EEG Signals For Authentication In Security Systems

Phạm Tiến Dũng, Đinh Hoàng Gia, Lê Khải, Đào Thị Hồng Vân

***Abstract*— Authentication has been playing an important role in security systems and security operations. In a general sense, there are three types of person authentication: something a person knows (password-based), something a person has (token-based), and something a person is (biometric-based). Each has its own merits but also there are drawbacks which can cause vulnerabilities to security systems. Recently, technological advances make it easy to obtain Electroencephalography (EEG) signals. Moreover, the evidence shows that finding repeatable and stable brainwave patterns in EEG signals is feasible, and the prospect of using EEG signals for person authentication promising. An EEG-based person authentication system has the combined advantages of all three types of person authentication currently in use, yet without their drawbacks. Therefore, an EEG-based person authentication system should be suitable for especially high security systems. In this paper, we further speculate on that issue to provide a comprehensive review of state-of-the-art methods and some research directions for such an authentication system.**

***Tóm tắt*— Xác thực người dùng đóng vai trò quan trọng trong các hệ thống an toàn thông tin. Có 3 phương thức xác thực chính gắn liền với người dùng là: dựa trên mật khẩu (password-based), dựa trên thiết bị lưu trữ (token-based) và dựa trên thông tin sinh trắc học của người dùng (biometrics-based). Tuy nhiên mỗi phương thức trên đều có những ưu điểm và nhược điểm riêng. Công nghệ hiện nay cho phép trích xuất tín hiệu sóng não từ người dùng khá dễ dàng và các nghiên cứu gần đây cho thấy sóng não có những mẫu tín hiệu lặp lại và duy nhất đối với mỗi người dùng. Do đó, việc sử dụng sóng não trong xác thực là rất khả quan. Hệ thống xác thực người dùng bằng sóng não sẽ có đầy đủ những ưu điểm của 3 phương thức xác thực kể trên và khắc phục được những điểm yếu của chúng, do đó rất phù hợp với các hệ thống thông tin có yêu cầu rất cao về an toàn. Trong bài báo này, chúng tôi giới thiệu những phương pháp mới nhất và một số hướng nghiên cứu cho một hệ thống xác thực như vậy.**

Keywords*— *authentication; biometrics; EEG; machine learning; pattern recognition.

Từ khóa*— *xác thực; sinh trắc học; sóng não; máy học; nhận dạng mẫu.

I. INTRODUCTION

From the point of view of computer security access control is the central element which assures legitimate users access to resources in an authorized manner. Such access control also prevents unauthorized users from accessing resources, as well as legitimate users from using resources which are out of their privileges [1].

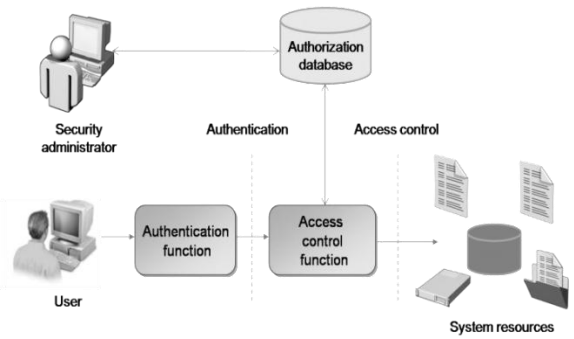

Figure 1. Relationship among authentication and other security functions [2]

According to [2], access control involves authentication and authorization functions which grant permissions to a user to access a system resource, as illustrated in Figure 1. Firstly, the authentication block verifies whether or not a user is permitted to access the system. The access control then determines which resources the authenticated user can manipulate using an authorization database. This database is maintained by a security administrator who defines user rights to corresponded with specific system resources.

It can be seen that person authentication block plays a vital role in security systems and security operations particularly in systems that have a high security requirement systems. It is the first line of defense that determines whether someone is who he or she is declared to be.

The process of authenticating a person is performed by comparing credentials which are provided by the person to those bound with the person identifier in a trusted source. If the credentials match, the person is allowed to access the system. In a general sense, there are three means by which to conduct person authentication:

(i) Something a person knows, for example, a password and PIN (personal identity number).

(ii) Something a person has, for example, physical keys and smart cards.

(iii) Something a person is or does, or so called biometric authentication, involving such as voice recognition and fingerprint matching.

Person authentication based on something a person knows, also known as password-based authentication, is the most popular authentication mechanism; it is where a user has to provide not only an ID but also a password. The system is simple, accurate and effective. However, password-based authentication is not immune from malicious attacks. Some popular password attack approaches are an action of off-line dictionary attack, a popular password attack, exploitation of user mistakes, and exploitation of multiple password use [1]. The dilemma today is that, with ever increasing computer power which can crack even longer passwords in shorter time, the memory of the human brain for the length of a password stays the same [1]. Therefore, a feasible alternative to password and PIN authentication is extremely desirable.

Person authentication based on something a person has, also known as token-based authentication, is an authentication mechanism that is based on objects a user possesses, such as a bank card, a memory card, a smart card, and a USB Dongle. This kind of authentication requires a user to provide the appropriate token when he or she needs to access a system. Presenting a token - a foreign object, which is neither a part of the human body nor a part of the knowledge of the person, can be inconvenient. Another inconvenience of token-based authentication is that special readers are always required which can be expensive to install. In addition, tokens can be physically stolen, duplicated, and hacked by engineering techniques [1, 3]. Securing a token is itself a challenge.

Person authentication based on something a person is or does, also known as biometric authentication, tries to authenticate users based on their biometric characteristics. The characteristics can be divided into two classes: physical characteristics such as fingerprint, face, hand geometry and iris; and behavioural characteristic such as handwriting and voice [4]. Although biometric authentication can avoid some of the disadvantages of both password-based and token-based authentication, the conventional biometric modalities have some security disadvantages. Face, fingerprint and iris information can be photographed. Voice can be recorded, and handwriting may be mimicked [4, 5]. Moreover, individuals may lose or change their biometric characteristics such as finger or face in certain circumstances; for example, changes may occur due to injury. With these disadvantages, there is a requirement for a better biometric modality for security systems.

Recently, researchers have successfully explored the potential of using the EEG as a new type of biometrics in person authentication. The conventional types of authentication each has major drawbacks, which means the EEG emerges as potential modality for authentication because it has quite clear advantages while it comes without the shortcomings of the conventional types authentication:

- EEG signals are confidential because they correspond to a secret mental task which cannot be observed;
- EEG signals are very difficult to mimic because the signals of similar mental tasks are person dependent;
- EEG signals are almost impossible to steal because the brain activity producing them issensitive to the stress and the mood of the person. An aggressor cannot force a person to reproduce the same signals while he or she is under stress [6].
- EEG signals, by nature, require a living person to produce the record.

The rest of the paper is organized as follows. Section II introduces EEG signals providing the background to development, the main brain rhythms and the signal recording. Section III provides an analysis of EEG signal characteristics for biometrics. A detail account of an EEG-based person authentication components with state-of-the-art techniques involving pre-processing, feature extraction, and classification is presented in Section IV. Section V suggests some directions research on using EEG signals for security systems particular in authentication purpose, and the conclusion is presented in Section VI.

II. ELECTROENCEPHALOGRAPHY (EEG) SIGNALS

A. EEG generation

The human brain contains nerve cells, structured by axons, dendrites, and cell bodies as illustrated in Figure 2. When stimulated by many

different types of stimuli, such as chemical during synaptic activities, light and electricity the ions in the cell bodies are exchanged across the neuron membrane in the direction controlled by the membrane potential [7]. The electrical impulse is transmitted along the axon and the signals are relayed to other cells by dendrites. The measurement of the electrical field over the scalp of a human subject provides a reading of the signals or Electroencephalography (EEG) signals.

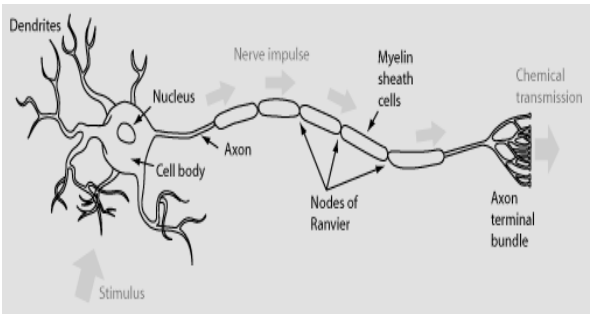

Figure 2. Structure of a neuron [7]

It is worth pointing out that there are different layers to the structure of a human head, for example there is the scalp, skull, brain and other thin layers between. These layers can degrade the signals, so an EEG is only recorded by the scalp electrodes when there is a sufficient large number of activated neurons which can generate enough potential [8].

B. EEG signal rhythms

EEG signals are divided into five major bands of waves, namely delta (0.5-3 Hz), theta (4-7 Hz), alpha (8-13 Hz), beta (14-30 Hz), and gamma (>30 Hz) waves. The examples of these bands are depicted in Figure 3. Delta waves are mainly associated with deep sleep and may also be observed in a waking state, while theta waves are associated with creative inspiration and deep meditation. Alpha waves are the most common in brain activities. Beta waves are the usual waking rhythms in the brain associated with active thinking, active attention or problem solving [8]. Gamma waves usually have low amplitudes, rare occurrences and relate to the movements of the left index finger, right toes and the tongue [9]. A summary of EEG frequency bands is shown in Table 1.

TABLE 1. A SUMMARY OF EEG FREQUENCY BAND

Name	Frequency Band	Dominated Brain Activity
Delta (δ)	0.5-4 Hz	Deep sleep
Theta (θ)	4-8 Hz	Creative inspiration, deep meditation
Alpha (α)	8-13 Hz	Relaxation state, performing movements
Beta (β)	13-30 Hz	Active thinking, solving problems
Gama (ɣ)	Over 30 Hz	Cognitive and motor functions

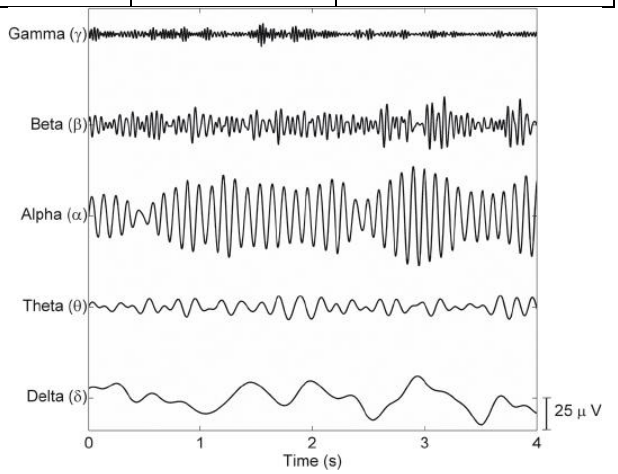

Figure 3. EEG major bands [8]

C. EEG signal acquisition

The first obtained human EEG recording was reported by Hans Berger in 1924. EEG signals can be acquired by using the portable devices with electrodes on the subject person's scalp. The number of electrodes can be varied depending on the experiment's design; for example, they are from 1 to 256 in Brain-Computer Interface (BCI) systems [10]. The electrodes are placed according to the 10-20 international system [11] as illustrated in Figure 4. The distance between two adjacent electrodes is 10% or 20% of the distance between inion and nasion as shown in Figure 4 (A) and (B).

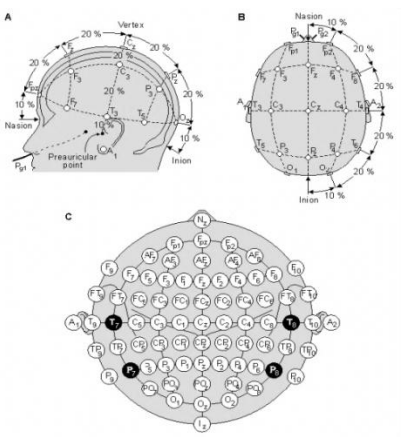

Figure 4. The international 10-20 system seen from (A) left and (B) above the head. (C) indicates a two-dimensional view of the electrode setup configuration [11]

The brain responses to different types of stimuli give certain types of EEG signals that are grouped into two main categories: evoked signals and spontaneous signals [12]. Evoked signals or evoked potentials occur unconsciously when a subject is stimulated by a known stimulus, while spontaneous signals are intentionally generated without any external stimulus. Visual stimuli with numbers and pictures are usually used during an EEG recording to elicit the evoked signals in which P300 component is a typical instance. This component is a large positive wave that occurs approximately 300 *ms* after a rare event is displayed [8]. In spontaneous signals, motor imagery where the subjects were asked to imagine moving a hand, finger, foot or tongue while EEG data is recorded, is applied widely in BCI systems.

III. EEG SIGNAL CHARACTERISTIC FOR BIOMETRICS

In recent years, researchers have started to establish the fact that brain-wave patterns are unique to every individual, and thus EEG signals can be used in biometrics. As with the required biological measurements of other popular biometrics [3], the different characteristics of EEG as a biometric identifier include:

Universality: Each person should have the characteristic. This requirement is highly satisfied by the EEG since any person, by nature, contains brain signals.

Distinctiveness: Any two persons should be sufficiently different in terms of the characteristic. Although the uniqueness of EEG signals is a complex issue [13], the evidence from recent EEG-based person recognition research, for example that of [6, 14] shows that EEG is a highly individual characteristic, which is consistent with previous neurophysiology studies such as [15-18].

Permanence: The characteristic should be sufficiently stable over a period of time.

A significant effort has been made to determine the reproduction of EEG signals by conducting test-retest analysis in neurophysiology scientific communities [19-22]. The authors showed that the considered features had a high reliability across the periods of time. In the biometric community, some session-to-session tests [23-25] have been conducted to validate the variability of EEG. These studies have concluded that EEG biometrics has a significant degree of repeatability.

Collectability: The characteristic can be measured quantitatively.

EEG signals are acquired by placing electrodes on the scalp of a person. The sheer number of electrodes and the use of conductive gel can cause users inconvenience. However, these limitations of EEG biometric's collectability can be overcome with the recent introduction of the dry electrode and limiting the number of electrodes used [13].

Performance: The characteristic used should have to achieve a good recognition accuracy. A variety of EEG-based biometric systems have been studied, and the results have shown that the recognition rates are promising. The performance of an EEG-based recognition system is evaluated by using different measures such as the genuine authentication rate (GAR), the false acceptance rate (FAR), and the false rejection rate (FRR). Some other studies have used the half total error rate (HTER = (FAR+FRR)/2) and the equal error rate (EER) to present the performance of the system.

Acceptability: People are willing to accept the use of the characteristic in their daily lives. EEG signals have been playing an important role in health and medical applications for sometime. Moreover, affective computing research has been trying to understand the states of human minds and emotions through EEG signals. Therefore, recording EEG signals for biometric systems may raise the privacy issue for users that relates to the diagnostic value of EEG signals and "mind reading" and emotion analysis [13, 26, 27]. Although some solutions have been proposed to deal with this privacy issue, for example [28, 29], more studies on the acceptability issue of EEG biometrics is needed.

TABLE 2. COMPARISON BETWEEN THE BRAINWAVE BIOMETRIC AND OTHER POPULAR BIOMETRICS.

Biometrics	Universality	Distinctiveness	Permanence	Collectability	Acceptability	Circumvention	Performance
Brainwave	✓✓	✓✓	✓✓	✓✓	✓		✓
DNA	✓✓	✓✓	✓✓				✓✓
Ear	✓	✓	✓✓	✓	✓✓	✓	✓
Face	✓✓		✓	✓✓	✓✓	✓✓	
Fingerprint	✓	✓✓	✓✓	✓	✓	✓	✓✓
Gait	✓			✓✓	✓✓	✓	
Hand geometry	✓	✓	✓	✓✓	✓	✓	✓
Iris	✓✓	✓✓	✓✓	✓			✓✓
Keystroke				✓	✓	✓	
Odor	✓✓	✓✓	✓✓		✓		
Palm	✓	✓✓	✓✓	✓	✓	✓	✓✓
Rentina	✓✓	✓✓		✓			✓✓
Signature				✓✓	✓✓	✓✓	
Voice	✓			✓	✓✓	✓✓	

Circumvention: The characteristic should be resistant to attacks. EEG signals relate to the activities inside the brain, so by their nature, EEG biometrics are difficult to fake, impossible to be observed, and it is easy to do live detection [6] Table 2 provides an overview comparison of brainwave biometric and other popular biometrics where high, medium and low are represented by two ticks (✓✓), one tick ✓ and no tick, respectively [3, 30].

IV. EEG-BASED PERSON AUTHENTICATION

The use of EEG signals for an automatic person recognition system was first introduced in 1980 by Stassen [31]. The study of EEG biometrics has received increased attention from the research community in recent years and they are large numbers of publications [13] which are almost entirely focused on the task of person identification.

Having the advantages of being very difficult (close to impossible) to fake, impossible to be observed or intercepted, unique, un-intrusive, and requiring live person recording [6], EEG signals are attractive researchers in the security area. [32] proposed a person authentication method for accessing computing devices by thinking a pass-thought instead of typing a password. After that, using brainwave patterns for person authentication was investigated and confirmed by [6] at the Dalle Molle Institute Intelligence Artificial Perceptive (IDIAP) in Switzerland.

An EEG-based person authentication system usually has two phases: enrollment and verification (Figure 5). The two main components in each of the phases are feature selection and classification. First, in the enrollment phase, a person is asked to do a task, for example imagine moving a hand, a foot, a finger or the tongue, and EEG signals of that user are acquired from his or her brainwave signals. Next, EEG data pre-processing is conducted to reduce noise. Then, features are extracted by a feature selection algorithm that enables the selection of only useful features. Finally, these extracted feature vectors are used to train and build the models.

In the verification phase, when a user wants to access the system, he or she must provide EEG signals that are generated by repeating the task which he/she did in the enrollment phase. These input EEG data are processed in the same way as in the enrollment. The obtained vector features are then fed into the classifier as testing data to match with the model of the individual who he or she claims to be. Based on the matching score and the threshold, the system will give the decision accepting or rejecting the claimed identity.

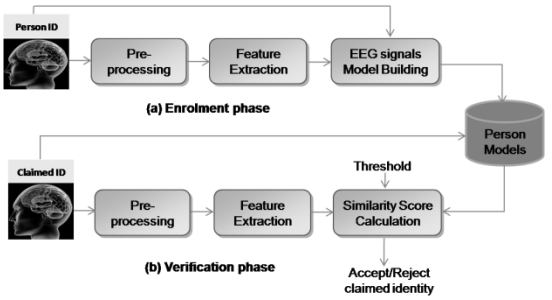

Figure 5. Typical EEG-based person authentication diagram

As with other biometric authentication systems, an EEG-based person authentication system has two types of error to overcome: false acceptance or false match, and false rejection or false non-match. A false acceptance error occurs when the system accepts an impostor, and the false rejection error occurs when a valid identity claim from a genuine user is rejected. A threshold is used in the decision making process. As illustrated in Figure 6, the threshold value t is selected so that if the matching score of claimed identity $s \geq t$ then a match is declared, otherwise it is a mismatch. By moving the threshold, the system can become more restrictive with a decrease of false acceptance, or more sensitive with a decrease of false rejection. However, the dilemma is that decreasing false acceptances causes increasing false rejections, and vice versa [1].

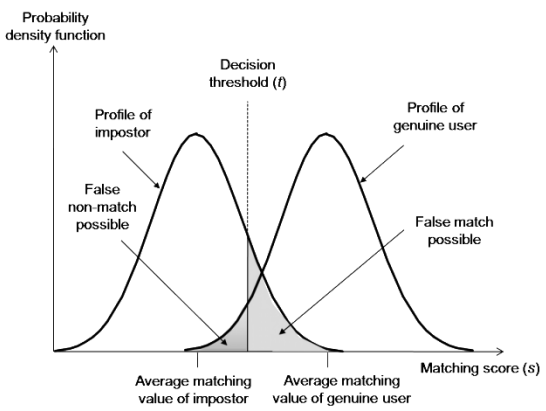

Figure 6. Typical biometric authentication diagram [1]

The performance of an EEG-based person authentication system is usually evaluated using a Decision Error Trade-off (DET) curve, which is a

plot of False Acceptance Rate (FAR) versus False Rejection Rate (FRR) [33]. To compare the accuracy of the systems with different DET curves, researchers use Equal Error Rate (EER) that is a point on a DET curve where FAR and FRR are equal. An example of DET curves and EER can be seen in Figure 7.

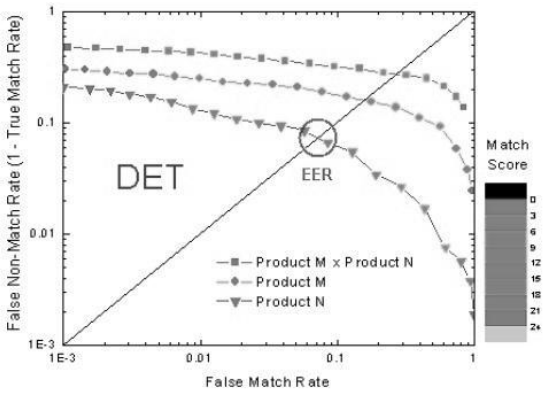

Figure 7. An example of DET curves [74]

It is worth pointing out that an EEG-based person recognition system has two different tasks, namely EEG-based person identification and EEG-based person verification. For biometric verification the user has to provide not only biometric information, but also the ID, and the system will compare the model extracted from the biometric sensor to the claimed model stored in the database in order to uthenticate the user. In an identification system, the individual provides only biometric data without any extra information, and the system will compare the extracted model to all stored models in the database, and the user is identified if there is a match [1]. Both identification and verification tasks have the same main components in operation including preprocessing, feature extraction, and classification. Also, according to [1], person authentication either involves verifying a claimed person or identifying an unknown person depending on the application. Therefore, the related techniques in published EEG-based person recognition literature was reviewed for the EEG-based person authentication system.

A. EEG signal preprocessing

The human head has different layers including the scalp, skull, brain, and many other thin layers in between, so EEG signals over the scalp are relatively weak and subject to contamination from noise which is generated both inside the brain and the EEG device, for example from power supply interference or changes in electrode impedances [8]. Moreover, EEG signals are known to be subject to contamination from artifacts that usually come from muscular, ocular and heart activity [34] namely electromyography (EMG), electrooculography (EOG), and electrocardiography (ECG) artifacts respectively. After recording, EEG signals need to be preprocessed to reduce these noises and artifacts as much as possible, and band pass filtering, which works by analyzing the signal across a period of time, is a widely applied technique for doing this. Band pass filtering can work on short time segments, and it has proven useful in maximizing the signal-to-noise ratio [35]. In band pass filtering, a high-pass filter is used to remove the very low-frequency noise, for example 0.5 Hz, and a low-pass filter is then used to remove high-frequency noise, for instance 50Hz.

For filtering, in [36] a dataset of 20 subjects who were exposed to a stimulus which consisted of drawings of objects chosen from a Snodgrass and Vanderwart picture set [37], was filtered by a band pass Butterworth filter to obtain the gamma band 30-50Hz. The same stimulus and protocol recording with a dataset of 40 participants was introduced in [38]. The authors proposed an improved method in which an Elliptic Finite Impulse Response (FIR) filter was used because it required a lower order than the Butterworth filter. The band pass filter in this study was 30-70 Hz. Using that dataset, [39] followed two steps for preprocessing. Firstly, eye blink contaminated EEG signals that exceeded a threshold, say 100 μV, were discarded. Then, signals were filtered with a 30-50Hz pass-band using a Butterworth filter. In subsequent research [40] used EEG signals from electrodes C3, C4, P3, P4, O1 and O2 of 5 subjects doing the mental tasks to undertake a band-pass filtering from 0.1 to 100 Hz. After that the baseline noise was reduced by using an Elliptic FIR filter to high-pass filter the EEG signals above 0.5 Hz.

In [41], the Visual Evoked Potentials signals of 70 subjects were filtered with a 30-50Hz pass-band using a 10th order Butterworth digital filter. Before the filtering, eye blinking artifacts were removed by discarding the signals which had a magnitude above 50 μV. Filtering Visual Evoked Potentials signals also can be seen in [42], and [43]. A band-pass filter between 0.1Hz and 100Hz was used by [42] where 10 people were stimulated by self-face and non-self-face images. Moreover, a 50Hz Notch filter was applied to remove line

contamination. In [43], 32 participants were recorded during exposure to reading silently a text with a list of 75 words. After that, a 60 Hz low-pass filter was used to remove the noise out of the major range of the EEG data.

The band pass filter has also been used in other types of EEG data. In [44], raw EEG signals of 7 subjects doing motion tasks had noise removed using a band pass 5Hz-100Hz filter. They also applied this band pass filter to another study in [45] with 4 subjects. In [46], a band-pass Notch filter 1Hz-50Hz was reported used to pre-process a motor imagery dataset with 3 subjects. In [47] the signals of 100 subjects in resting with eyes close were applied a 3rd order Butterworth band pass filter with 0.5 and 45Hz to remove the noises, which could have been caused by hand or body movement.

A summary of some recent studies that have used band pass filtering can be seen in Table 3.

TABLE 3. A SUMMARY OF USED FILTERING TECHNIQUES IN RECENT STUDIES

Paper	Subjects	Control Signal	Filtering technique
[36]	20	VEP	Butterworth filter, band pass 30-50Hz
[38]	40	VEP	Elliptic filter, band pass 30-70Hz
[48]	40	VEP	Butterworth filter, band pass 30-50Hz
[40]	5	Mental tasks	Elliptic filter, high-pass 0.5 Hz
[44]	7	Motion task	Band pass 5Hz-100Hz
[45]	4	Motion task	Band pass 5Hz-100Hz
[41]	70	VEP	Butterworth filter, band pass 30-50Hz
[46]	3	Motor imagery	Notch filter, band pass 1Hz-50Hz
[47]	100	Resting	Butterworth filter, band pass 0.5-45Hz
[42]	10	VEP	Band-pass 0.1-100Hz, 50Hz Notch filter
[43]	32	VEP	Low-pass lter 60 Hz

B. Feature extraction

According to [49], feature extraction in EEG processing is a component "that translates the (artifact-free) input brain signal into a value correlated to the neurological phenomenon". Selecting the representative and stable features from acquired EEG signals is a vital step in an EEG-based biometric system because these features present different degrees of distinctiveness among people [13]. EEG features can be extracted by using a single channel or using information from more than one channel in different domains such as time, time-spatial, and frequency domain. After the feature extraction step, feature vectors are obtained by concatenating the extracted values. These vectors are usually significantly shorter and contain more relevant information than the input brain signals.

A variety of features have been explored and applied on BCI systems [50], and particularly on EEG-based person recognition, in which Autoregressive (AR) and Power spectral density (PSD) are some of the most popular features.

1. Autoregressive features: Autoregressive (AR) is a parametric modelling technique in which a mathematical model is used to formulate a linear prediction in order to describes the signal generation system [51], [52]. The value of each current sample s_n in an AR model is considered to be linearly related to the p most recent sample values [52], [8]:

$$s_n = -\sum_{k=1}^{p} a_k s_{(n-k)} + x_n \quad (1)$$

Where $a_k, k = 1, 2, \dots, p$ are the linear parameters, p is model order n denotes the discrete sample time, and x_n is the noise input.

In terms of EEG signals analysis, the AR model can be applied for a single-channel EEG signals, and then the linear parameters of different EEG channel are taken as the features.

2. Power spectral density features: Power spectral density (PSD) is a function of signal's frequencies in which the distribution of signal power over frequencies is able to be observed. According to [53], the definition of PSD is presented as the discrete time Fourier transform (DTFT) of the covariance sequence (ACS) as follows:

$$\phi(\omega) = \sum_{k=-\infty}^{\infty} r(k) e^{-i\omega k} \quad (2)$$

where the auto covariance sequence $r(k)$ is defined as:

$$r(k) = E\{y(t) y^*(t-k)\} \quad (3)$$

while $y(t)$ is the discrete-time signal $\{y(t); t = 0, \pm 1, \pm 2, \dots\}$ which it is assumed to be a sequence of random variables with zero mean.

$$E\{y(t)\} = 0 \text{ for all } t \quad (4)$$

To estimate power spectral density, some methods in nonparametric approach have been applied such as [54, 55]. These methods uses periodogram for estimating the power of a signal at different frequencies, but the Welch method can reduce noise and the frequency resolution compared to the standard Bartlett's method. As a result, Welch method is adopted in this research for the experiments.

Similar to AR model, the PSD estimation in EEG signals analysis can be applied for a single-channel EEG signals, and then the energy within a specific frequency range of different EEG channel are taken as the features.

Variety of studies have applied AR model and PSD as features. In [56], Poulos et al. proposed a person identification method based on parametric spectral of EEG signals. AR model order 8^{th} were extracted from 1 channel (O2) on alpha band using a dataset of 4 subjects in resting and eyes closed. Experimental results obtained a correct classification range from 72-84%. The authors stated that this result is consistent to their previous studies to prove that EEG signals carry genetic information. In [57], AR model was used to examine the characteristics of the EEG as a biometric with a dataset of 40 subjects. EEG data was recorded on 8 channels while subjects were in resting with eyes open (EO) and eyes closed. The authors used only one channel P4 as it typically contains the alpha rhythm to investigate AR models with the orders varied from 3^{th} to 21^{th}. The result showed that 100% of subjects are correctly identified when all data is used while the accuracy is over 80% when using 50% data for training and the remain for testing. The study also finds out impact of AR model order on the classifying accuracy as stated "the model order is increased from 3 to 21 the level of correct classification increases and remains high across an increasing number of subjects". Also, in [58], autoregressive (AR) model was extracted from 4 channels C3, P3, C4, and P4 for person identification using a dataset of 10 participants resting with eyes open and eyes closed in 5 different sessions in a course of 2 weeks. The order of AR model was tested from 3^{th} to 21^{th}. Different experiments were conducted using eyes close and eyes open data separately in 1 channel, a combination of channels, and all 4 channels. The authors observed that eyes close EEG signals in 4 channels gave the best recognition rate of 97%.

Not only applying for resting state EEG signals, AR could be applied for EEG data which is elicited by different protocols. In [44], AR models were investigated for person authentication purpose using EEG signals from 7 participants performing motion related tasks. After preprocessing data with a band pass filter 5-100Hz, 17 channels were divided into ve regions including (F7,Fp1,F3), (Fp2,F8,F4), (FZ,C3,CZ,C4,PZ), (P3,P7,O1) and (P4,P8,O2) to make 5 Dominating Independent Components (DIC) by applying independent component analysis. AR coefficients were calculated for each channel from each DIC, and combined to make feature vector. Some AR model orders were tested, and the best overall performance is HTER=4.1% with AR order 5^{th} to 7^{th}. Further, in [59] the authors proposed using electrical brainwave signals during imagined speech for person identification as it easy to do and no need any external stimuli. EEG data was recorded from 6 participants imagining speaking one of two syllables, /ba/ and /ku/. After preprocessing, feature extraction was followed by computing AR coefficients on the gamma band for each of 96 channels using the Burg method with the orders from 2^{th} to 6.... Experiments showed the best identification accuracy of 99.76%, and the optimal AR order for the imagined speech EEG dataset was 2^{th}. The proposed approach was also tested on another dataset of 120 subjects whose EEG signals corresponding to Visual Evoked Potentials (VEPs). The results showed a classification accuracy of 98.96% with the optimal order AR was 4^{th}.

Autoregressive feature was also combined to some other feature to investigate using EEG signals as biometrics. In [60], five different features including Autoregression (AR) order 100^{th}. Fourier transform (FT), Mutual information (MI), coherence (CO), and cross-correlation (CC) were extracted and analyzed on the frequency range 0.5-70Hz from a dataset of 87 subjects in resting with eyes close. Data signals on two electrodes (FP1 and FP2) were divided into 4 second epochs for feature extraction. After conducting experiments with 51 subjects and 36 intruders, the authors obtained an equal error rate (EER) of 3.4%. Similarity, Palaniappan [40] proposed a two-stage authentication method using AR and some other features. EEG signals of 5 subjects were recoded while doing some mental task such as math, geometric gure rotation, letter composing, and visual counting. Signals from 6 channels C3, C4, P3, P4, O1 and O2 were extracted to obtain features of autoregressive coefficients (AR) order 6^{th}, channel spectral powers and inter-hemispheric channel spectral power differences, inter-hemispheric channel linear complexity, and non-linear complexity. In the stage one, the threshold Th1 was used to reduce the false accept error (FAE) while another threshold Th2 was applied to reduce the false

reject error (FRE) in the stage two on 6 channels. Experiments show that two-stage authentication method obtains FAE=0%, and FRE ranging from 0% to 1.5%. The combination of AR and some other features also can be seen in [46] where the author focused on person authentication problem by using AR, Linear Complexity (LC), Energy Spectrum Density (ESD), Energy Entropy (EE), Phase Locking Value (PLV), Mutual Information (MI) and Cross Correlation. Features were extracted on the frequency of 2-40Hz from the electrodes C3, C4, P3, P4, O1 and O2. Experiments were conducted on 3 subjects performing imagery left hand, right hand, foot or tongue movements according to a cue. The author obtained the False acceptance rate (FAR) from 0% to 30%, and the True acceptance rate (TAR) from 80% to 100%.

Regarding power spectral density (PSD), the authors in [6] tried to explore this feature when they investigated the use of brain activity for person authentication. EEG data was recorded from 9 subjects during doing some tasks including imagination of left hand, right hand movement, and generation of words. Power spectral density (PSD) in the band 8-30 Hz was calculated using the Welch periodogram algorithm [55] for the eight centroparietal channels C3, Cz, C4, CP1, CP2, P3, Pz, and P4. Eight channels with 12 frequency components make the feature vector of 96 dimensions. Some protocol experiments were conducted, and the best result obtained HTER=7.1%. The authors also noted that PSD features in their experiment could give better performances than more elaborated features such as parameters of autoregressive models and wavelets. Using both AR and PSD features can be found in some works such as [61, 62]. More detail, in [61] an EEG-based person authentication system is proposed using a set of features from a dataset of 5 subject performing some mental imagery tasks. Firstly, each one second segment data was extracted from each of 14 electrodes to obtain three sets of features including AR coefficients order 6^{th}, PSD, and total power in five frequency bands from alpha band to gamma band. Secondly, interhemispheric power differences and interhemispheric linear complexity were extracted and combined to the previous 3 set of features to present a feature vector. Experimental results show that the task of referential limb movement activity give the best performance with FRR=2.4% and FAR=0.7%. In [62], Nguyen et al. investigated both AR and PSD as features for person verification using EEG signals of 9 people performing the motor imagery of left hand and right hand. Three channels C3, C4 and Cz were selected for feature extraction. AR model order 21^{th}, and PSD with the Welch's averaged modified periodogram method [55] were estimated in the band 8-30Hz to make the feature vector of 3*(21+12)=99 dimensions. The authors obtained the best equal error rate (EER) of 4%. In another study [63], the same feature extraction method was applied, but the number of used electrodes was 6 including C3, C4, Cz, P3, P4 and Pz. The method was tested with several datasets. Both datasets of 40 subjects doing free task, and the one with 90 participants performing motor imagery gave the EER of 2.21% while the VEP dataset of 120 subjects brought a result of EER=3.5%.

B. Classifier algorithms

EEG signals are noisy and sometimes the noise is considerably stronger than the signal [64]. Another important issue in EEG analysis is the large temporal variation between subjects and even within subjects. As a result, EEG analysis becomes an interesting and challenging field of knowledge discovery, data mining and machine learning.

Using a suitable classifier is important to EEG-based person authentication since different machine learning algorithms present different capabilities for determining the boundary which separates EEG data into classes of genuine and impostor [13]. This research focused on using Support Vector Machine (SVM) and Support Vector Data Description (SVDD) because of their success in published EEG signals analyses [50, 65].

1. Support Vector Machine (SVM) : Support vector machine (SVM) [66, 67] aims to find an optimal hyperplane for separation of training data without errors. Let $\{x_i \dots x_n\}$ be training vectors, where $x_{i=}R^d$, n is number of vectors, and d is the dimension of feature space. Each vector x_i is labeled by $y_i \in \{-1,1\}$. The hyperplane $f(x)$ is defined as follows:

$$f(x) = \omega^T \phi(x) + b \qquad (5)$$

where ω is normal to the hyperplane, $\phi(.)$ is a transformation function, and b is a constant. The optimal hyperplane with maximum margin can be

obtained by solving the following optimization problem:

$$min\frac{1}{2}\|\omega\|^2 + C\sum_{i=1}^{l}\xi_i \quad (6)$$

subject to

$$y_i[\omega^T\phi(x_i + b) \geq 1 - \xi_i \text{ and } x_i \geq 0, i = 1, \dots, l \quad (7)$$

where $\xi_i = 1, \dots, l$ are slack variables and C is a parameter chosen by the user.

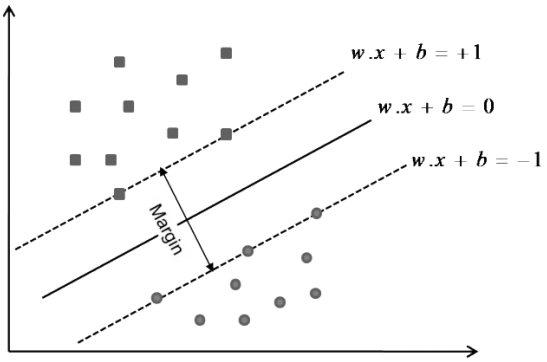

Figure 8. Support Vector Machine [67]

In the testing phase an unknown data sample x is determined to be normal if $f(x) = +1$ or abnormal if $f(x) = -1$ by computing:

$$f(x) = \sum_{i}^{N_S} \propto_i y_i\phi(S_i)^T\phi(x) + b = \sum_{i}^{N_S} \propto_i y_i K(S_i, x) + b \quad (8)$$

where S_i are the support vectors, N_S is the number of support vectors, and K is the kernel with $K(x_i, x_j) = \phi(x_i)^T\phi(x_j)$.

2. Support Vector Data Description (SVDD):

Support Vector Data Description was proposed by [68] in which the main idea is to determine an optimal hypersphere in the feature space containing all normal data samples, while abnormal data samples are not included. Let $X = \{x_1, x_2, \dots, x_n\}$ be the normal data set, R be the radius of the hypersphere and c be the centre of the hypersphere. The optimisation problem of the hypersphere is achieved by minimising its square radius R^2 as follows:

$$\min_{R,c,\xi}\left(R^2 + C\sum_{i=1}^{n}\xi_i\right) \quad (9)$$

subject to

$$\|\phi(x_i) - c\|^2 \leq R^2 + \xi_i \quad i = 1, \dots, n \quad (10)$$
$$\xi_i \geq 0, \quad i = 1, \dots, n$$

where C is a parameter to control the trade-off between the volume of the hypersphere and the errors, $\xi = |\xi_i|_{i=1,\dots,n}$ is the vector of slack variables, $\phi(.)$ is the transformation function related to the kernel function $K(x_1, x_2) = \phi(x_1)^T\phi(x_2)$, and n is number of normal data points.

An unknown data point x is classified based on the decision function: $f(x) = sign\,(R^2 - \|\phi(x_i) - c\|^2)$. If $f(x) = +1$, the unknown data point x is considered as normal while it is abnormal if $f(x) = -1$.

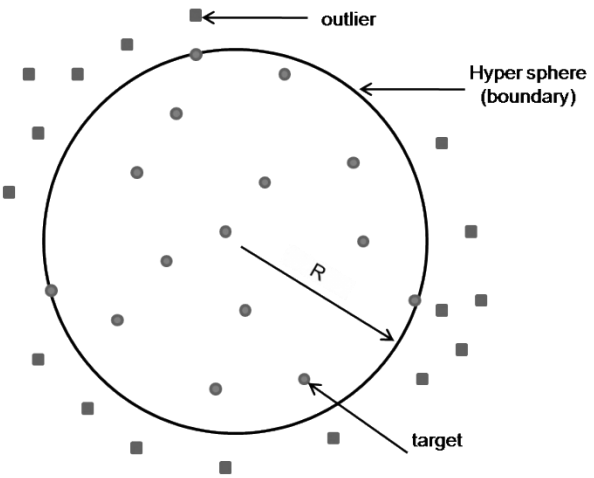

Figure 9. Support Vector Data Description

In [69], linear SVM was used to classify 20 people while the authors investigated the potential of using EEG signals for person identification. Visual Evoke Potentials data from 20 electrodes were divided into 0.5s epochs to compute the coefficients of the LDA feature extraction matrix. Classification phase was conducted with SVM algorithm using cross-validation from 2 to 10 fold. Also Discriminant Analysis based on linear discriminant function was used for a thorough investigation. Experiments show that SVM outperformed LDA significantly, and both SVM and LDA obtained the best accuracy at 10-fold cross validation with 94.08% and 87.78% respectively. According to the authors, the highly non-Gaussian distribution of the EEG data could be the reason of the superior SVM performance. Also, linear SVM was applied in [59] to classify 6 persons using electrical brainwave signals which were recorded while subjects doing imagined speech. After extracting features with AR model on the gamma band, data was divided in training and testing sets for classification with the LibSVM software package [70], but the exact ratio of the data for training and testing was not presented. The k-Nearest Neighbors classifier also was used

to compare the performance to SVM. Experiments showed the best identification accuracy of 99.76%, and 99.41% to SVM and k-NN, respectively. Moreover, the data of one session, about 25%, was used for training while the data of each of other sessions, totally about 75%, were used for testing to investigate the session-to-session variability. The authors observed that the classification performance decreases when the testing session is far from training session; therefore, according to the authors, updating the training set with current data after identification is needed. The proposed approach was also tested on another dataset of 120 subject whose EEG signals corresponding to Visual Evoked Potentials (VEPs). The results showed a classification accuracy of 98.96% for linear SVM, and 96.34% for k-NN classifier. In addition, linear SVM was used to classify the feature vectors with a one-versus-all approach in [61]. EEG data of 5 people was recorded during performing four mental imagery tasks including baseline measurement, referential limb movement, counting, and rotation for 10 sessions, 15 seconds each were divided into 15 blocks for each task after extracting the features. The samples of 14 blocks of each task, about 93%, were fed into the classifier for training, and the left 1 block of each task, about 7%, was used for testing. The authors obtained the experimental results of FRR=2.4% and FAR=0.7%.

Other kernel functions of SVM also can be seen in the published works. In [42], SVM Gaussian kernel was explored for person authentication. Experiments were conducted with a dataset of 10 subject exposing to self-face and non-self-face images as stimulus. The dataset consists 2 sessions on different days with 2 runs each session. For each run, 50 trials were composed, so there are 200 trials for each participant. Features then were calculated based on the difference of brain signals in response to self-face and non-self-face images. The feature vectors of 180 trials were used for training, and the rest, 20 trials, were used for evaluation. The 10-fold cross validation was run to evaluate of the system. Authors obtained an average accuracy of 85%, a False Acceptance Rate (FAR) of 14.5%, and a False Rejection Rate (FRR) of 14.5%. In [71], SVM classifier was compared to LDA and BP neural network algorithms in person identification. EEG signals of 13 people in resting state with eye closed were followed AR model feature extraction, and then 66% data were fed into the classifier for training while 34% were used for testing. Experiments showed the best accuracy of 87.1%, 75%, and 87% to SVM, BP neural network, and LDA, respectively. Although SVM and LDA had the similar experimental results, the authors prioritized SVM as it is suitable for small sample and training time is short.

Regards to SVDD algorithm, Zuquet et al. proposed using SVDD with a Radial Basis Function kernel for EEG-based person authentication in [41]. Visual Evoked Potentials signals in the γ band of 70 subjects were extracted the energy of differential EEG signals on 8 occipital electrodes, then 30 features, about 66%, of each person was fed into the classifier to train that one's model and 15 features, about 34%, was used for testing. Authors observed an average performance of TAR=92.5%, and FAR=6.27%. KNN algorithm with k=1 was also tested to compare the performance to SVDD, and it achieved TAR=78.5% and FAR=3.4% on average. Although the authors concluded both classifiers having advantages and disadvantages, SVDD seems to be superior since it obtained a much higher TAR than KNN while KNN only had a little bit smaller FAR than SVDD. Also, the authors try to evaluate the ability to improve the performance of the system by combining the outputs of SVDD and KNN with OR and AND combinations. AND KNN-SVDD provided the average result of TAR=90.4% and FAR=3% while the average performance of OR KNN-SVDD were TAR=90.8% and FAR=3.14%. Also, SVDD with a Radial Basis Function kernel was used by [62] for person verification using EEG signals of 9 people performing the motor imagery of left hand and right hand. AR model order 21th and PSD were estimated in the band 8-30Hz on 3 channels to make the feature vector of 3*(21+12)=99 dimensions. Firstly, 5-fold cross validation training was run to find out the best parameters. Secondly, the found parameters were applied to train the models using training set, and evaluate using testing set which is separated from training set. Gaussian Mixture Model (GMM) also was used as another classifier. The authors obtained the best equal error rate (EER) of 4%, and 4.41% for SVDD and GMM, respectively. In another study [63], the Multi-Sphere SVDD universal background model (UBM) was used. The method was tested with several datasets. Both datasets of 40 subjects doing free task, and the one with 90

participants performing motor imagery gave the EER of 2.21% while the VEP dataset of 120 subjects brought a result of EER=3.5%.

V. RESEARCH DIRECTIONS

EEG signals are responses to the activities that are generated inside the human brain, so they are private, and very difficult to mimic or steal. Moreover, recording EEG data requires a live person. These peculiarities are not shared by the most commonly used biometrics, such as face, iris, voice and fingerprints. As a result, the use of EEG signals for security particular in authentication purpose is receiving serious attention from the research community. Nevertheless, there are some gaps and directions in current research on security systems and EEG-based person authentication which itself involves the high security, performance, usability, and stability of the system need to be addressed as follow.

1. The performance of an EEG-based person authentication system depends on data pre-processing, feature extraction and modeling techniques. Numerous pre-processing, feature extraction and modeling techniques have been proposed and explored that focus on accuracy, but no technique has been identified as the best [50]. False acceptance rate (FAR) and false rejection rate (FRR) are commonly used to evaluate the performance of an authentication system. These two measurements can be controlled by adjusting a threshold, but it is not possible to exploit this threshold by simultaneously reducing FAR and FRR. Therefore, a flexible authentication mechanism that can improve both of these measurements is necessary and feasible options to achieve this need to be investigated.

2. EEG signals are week and subject to contamination from many artifact signals that usually come from muscular, ocular and heart activity [34] namely electromyography (EMG), electrooculography (EOG), and electrocardiography (ECG) artifacts, respectively. It is not easy to clearly separate the artifacts from the true EEG signals. A method which is simple to implement and easy to use and overcomes the EEG artifacts issue should be considered for EEG-based person authentication system.

3. EEG signals are usually recorded by placing electrodes on the scalp of a person. Many such EEG acquisition protocols have been employed for person identification and verification such as motor imagery [6, 72], mental tasks (e.g., mental multiplication) [40], and responses to visual stimuli (i.e., Visual Evoked Potentials (VEPs)) [59]. These protocols have their own disadvantages. Motor imagery and mental tasks are difficult to perform, and they require users to be trained [59]. VEPs is a slow method and not universally applicable since some users are visually impaired. Moreover, EEG recording experiments usually have been conducted in a dimly lit room with complex medical devices, so it is really difficult for a real life EEG-based authentication system to function optimally. Also according to [73] the difficulties faced by humans while interacting with the system in real life situations can fail a security solution despite its highly secure technical design. Therefore, an EEG-based person authentication method that is easy and comfortable to use is really desired.

4. The reproducibility of an EEG biometric is an issue that has not received the necessary attention from researchers [13]. There are only a few non-comprehensive analyses that have been conducted and all of them focus on session to session EEG stability during the time from 1 week to 5 months [23-25]. There is no publication that clarifies the stability of an EEG pattern for authentication purposes in varied emotions, yet EEG signals are known to be sensitive to emotion [6, 24]. In real life EEG-based person authentication system, a person usually records EEG signals for enrollment in a calm or normal emotional state, but in verification attempts he or she may be in a quite different emotional state because it is impossible for a person to remain calm all the time. As a result, the impact of varied emotional states on the stability of an EEG-based person authentication system needs to be thoroughly investigated.

5. EEG signals can be used for person authentication because they are unique and repeatable. This evidence introduces the idea that stable EEG patterns can be used to seed cryptographic keys. As a result, combining EEG biometrics and cryptography is a promising and interesting direction.

VI. CONCLUSION

Using EEG signals for authentication has the of both password based and biometric based authentication approaches, yet without their drawbacks. Firstly, EEG signal are biometric information of individuals. Secondly, brain patterns correspond to particular tasks, and they be regarded as individualized passwords. As the

result, EEG based authentication can overcome the disadvantages of password based and conventional biometric based authentication. In this paper we have presented a comprehensive review on the state-of-the-art of EEG-based authentication systems. An overview of the EEG signals as new type of biometrics has been provided, and then employed data recording and filtering protocols, features extraction algorithms, and classification algorithms which were used in state-of-the-art approaches have been detailed. Some gaps and directions in current research on using EEG signals for security systems particular in authentication purpose also have been suggested.

REFERENCES

[1]. W. Stalling and L. Brown, "Computer security: Principles and practice-third edition", William Stallings, 2015.

[2]. R. S. Sandhu and P. Samarati, "Access control: principle and practice", Communications Magazine, IEEE, vol. 32, no. 9, pp. 40-48, 1994.

[3]. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pp. 4-20, 2004.

[4]. C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics", EURASIP Journal on Information Security, vol. 2011, no. 1, pp. 1-25, 2011.

[5]. V. Matyas and Z. Riha, "Security of biometric authentication systems", in Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on. IEEE, pp. 19-28, 2010.

[6]. S. Marcel and J. d. R. Millan, "Person authentication using brainwaves (eeg) and maximum a posteriori model adaptation", Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29, no. 4, pp. 743-752, 2007.

[7]. B. Obermaier, C. Neuper, C. Guger, and G. Pfurtscheller, "Information transfer rate in a five-classes brain-computer interface", Neural Systems and Rehabilitation Engineering, IEEE Transactions, vol. 9, no. 3, pp. 283-288, 2001.

[8]. S. Sanei and J. A. Chambers, "EEG signal processing", Wiley Interscience, 2008.

[9]. G. N. G. Molina, T. Ebrahimi, and J.-M. Vesin, "Joint time-frequency-space classification of eeg in a brain-computer in-terface application", EURASIP journal on applied signal processing, vol. 2003, pp. 713-729, 2003.

[10]. F. Lotte, "Study of electroencephalographic signal processing and classification techniques towards the use of brain-computer interfaces in virtual reality applications", Ph.D. dissertation, INSA de Rennes, 2008.

[11]. F. Sharbrough, G. Chatrian, R. Lesser, H. L¨ uders, M. Nuwer, and T. Picton, "American electroencephalographic society guidelines for standard electrode position nomenclature", J. clin. Neurophysiol, vol. 8, no. 2, pp. 200-202, 1991.

[12]. E. A. Curran and M. J. Stokes, "Learning to control brain activity: a review of the production and control of eeg components for driving brain computer interface (BCI) systems", Brain and cognition, vol. 51, no. 3, pp. 326-336, 2003.

[13]. P. Campisi and D. La Rocca, "Brain waves for automatic biometric based user recognition", 2014.

[14]. M. Poulos, M. Rangoussi, N. Alexandris, A. Evangelou et al., "Person identification from the EEG using nonlinear signal classification", Methods of information in Medicine, vol. 41, no. 1, pp. 64-75, 2002.

[15]. J. Berkhout and D. O. Walter, "Temporal stability and individual differences in the human EEG: an analysis of variance of spectral values", IEEE Transactions on Biomedical Engineering, vol. 3, no. BME-15, pp. 165-168, 1968.

[16]. F. Vogel, "The genetic basis of the normal human electroen- cephalogram (EEG)", Humangenetik, vol. 10, no. 2, pp. 91-114, 1970.

[17]. J. J. Lynch, D. A. Paskewitz, and M. T. Orne, "Inter-session stability of human alpha rhythm densities", Electroencephalography and clinical neurophysiology, vol. 36, pp. 538-540, 1974.

[18]. B. P. Zietsch, J. L. Hansen, N. K. Hansell, G. M. Geffen, N. G. Martin, and M. J. Wright, "Common and specific genetic influences on EEG power bands delta, theta, alpha, and beta", Biological psychology, vol. 75, no. 2, pp. 154-164, 2007.

[19]. T. Gasser, P. B¨ acher, and H. Steinberg, "Test-retest reliability of spectral parameters of the EEG", Electroencephalography and clinical neurophysiology, vol. 60, no. 4, pp. 312-319, 1985.

[20]. M. Salinsky, B. Oken, and L. Morehead, "Test-retest reliability in EEG frequency analysis", Electroencephalography and clinical neurophysiology, vol. 79, no. 5, pp. 382-392, 1991.

[21]. M. N¨ apflin, M. Wildi, and J. Sarnthein, "Test–retest reliability of resting eeg spectra validates a statistical signature of persons", Clinical Neurophysiology, vol. 118, no. 11, pp. 2519-2524, 2007.

[22]. L. McEvoy, M. Smith, and A. Gevins, "Test–retest reliability of cognitive eeg", Clinical Neurophysiology, vol. 111, no. 3, pp. 457-463, 2000.

[23]. D. La Rocca, P. Campisi, and G. Scarano, "On the repeatability of EEG features in a biometric recognition framework using a resting state protocol", in BIOSIGNALS, pp. 419-428, 2013.

[24]. H. J. Lee, H. S. Kim, and K. S. Park, "A study on the reproducibility of biometric authentication based on electroen-cephalogram (EEG)", in Neural Engineering (NER), 2013 6th International IEEE/EMBS Conference on. IEEE, pp.13-16, 2013.

[25]. R. Palaniappan and K. Revett, "Pin generation using EEG: a stability study", International Journal of Biometrics, vol. 6, no. 2, pp. 95-105, 2014.

[26]. K.-Y. Lee and D. Jang, "Ethical and social issues behind brain computer interface", in Brain-Computer Interface (BCI), 2013 International Winter Workshop on. IEEE, pp. 72-75, 2013,.

[27]. A. Stopczynski, D. Greenwood, L. K. Hansen, and A. Pentland, "Privacy for personal neuroinformatics", Available at SSRN 2427564, 2014.

[28]. T. Bonaci, R. Calo, and H. J. Chizeck, "App stores for the brain: Privacy & security in brain-computer interfaces", in Ethics in Science, Technology and Engineering, 2014 IEEE International Symposium on. IEEE, pp. 1-7, 2014.

[29]. C.-F. Lin, S.-H. Shih, and J.-D. Zhu, "Chaos based encryption system for encrypting electroencephalogram signals", Journal of medical systems, vol. 38, no. 5, pp. 1-10, 2014.

[30]. P. T. Nguyen, "On EEG-based person recognition and human characteristics classification", 2015.

[31]. H. Stassen, "Computerized recognition of persons by EEG spectral patterns", Electroencephalography and clinical neurophysiology, vol. 49, no. 1, pp. 190-194, 1980.

[32]. J. Thorpe, P. C. van Oorschot, and A. Somayaji, "Pass thoughts: authenticating with our minds", in Proceedings of the 2005 workshop on New security paradigms. ACM, 2005, pp. 45-56, 2005.

[33]. A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The det curve in assessment of detection task performance", DTIC Document, Tech. Rep, 1997.

[34]. M. Fatourechi, A. Bashashati, R. K. Ward, and G. E. Birch, "Emg and eog artifacts in brain computer interface systems: A survey", Clinical neurophysiology, vol. 118, no. 3, pp. 480-494, 2007.

[35]. A. Vallabhaneni, T. Wang, and B. He, "Braincomputer interface", in Neural engineering. Springer, pp. 85-121, 2005.

[36]. R. Palaniappan, "Method of identifying individuals using vep signals and neural network", IEE Proceedings-Science, Measurement and Technology, vol. 151, no. 1, pp. 16-20, 2004.

[37]. J. G. Snodgrass and M. Vanderwart, "A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity", Journal of experimental psychology: Human learning and memory, vol. 6, no. 2, pp.174, 1980.

[38]. R. Palaniappan and D. P. Mandic, "Energy of brain potentials evoked during visual stimulus: A new biometric?", in Artificial Neural Networks: Formal Models and Their Applications – ICANN 2005. Springer, pp. 735-740, 2005.

[39]. K. Ravi and R. Palaniappan, "Leave-one-out authentication of persons using 40 hz eeg oscillations", in Computer as a Tool, 2005. EUROCON 2005. The International Conference on, vol. 2. IEEE, pp. 1386-1389, 2005.

[40]. R. Palaniappan, "Two-stage biometric authentication method using thought activity brain waves", International Journal of Neural Systems, vol. 18, no. 01, pp. 59-66, 2008.

[41]. A. Z´ uquete, B. Quintela, and J. P. da Silva Cunha, "Biometric authentication using brain responses to visual stimulus", In BIOSIGNALS, pp. 103-112, 2010.

[42]. S.-K. Yeom, H.-I. Suk, and S.-W. Lee, "Eeg-based person authentication using face stimulus", in Brain-Computer Interface (BCI), 2013 International Winter Workshop on. IEEE, pp. 58-61, 2013.

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

[44]. C. He and Z. J. Wang, "An independent component analysis (ICA) based approach for eeg person authentication", in Bioin-formatics and Biomedical Engineering, 2009. ICBBE 2009. 3rd

International Conference on. IEEE, pp. 1-4, 2009.

[45]. C. He, X. Lv, and J. Wang, "Hashing the mar coefficients from EEG data for person authentication", in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. IEEE, pp. 1445-1448, 2009.

[46]. H. Jian-feng, "Biometric system based on eeg signals by feature combination", in Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on, vol. 1. IEEE, pp. 752-755, 2010.

[47]. H. A. Shedeed, "A new method for person identification in a biometric security system based on brain EEG signal processing", in Information and Communication Technologies (WICT), 2011 World Congress on. IEEE, pp. 1205-1210, 2011.

[48]. K. Ravi and R. Palaniappan, "Neural network classification of late gamma band electroencephalogram features", Soft Computing, vol. 10, no. 2, pp. 163-169, 2006.

[49]. S. Mason, A. Bashashati, M. Fatourechi, K. Navarro, and G. Birch, "A comprehensive survey of brain interface technology designs", Annals of biomedical engineering, vol. 35, no. 2, pp. 137-169, 2007.

[50]. F. Lotte, M. Congedo, A. L´ Ecuyer, F. Lamarche, B. Arnaldi et al., "A review of classification algorithms for EEG-based brain-computer interfaces", Journal of neural engineering, vol. 4, 2007.

[51]. J. Makhoul, "Linear prediction: A tutorial review", Proceedings of the IEEE, vol. 63, no. 4, pp. 561-580, 1975.

[52]. J. Pardey, S. Roberts, and L. Tarassenko, "A review of parametric modelling techniques for EEG analysis", Medical engineering & physics, vol. 18, no. 1, pp. 2-11, 1996.

[53]. P. Stoica and R. L. Moses, "Spectral analysis of signals", Pearson/Prentice Hall Upper Saddle River, NJ, 2005.

[54]. M. S. Bartlett, "Smoothing periodograms from time series with continuous spectra", Nature, vol. 161, no. 4096, pp. 686-687, 1948.

[55]. P. Welch, "The use of fast fourier transform for the estimation of power spectra: a method based on time averaging over short, modified periodograms", IEEE Transactions on audio and electroacoustics, pp. 70-73, 1967.

[56]. M. Poulos, M. Rangoussi, V. Chrissikopoulos, and A. Evangelou, "Person identification based on parametric processing of the EEG", in Electronics, Circuits and Systems, 1999. Proceedings of ICECS'99. The 6th IEEE International Conference on, vol. 1. IEEE, pp. 283-286, 1999.

[57]. R. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric", in Electrical and Computer Engineering, 2001. Canadian Conference on, vol. 2. IEEE, pp. 1363-1366, 2001.

[58]. M. K. Abdullah, K. S. Subari, J. L. C. Loong, and N. N. Ah-mad, "Analysis of effective channel placement for an EEG-based biometric system", in Biomedical Engineering and Sciences (IECBES), 2010 IEEE EMBS Conference on. IEEE, pp. 303-306, 2010.

[59]. K. Brigham and B. V. Kumar, "Subject identification from electroencephalogram (EEG) signals during imagined speech", in Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on. IEEE, pp.1-8, 2010.

[60]. A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis", EURASIP Journal on Advances in Signal Processing, vol. 2008, pp. 18, 2008.

[61]. C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-cost electroencephalogram (EEG) based authentication", in Neural Engineering (NER), 2011 5th International IEEE/EMBS Conference on. IEEE, pp. 442-445, 2011.

[62]. P. Nguyen, D. Tran, X. Huang, and W. Ma, "Motor imagery EEG-based person verification", in Advances in Computational Intelligence. Springer, pp. 430-438, 2013.

[63]. P. Nguyen, D. Tran, T. Le, X. Huang, and W. Ma, "EEG-based person verification using multi-sphere SVDD and UBM", in Advances in Knowledge Discovery and Data Mining. Springer, pp. 289-300, 2013.

[64]. A. Flexer, "Data mining and electroencephalography", Statistical Methods in Medical Research, vol. 9, no. 4, pp. 395-413, 2000.

[65]. X. Wu, V. Kumar, J. R. Quinlan, J. Ghosh, Q. Yang, H. Motoda, G. J. McLachlan, A. Ng, B. Liu, S. Y. Philip et al, "Top 10 algorithms in data mining", Knowledge and Information Systems, vol. 14, no. 1, pp. 1-37, 2008.

[66]. B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers", in Proceedings of the feifth annual workshop on Computational learning theory. ACM, pp. 144-152, 1992.

[67]. C. Cortes and V. Vapnik, "Support-vector networks", Machine learning, vol. 20, no. 3, pp. 273-297, 1995.

[68]. D. M. Tax and R. P. Duin, "Support vector data description", Machine learning, vol. 54, no. 1, pp. 45-66, 2004.

[69]. K. Das, S. Zhang, B. Giesbrecht, and M. P. Eckstein, "Using rapid visually evoked EEG activity for person identification", in Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE. IEEE, pp. 2490-2493, 2009.

[70]. C.-C. Chang and C.-J. Lin, "Libsvm: A library for support vector machines", ACM Transactions on Intelligent Systems and Technology (TIST), vol. 2, no. 3, pp. 27, 2011.

[71]. Z. Dan, Z. Xifeng, and G. Qiangang, "An identification system based on portable EEG acquisition equipment", in Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on. IEEE, pp. 281-284, 2013.

[72]. S. Sun, "Multitask learning for EEG-based biometrics," in Pattern Recognition, 2008. ICPR 2008. 19th International Conference on. IEEE, pp. 1-4, 2008.

[73]. J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore I am: Usability and security of authentication using brainwaves," in Financial Cryptography and Data Security. Springer, 2013, pp. 1-16, 2013.

[74]. http://fingerchip.pagespersoorange.fr/biometrics/accuracy.html.

ABOUT THE AUTHORS

MS. Phạm Tiến Dũng

Workplace: The Central for Information Technology and Network Security Monitoring, Vietnam Government Information Security Commission.

Email: ptdung@bcy.gov.vn

The education process: Receiving bachelor degree in 2000 and master degree in 2008 from the Academy of Cryptography Techniques.

Research today: the field of computer security, biometrics, and machine learning.

MS. Đinh Hoàng Gia

Workplace : The Central for Information Technology and Network Sercurity Monitoring, Vietnam Government Information Security Commission.

Email: dhgia@bcy.gov.vn

The education process: Receiving bachelor degree in 1999 and master degree in 2012 from the Academy of Cryptography Techniques.

Research today: cryptography, web security, network security.

MS. Lê Khải

Workplace : The Central for Information Technology and Network Sercurity Monitoring, Vietnam Government Information Security Commission.

Email: lekhai@bcy.gov.vn

The education process: Receiving bachelor degree in 2004 and master degree in 2013 from the Academy of Cryptography Techniques.

Research today: applying EEG to user authentication, applying EEG to real-time authentication.

PhD. Đào Thị Hồng Vân

Workplace : The Central for Information Technology and Network Sercurity Monitoring, Vietnam Government Information Security Commission.

Email: dhvan@bcy.gov.vn

The education process: Receiving bachelor degree in 1995 and master degree in 2004 from the Academy of Cryptography Techniques. Reciving PhD mathemmatic in 2012.

Research today: web security, data security, applying EEG to network information technology.