.T., Fiederer, L.D.J., Glasstetter, M., Eggensperger, K., Tangermann, M., Hutter, F., Burgard, W., Ball, T., 2017. Deep learning with convolutional neural networks for EEG decoding and visualization.. Hum. Brain Mapp. 38 (11), 5391–5420.

Schons, T., Moreira, G.J.P., Silva, P.H.L., Coelho, V.N., Luz, E.J.S., 2018. Convolutional network for EEG-based biometric. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 10657 LNCS, pp. 601–608.

Sharma, P.K., Vaish, A., 2016. Individual identification based on neuro-signal using motor movement and imaginary cognitive process. Opt.-Int. J. Light Electron Opt. 127 (4), 2143–2148.

Singandhupe, A., La, H.M., Feil-Seifer, D., Huang, P., Guo, L., Li, M., 2017. Securing a UAV using individual characteristics from an eeg signal. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, pp. 2748–2753.

Singh, B., Mishra, S., Tiwary, U.S., 2015. EEG based biometric identification with reduced number of channels. In: International Conference on Advanced Communication Technology, ICACT 2015-August, pp. 687–691.

Snodgrass, J.G., Vanderwart, M., 1980. A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity. J. Exp. Psychol..

Sockeel, S., Schwartz, D., Pélégrini-Issac, M., Benali, H., 2016. Large-scale functional networks identified from resting-state EEG using spatial ICA. PLoS One.

Sohankar, J., Sadeghi, K., Banerjee, A., Gupta, S.K.S., 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, pp. 165–172.

Sohankar, J., Sadeghi, K., Banerjee, A., Gupta, S.K.S., 2017. Systematic analysis of liveness detection methods in biometric security systems. In: 2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 1–6.

Sun, Y., Lo, F.P., Lo, B., 2019. EEG-Based user identification system using 1D-convolutional long short-term memory neural networks. Expert Syst. Appl. 125, 259–267.

Sundararajan, A., Pons, A., Sarwat, A.I., 2015. A generic framework for EEG-based biometric authentication. In: 2015 12th International Conference on Information Technology-New Generations. IEEE, pp. 139–144.

Tabar, Y.R., Halici, U., 2016. A novel deep learning approach for classification of eeg motor imagery signals. J. Neural Eng. 14 (1), 016003.

Tangkraingkij, P., Lursinsap, C., Sanguansintukul, S., Desudchit, T., 2010. Personal identification by EEG using ICA and neural network. In: International Conference on Computational Science and Its Applications. Springer, pp. 419–430.

Thomas, K.P., Vinod, A.P., 2018. EEG-Based Biometric authentication using gamma band power during rest state. Circt. Syst. Signal Process. 37 (1), 277–289.

Thomas, K.P., Vinod, A.P., Robinson, N., 2017. Online biometric authentication using subject-specific band power features of EEG. In: Proceedings of the 2017 International Conference on Cryptography, Security and Privacy. ACM, pp. 136–141.

Vahid, A., Arbabi, E., 2016. Human identification with eeg signals in different emotional states. In: 2016 23rd Iranian Conference on Biomedical Engineering and 2016 1st International Iranian Conference on Biomedical Engineering (ICBME). IEEE, pp. 242–246.

Waili, T., Johar, M.G.M., Sidek, K., Nor, N.M., Yaacob, H., Othman, M., 2019. Eeg based biometric identification using correlation and MLPNN models.. Int. J. Online Eng. 15 (10), 77–90.

Wang, D., Cheng, H., Wang, P., Huang, X., Jian, G., 2017. Zipf's law in passwords. IEEE Trans. Inf. Forensics Secur. 12 (11), 2776–2791.

Wang, D., Wang, N., Wang, P., Qing, S., 2015. Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity. Inf. Sci. 321, 162–178.

Wang, D., Wang, P., 2016. Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans Dependable Secure Comput 15 (4), 708–722.

Wang, Y., Najafizadeh, L., 2016. On the invariance of EEG-based signatures of individuality with application in biometric identification. In: Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS, 2016, pp. 4559–4562.

Wang, Z., Healy, G., Smeaton, A.F., Ward, T.E., 2018. A review of feature extraction and classification algorithms for image rsvp based BCI. In: Signal Processing and Machine Learning for Brain-Machine Interfaces, pp. 243–270.

Wilaiprasitporn, T., Ditthapron, A., Matchaparn, K., Tongbuasirilai, T., Banluesombatkul, N., Chuangsuwanich, E., 2019. Affective eeg-based person identification using the deep learning approach. IEEE Trans. Cognit. Dev.Syst..

Wu, Q., Zeng, Y., Zhang, C., Tong, L., Yan, B., 2018. An EEG-based person authentication system with open-set capability combining eye blinking signals. Sensors 18 (2), 1–18.

Xiao, D., Hu, J., 2010. Identification of motor imagery EEG signal. In: 2010 International Conference on Biomedical Engineering and Computer Science, ICBECS 2010.

Xiao, Y., Jia, Y., Cheng, X., Yu, J., Liang, Z., Tian, Z., 2019. I can see your brain: investigating home-use electroencephalography system security. IEEE Internet Things J. 6 (4), 6681–6691.

Yang, S., Deravi, F., 2017. On the usability of electroencephalographic signals for biometric recognition: a survey. IEEE Trans. Hum. Mach. Syst. 47 (6), 958–969.

Yang, S., Deravi, F., Hoque, S., 2018. Task sensitivity in EEG biometric recognition. Pattern Anal. Appl. 21 (1), 105–117.

Yin, Z., Zhao, M., Wang, Y., Yang, J., Zhang, J., 2017. Recognition of emotions using multimodal physiological signals and an ensemble deep learning model. Comput. Methods Programs Biomed. 140, 93–110.

Zeng, Y., Wu, Q., Yang, K., Tong, L., Yan, B., Shu, J., Yao, D., 2019. Eeg-based identity authentication framework using face rapid serial visual presentation with optimized channels. Sensors 19 (1), 6.

Zhang, F., Mao, Z., Huang, Y., Lin, X., Ding, G., 2018. Deep learning models for eeg-based rapid serial visual presentation event classification. J. Inf. Hiding Multimed. Signal Process. 9 (1), 177–187.

Zhang, Y., Chen, Y., Bressler, S.L., Ding, M., 2008. Response preparation and inhibition: the role of the cortical sensorimotor beta rhythm. Neuroscience 156 (1), 238–246.

Zuquete, A., Quintela, B., Silva Cunha, J.P., 2010. Biometric authentication using brain responses to visual stimuli. In: International Conference on Bio-inspired Systems and Signal Processing, pp. 103–112.

Amir Jalaly Bidgoly received his BSc degree in computer engineering (software) from University of Kashan (Kashan, Iran), in 2005, MSc degree in computer engineering (software) from Iran University of Science and Technology (IUST) in 2009, and PhD in computer engineering (software) in Isfahan University (Isfahan, Iran) in 2015. He is currently an Associated Professor in Department of Computer Engineering and Information Technology in University of Qom. His research interests include System Security, Social Security, Trust and Reputation Systems, and Formal Verification.