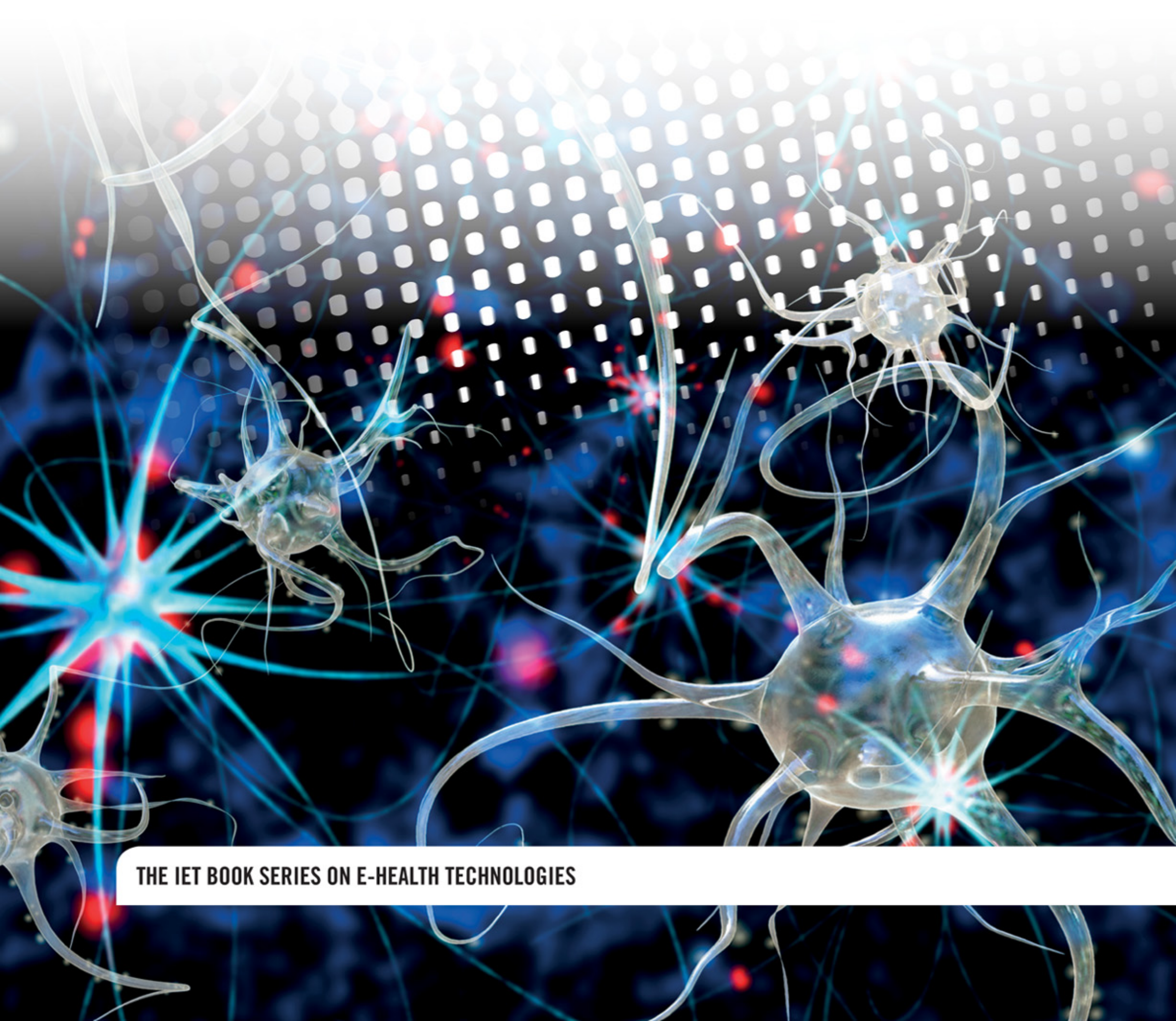
The Institution of Engineering and Technology

EEG Signal Processing

Feature extraction, selection and classification methods

Edited by
Wai Yie Leong



THE IET BOOK SERIES ON E-HEALTH TECHNOLOGIES

IET HEALTHCARE TECHNOLOGIES SERIES 16

EEG Signal Processing

Other volumes in this series:

Volume 1	**Nanobiosensors for Personalized and Onsite Biomedical Diagnosis** P. Chandra (Editor)
Volume 2	**Machine Learning for Healthcare Technologies** D.A. Clifton (Editor)
Volume 3	**Portable Biosensors and Point-of-Care Systems** S.E. Kintzios (Editor)
Volume 4	**Biomedical Nanomaterials: From design to implementation** T.J. Webster and H. Yazici (Editors)
Volume 6	**Active and Assisted Living: Technologies and applications** F. Florez-Revuelta and A.A. Chaaraoui (Editors)
Volume 7	**Semiconductor Lasers and Diode-based Light Sources for Biophotonics** P.E. Andersen and P.M. Petersen (Editors)
Volume 9	**Human Monitoring, Smart Health and Assisted Living: Techniques and technologies** S. Longhi, A. Monteriù and A. Freddi (Editors)
Volume 13	**Handbook of Speckle Filtering and Tracking in Cardiovascular Ultrasound Imaging and Video** C.P. Loizou, C.S. Pattichis and J. D'hooge (Editors)
Volume 14	**Soft Robots for Healthcare Applications: Design, modelling, and control** S. Xie, M. Zhang and W. Meng

EEG Signal Processing

Feature extraction, selection and classification methods

Edited by
Wai Yie Leong

The Institution of Engineering and Technology

Published by The Institution of Engineering and Technology, London, United Kingdom

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no. 211014) and Scotland (no. SC038698).

First published 2019

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way, Stevenage
Herts, SG1 2AY, United Kingdom

www.theiet.org

British Library Cataloguing in Publication Data
A catalogue record for this product is available from the British Library

ISBN 978-1-78561-370-8 (hardback)
ISBN 978-1-78561-371-5 (PDF)

Typeset in India by MPS Limited
Printed in the UK by CPI Group (UK) Ltd, Croydon

Contents

This page intentionally left blank

Foreword

A Brain Computer Interface (BCI) system monitors the brain activity and translates features related to the user's intent or feeling, into device commands. The electro-encephalography (EEG) is the most common method in order to record the brain activity in BCI systems. It is a non-invasive method that requires relatively simple and inexpensive equipment, and it is easier to use than other methods. Nevertheless, EEG-based BCIs provide modest speed and accuracy so it is necessary to use multichannel systems and proper signal processing methods. EEG signal processing is divided into several stages: feature extraction, selection and classification.

Feature extraction methods obtain specific information from EEG signals. These features can be useful in order to discriminate among different mental tasks. Then, using selection methods, a subgroup of the most relevant features for classification is chosen, namely

- Spectral features achieved from Fourier transform.
- Blind source separation
- Optimisation approach
- Autoregressive models
- Nonlinear methods
- Genetic algorithms
- Unsupervised learning

Feature classification methods allow from the selected features, to determine what class is the most probable for a specific sample. To that purpose, the aims of the book is to focus on Feature extraction methods to obtain specific information from EEG signals. These features can be useful in order to discriminate among different mental tasks. This book emphasizes strategies, case studies and clinical practices. Advanced Signal Processing methods will also be discussed in this title.

Ir Prof Wai Yie Leong

Chapter 4

Person authentication using electroencephalogram (EEG) brainwaves signals

Siaw-Hong Liew[1], Yun-Huoy Choo[1], Yin Fen Low[2], and Zeratul Izzah Mohd Yusoh[1]

This chapter starts with the introduction to various types of authentication modalities, before discussing on the implementation of electroencephalogram (EEG) signals for person authentication task in more details. In general, the EEG signals are unique but highly uncertain, noisy, and difficult to analyze. Event-related potentials, such as visual-evoked potentials, are commonly used in the person authentication literature work. The occipital area of the brain anatomy shows good response to the visual stimulus. Hence, a set of eight selected EEG channels located at the occipital area were used for model training. Besides, feature extraction methods, i.e., the WPD, Hjorth parameter, coherence, cross-correlation, mutual information, and mean of amplitude have been proven to be good in extracting relevant information from the EEG signals. Nevertheless, different features demonstrate varied performance on distinct subjects. Thus, the Correlation-based Feature Selection method was used to select the significant features subset to enhance the authentication performance. Finally, the Fuzzy-Rough Nearest Neighbor classifier was proposed for authentication model building. The experimental results showed that the proposed solution is able to discriminate imposter from target subjects in the person authentication task.

4.1 Introduction

Person authentication or verification is different from person identification. Person authentication or verification result is a one-to-one matching and it gives a yes or no answer (as shown in Figure 4.1). Meanwhile, person identification system is one-to-N matching where an individual identity is determined from a group of persons who are being evaluated [1]. Most of the past literature have focused on

[1]Computational Intelligence and Technologies (CIT) Research Group, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
[2]Machine Learning and Signal Processing (MLSP) Research Group, Centre for Telecommunication Research and Innovation (CeTRI), Faculty of Electronics and Computer Engineering, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia

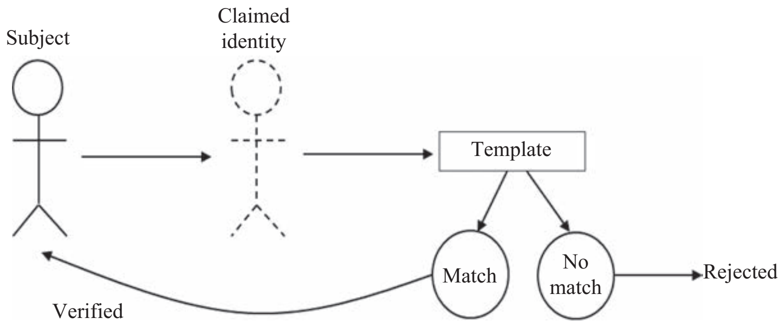


Figure 4.1 The principle of person authentication; one-to-one matching [2]

person identification. However, person authentication is increasingly catching the researcher's attention in line with the emergence of security as one of the important research topics recently. Applications of person authentication such as airport security checking, building gate control, passport confirmation, computer login, internet banking, ATM access, etc., are widely used. An identity authentication system has to deal with two kinds of events: either the person claiming a given identity is the one who he or she claims to be (in which case, he or she is called a client), or he or she is not (in which case, he or she is called an impostor). Moreover, the system may generally take two decisions: either accept the client or reject him or her and decide whether he or she is an impostor.

Several types of methods can be used to authenticate a person from others. Traditional methods of authentication such as knowledge-based and token-based are widely used methods. A password-based system is one of the examples of systems that are established on knowledge-based method while signature is an example of the system established on token-based method. With many new methods of person authentication, most of the people still prefer the use of signature and password as an authentication method because it is easier and does not need any maintenance [3]. Unfortunately, password model and signature are no longer considered reliable enough to satisfy the security requirements because password can be stolen and guessed easily by shoulder surfing and signature can be forged easily. The traditional authentication methods suffer from their inability to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of the authorized person [4].

Biometric authentication systems were introduced to overcome traditional authentication methods. Biometric is any measurable, physical or physiological feature or behavioral trait that can be used to authenticate the claimed identity of an individual [5]. The major difference between biometric and traditional authentication method is the way how it authenticates a person based on the physical characteristic. It relies on "something that you are" to differentiate between an authorized person and a fraudulent imposter [4]. Physiological biometrics include fingerprint, face, iris, hand geometry, retina, and body odor, while behavioral biometrics include voice, keystroke dynamics, and gait [6]. Nevertheless, these modalities are still facing many challenges. A biometric authentication as long as it satisfies the following requirements [7]:

- **Universality:** Every person should have the characteristics.
- **Uniqueness:** Every person should have different characteristics.
- **Constancy:** The characteristic should remain fairly constant with time.
- **Collectability:** The characteristic can be measured quantitatively.

Fingerprint authentication system considers one of the most popular and oldest biometrics authentication systems. However, due to the advancement of technologies and the evilness of human beings, fingerprint can be imitated, which brings down the uniqueness of it. Apart from that, fingerprint system depends largely on the surface of one's finger. People with physical disabilities or severe injuries such as missing hands or burned fingers are unable to use this system. Other than that, fingerprint nowadays is not secure due to the advancement of technology. There is some research showing that fingerprint can be forged and various algorithms are being developed to detect fingerprint forgery [8]. Fingerprint is public as we place it everywhere when we touch something. Fingerprint authentication system can be forged using artificial fingers and fingerprints made from readily available materials (e.g., silicon, gelatin) or even cadaver fingers (finger of a dead person) [5].

Meanwhile, facial recognition is a computer application that uses face to distinguish an individual from another. It is the most natural means of biometric authentication [9]. Nevertheless, it is less reliable because the human face structure will evolve and change throughout the lifecycle of human due to genetic or environmental factors. Besides, face recognition is not a perfect biometric authentication method because it is dependent on light, facial expression, resolution, and form of hair of an individual [10]. Individual features may not be easily distinguished in poor light condition. Most of the facial recognition systems require the user to stand a specific distance away from the camera and look straight at the camera. This is to ensure that the captured image of the face is within a specific size tolerance and keeps the features in as similar position each time as possible.

Voice can also act as a biometric method in person authentication because every person has a different pitch and it is unique. The sound is produced when air leaves the body of an individual through oral cavity (mouth), nasal cavity (nose), and larynx. Obstructions such as lips, teeth, tongue, size, and position are used to produce sound [10]. However, with the advancement of technology, voice can be easily recorded and forged by an attacker. In addition, voice recognition can be easily affected by environmental factors such as background noise. It might take hours to record the voice, but the system tends to make error.

Hand geometry recognition system was once popular 10 years ago, but it is seldom used nowadays [10]. This recognition system is based on the shape of the hand of an individual, which differs from another person, and the shape of hand does not change after certain age [9]. The main advantages of hand geometry recognition are ease of use, low cost, and simplicity. Environmental factors such as dry skin cannot have influence on the results. Unfortunately, it is less reliable because the measurements of this method are measuring and recording only the length and height of the fingers, shape of the knuckles, distance between joints, and surface area of the hand. Hand geometry recognition system is ideal for adults but not for growing children as their hand characteristics can change in time.

Palmprint refers to an image required of the palm region of the hand. It can be used as a biometric for authentication system. In 1858, palmprint was first introduced by Sir William Herschel in India [11]. Palmprint carries similarities with fingerprint and it consists of some properties such as universality, uniqueness, stability, and collectability for authentication. Every person has a different palmprint; even the palmprints of twins are different. Palmprint area is larger than fingerprint area and hence it provides more information about the person. The features include the principal lines, wrinkles, minutiae, ridges, and delta points of the palms. Palmprinting does not bring any harm to the health of people. Palmprint can be easily captured with low-resolution (at most 400 dpi) devices and thus the devices are not expensive [11]. However, the palmprint authentication system has limitation to mobile users as the size of the palmprint is bigger.

Iris recognition nowadays is with the combination of technologies from several fields such as pattern recognition, optics, and computer vision. Iris is a small internal organ and it is protected by cornea, eyelid, and aqueous humor. It is a unique characteristic of an individual and it does not change during the whole life. As iris is a small internal organ, it is hard to scan from a distance. Furthermore, individuals with eye problems such as cataracts and blindness will have problem using this kind of system due to the inability to scan their iris [10].

Retina scan also acts as biometric authentication, which is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than iris scan technology, which also uses a part of the eye. It is rarely used nowadays as it is not user friendly and the equipment remains very expensive. The retina scanning system is believed to be very accurate as it has reputedly never falsely verified an unauthorized user so far. However, the main disadvantage of the retina scan is its intrusiveness. The way to obtain retina is personally invasive and the operation of the retina scanner is not easy. A laser light must be directed through the cornea of the eye.

With the shortcomings that have been mentioned above, there is a need to use a biometric that is unique, confidential, and impossible to duplicate in person authentication. Thus, EEG signals is one of the biometric systems that can be used to overcome this problem.

4.2 The human brain

Human brain consists billions of nerve cells that make a large complex neural network. Each of the nerves in the human brain is connected to about 10,000 other nerves. The average human brain weighs around 1,400 g [12]. Human brain can be divided into four portions: brain stem, cerebral cortex, cerebellum, and diencephalon (hypothalamus and thalamus). Cerebral cortex can be divided into two hemispheres and these are connected to each other via corpus callosum. Each

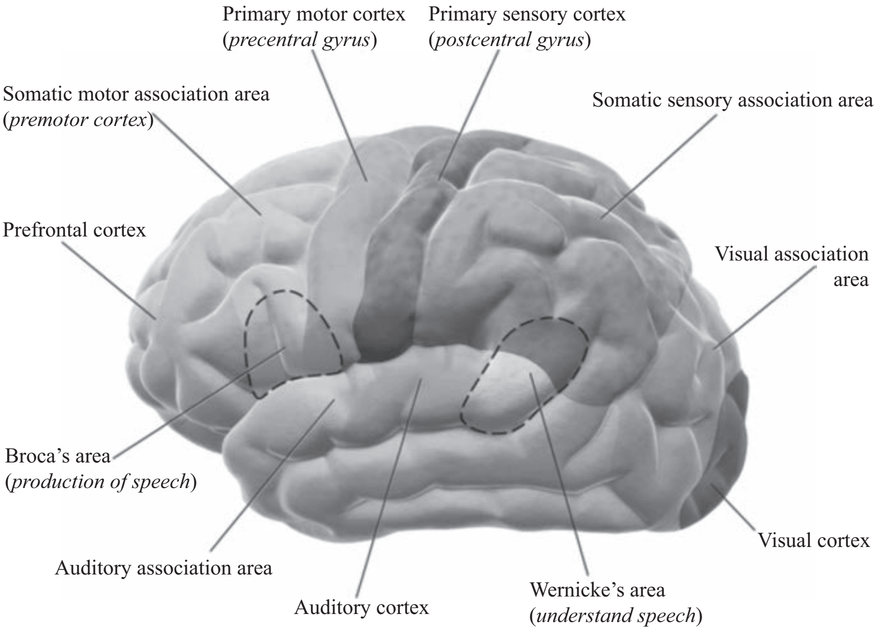


Figure 4.2 The function of the brain [13]

Table 4.1 Cortical area of the brain and their function [13]

Cortical area	**Function**
Primary Motor Cortex	Initiation of voluntary movement
Somatic Motor Association Cortex	Coordination of complex movement
Prefrontal Cortex	Problem solving, emotion and complex thought
Broca's Area	Speech production and articulation
Auditory Cortex	Detection of sound quality (loudness, tone)
Auditory Association Area	Complex processing of auditory information
Wernicke's Area	Language comprehension
Visual Cortex	Detection of simple visual stimuli
Visual Association Area	Complex processing of visual information
Sensory Association Cortex	Processing of multisensory information
Primary Somatosensory Cortex	Receives tactile information from the body

hemisphere can be divided into four lobes: frontal, parietal, occipital, and temporal. The cerebral cortex can be divided into several areas as shown in Figure 4.2.

The functions of cerebral cortex are problem solving, processing of complex visual information, and language information. The functions of each cortical area are described in Table 4.1.

4.3 Electroencephalogram (EEG)

In 1929, the first signal of electroencephalogram (EEG) was recorded by Berger. EEG signals are brain activities that are recorded from electrodes mounted on the scalp. EEG signals are the product of ionic current flows that happen in the brain's neurons. Some of the connections are excitatory while others are inhibitory. EEG signals have been categorized into six basic rhythms [12] as shown in Table 4.2: Gamma (γ), Beta (β), Mu (μ), Alpha (α), Theta (θ), and Delta (δ). With the advancement in hardware devices, EEG is the most practical method that can be used in biometric. EEG is the most practical capturing method that can be used in biometrics due to the advances in its hardware devices.

The advantages of using brain electrical activity in EEG signals are unique and confidential; the recorded brain response cannot be duplicated, and a person's identity is therefore unlikely to be stolen. A research work done by [7] shows that the EEG signals of a person is unique and differ from person to person, even when they are performing the same task or thought when responding to same visual stimuli. EEG signals can be easily affected, but they cannot be easily reproduced under conditions of stress, fatigue, anxiety, drowsiness, medication, environment, etc. [14]. For example, a person who has been forced or pointing a gun to the head will create different EEG signals from a normal person who is in a relaxed state. In the security aspect, the EEG-based authentication system is not immune to phishing attacks. EEG signals are not 100% identical [15]. With the strength and uniqueness of EEG signals, we believe that the EEG signals are reliable and suitable to be used as a biometric in authentication system.

The EEG recording electrodes and their function are critical for obtaining high-quality data for interpretation [16]. One important problem of EEG signals recording is the artifacts. Examples of the artifacts in EEG signals recording are blinking, head movements, muscle activity, and electrocardiogram. Due to the very low amplitude of EEG signals, artifacts often contaminate the recordings restricting or making difficult in analysis or interpretation. Therefore, the position of subjects

Table 4.2 EEG signal rhythms [12]

Rhythm	Bandwidth	Description
Gamma (γ)	[30,40] Hz	Low in amplitude; can indicate event brain synchronization; and be used to confirm some brain disorders.
Beta (β)	[13,30] Hz	Indicates an alert state, with active thinking and attention.
Mu (μ)	[8,13] Hz	Locates in the motor and sensorimotor cortex; the amplitude varies when the subject performs movements.
Alpha (α)	[8,12] Hz	Indicates a relaxed state, with little or no attention, mainly appear at occipital lobe.
Theta (θ)	[4,8] Hz	Indicates creative inspiration or deep meditation; can also appear in dreaming sleep (REM stage).
Delta (δ)	[0.5,4] Hz	Primarily associated with deep sleep or loss of body awareness, but can be present in the waking state.

during EEG recording should be comfortable enough to avoid unwanted activities; a lying position diminishes the occurrence of some artifacts caused by feeble motion.

Research work done by [1] has obtained highest accuracy of 93.4% for person authentication with a dataset of nine normal subjects performing three tasks during twelve non-feedback sessions over 3 days, which is four sessions per day. A modality for biometric authentication based on EEG signals done by [17] has three tasks of classification accuracy: reading task (97.3%), relax task (94.4%), and multiplication task (97.5%). They analyzed a dataset of 8-channel EEG recordings from 40 volunteer subjects when performing simple tasks such as resting with eyes open and resting with eyes closed. In addition, research work done by [18] used the BCI competition 2003 dataset with the EEG recording from a 64-channel and sampled in 250 Hz. The authentication classification result obtained by [18] ranged from 75% to 85%.

4.3.1 Event-related potentials

Event-related potentials (ERPs) are the potential changes in the EEG signals that occur in response to "event" or stimulus. The changes of the EEG signals are very small and the EEG signals have to be averaged from many trials in order to reveal them. ERPs can be divided into two categories: exogenous (involuntary) and endogenous (voluntary). Exogenous ERPs normally occur up to about 100 ms after the stimulus onset while endogenous ERPs occur from 100 ms onward. It depends on the properties of physical stimulus and behavioral processes related to the event.

The most commonly studied ERP is P300. P300 indicates that positive deflection in EEG occurs approximately 300 ms after the stimulus onset. This effect was present for visual (light flashes) and auditory (clicks) stimuli [19]. P300 is commonly recorded during an "oddball paradigm" where a target stimulus is presented infrequently among more common distracter stimuli. On the other hand, evoked potentials (EPs) is a subset of the ERP, which rise in response to a certain physical stimulus such as visual-evoked potential (VEP), auditory-evoked potential (AEP), and somatosensory-evoked potential (SEP).

Motor imagery is one of the ERP activities. The subjects performed three tasks such as left-hand movements, right-hand movements, and word generation beginning with the same random letter. The classification accuracy achieved about 80% in the research work [20]. One of the ideas that combined EEG signals with authentication system was proposed by [21]. The authentication system was designed by using pass-thoughts, which is reliable and could work as EEG signals are unique and impossible to duplicate.

4.3.2 Visual-evoked potential

EEG signals can be recorded in several types of condition, for example, baseline activity, math activity, letter composing activity, and VEP [22]. The EEG signals recorded when an individual is in a relaxed condition is called baseline activity. The EEG signals recorded in [5] when people were in baseline activity are used to identify the people. Math activity is a simple mathematical equation such as addition, subtraction, multiplication, and division, which a person had to solve without vocalizing and making any movements. A person who was asked to compose a letter to a friend without vocalizing is called letter composing activity. Furthermore, VEP is one of the ERPs that are brain activities that respond to visual stimuli and recorded from the occipital scalp electrode.

VEP is the operational measurement of the visual journey from the retina to the visual cortex of the brain using the optic nerves. The main advantages of VEP signals are short training time, high data transmission rate, and no significant effect on the subjects. VEP may compromise several components such as texture, color, objects, motion, readability (i.e., text vs non-text), and others. Each of these components produced different frequency bands due to the impact in special dispersion of the VEP through the scalp. Therefore, production of VEP should be the focus and stimulate in the same brain area.

Research work in [23] proposed a new method to identify individuals using VEP signals. A dataset of 61-channels placed on the scalp is taken from 20 subjects. The average VEP classification accuracy obtained for identification is 94.18%. Furthermore, the classification accuracy ranged from 95% to 98% for a personal identification experiment based on VEP signals that were recorded from 102 subjects [24]. Malinka [25] designed and implemented VEP as a biometric characteristic. The author proved that VEP is fully suitable for the biometric recognition and the result showed that eight occipital channels are enough to build the biometric authentication system.

The authors in [7] proposed to use brainwave signals that respond to visual stimuli for the purpose of verification. Typically the active electrode is placed over the occipital cortex defined by the International Standard 10–20 EEG System. Research work in [7] considered 8 occipital channels from a total of 64 channels available in dataset for building their authentication system. They presented an EEG authentication system by conducting experiments to investigate the similarities and differences during picture recognition process. A standard set of 260 black-and-white line pictures from [26] will be used in the experiment. The result showed that eight occipital channels are enough to build the biometric authentication system.

EEG signals are unique and particularly strong when a person is exposed to visual stimuli [15]. The main advantage of EEG signal is that it can detect changes over milliseconds. In the research work [15], the authors interviewed a neurologist and EEG expert, Dr Jesper Ronager, who worked at the national hospital of Denmark, Rigshospitalet in Copenhagen. Dr Jesper Ronager mentioned that the visual cortex area of the brain is located at the occipital area and it is the best place to measure EEG signals and the most informative for finding picture recall thought patterns. According to Dr Jesper Ronager, it should not be a problem if the sensors or electrodes are not placed millimeter-precise.

Because EEG signals are highly sensitive to the emotional state, Lee *et al.* [27] studied in EEG-based authentication using three different tasks, i.e., the resting state, the visual stimuli, and the movement or the mental tasks to reduce the high

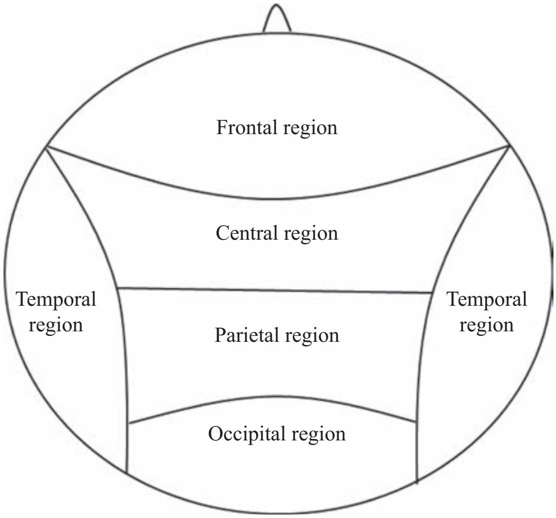


Figure 4.3 Six primary brain regions [28]

sensitivity of the EEG signals on emotional state. The EEG recording measured during resting state by using two channels gained the classification accuracy in the range from 87.5% to 98.1%. Next, the EEG signals recorded from two channels in mental task had the classification accuracy in the range from 91.6% to 97.5% in classification rate. Last but not least, the studies on the VEP gained the best result compared to resting state and mental tasks. The classification result ranged from 92.9% to 98.1%.

4.3.3 Electrode placements

The EEG signals are recorded with electrodes mounted on the scalp. The electrodes are small, conduct electricity, and provide electrical contact between the EEG recording apparatus and the skin by transforming the ionic current on the skin to the electrical current in the wires. Different tasks associated different functional regions in the brain are depicted in Figure 4.3. The frontal region is responsible for problem solving and movement control; the central region manages the initiation of voluntary movement and coordination of complex movement; the parietal region receives sensory information from the body; the temporal region detects sound and performs auditory processing; while the occipital region detects visual stimuli and processes the visual information.

The arrangement of the electrodes is normally based on the International 10–20 system (Figure 4.4). The distance between the electrodes is 10% and 20% and the system consists of 21 electrodes. Each electrode position has a letter and a number to identify the location. The letters C, F, O, P, and T stand for central, frontal, occipital, parietal, and temporal lobes, respectively. Odd numbers indicate the

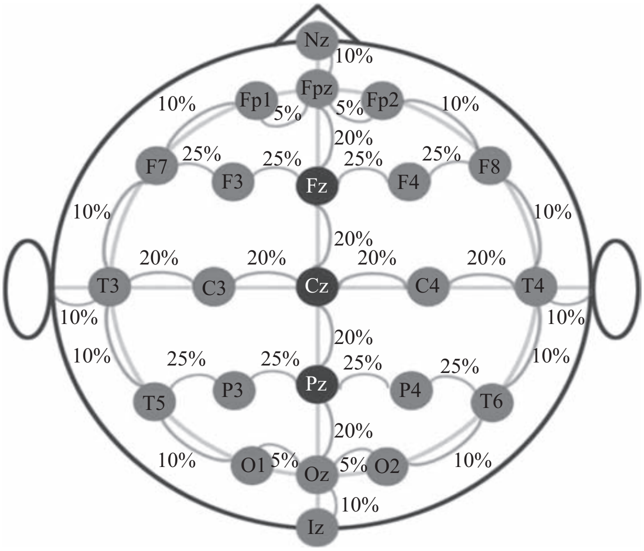


Figure 4.4 International 10–20 electrode placements [29]

electrode position on the left side and even numbers indicate the electrode position on the right side. Z stands for zero and refers to the electrode placements at midline.

Nevertheless, the system allows the use of additional electrodes. The new letter codes for intermediate sites are: AF—intermediate between frontal pole and frontal, FC—between frontal and central, FT—intermediate between frontal and temporal, CP—intermediate between central and parietal, TP—intermediate between temporal and parietal, and PO—intermediate between parietal and occipital. Figure 4.5 shows the 64 EEG electrodes placements.

4.4 Experimentation

A simple flow chart as illustrated in Figure 4.6 describes the person authentication model. It consists of several steps that are EEG signal recording, segmentation, filtering, artifact rejection, feature extraction, feature selection, and classification. Finally, users are classified as client or impostor according to the classification algorithm.

4.4.1 EEG signal recording and segmentation

Collected raw EEG data are non-stationary, noisy, complex, and difficult to analyze. Thus, segmentation according to trials must be performed prior to further analysis such as feature extraction, feature selection, and classification. On the other hand, filtering and artifact rejection are also important to avoid misleading information on signal interpretation. The reading with excessive body movements or others types of artifacts will be discarded.

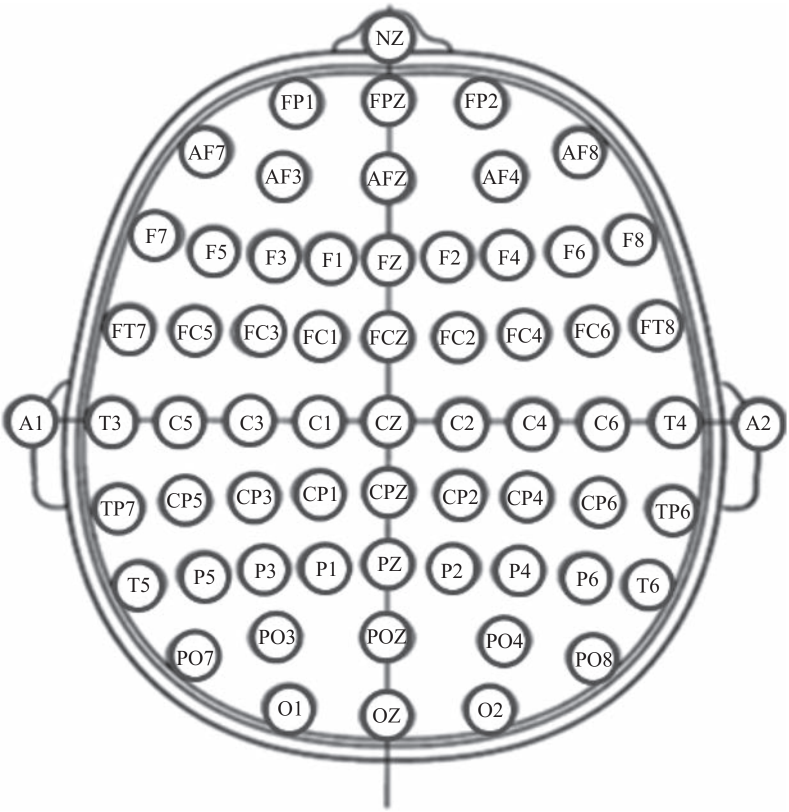


Figure 4.5 The 64 EEG electrode placements [29]

Figure 4.6 EEG-based authentication model

4.4.2 Feature extraction

Feature extraction is to extract the relevant information or characteristics from the EEG signals. Features extracted from EEG signals are unique between subjects and sufficient for person authentication [18]. Different features provide different discriminative power for different subjects. Most of the authentication system will make use of features combination architecture. The results were able to demonstrate significant improvement in the system performance [30]. The feature extraction methods used in this study are as follows:

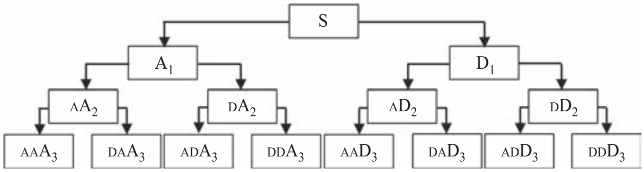


Figure 4.7 Level 3 of wavelet packet decomposition (WPD) tree

4.4.2.1 Wavelet packet decomposition

In [31], the authors have demonstrated wavelet packet decomposition (WPD) is an excellent feature extraction method for non-stationary signals such as EEG signals and it is very appropriate for EEG signals analysis. WPD provides a multilevel time–frequency decomposition of signals and is able to provide more significant features. The wavelet decomposition splits the original signal into detail and approximation coefficients, respectively. After that, the approximation is split into next level approximation and detail. This process will be repeated until n-level. On the other hand, the detail also is split into the next level to yield more than different ways to encode the signal. Figure 4.7 shows a complete decomposition tree of a signal.

Research work by [32] has proven that Daubechies with order 4 (DB4) wavelet and sixth level of WPD is an appropriate parameter in order to analyze the EEG signals with 256-Hz sampling rate. As the frequency of useful EEG signals is lower than 50 Hz, we use 25 sub-bands in each channel. The combination with the time domain and frequency domain can provide more significant features; we characterized the time–frequency distribution of EEG signals by combining the features below:

Average coefficients in sixth sub-band: A total of 8 channels were selected from 64 available channels in the dataset and the sampling rate for each channel is 2^8, the sub-band means (M_j) at jth level is defined as in (4.1):

$$M_j = \frac{1}{2^j} \sum_{k}^{2^8} d_j(k) \tag{4.1}$$

where $d_j(k)$ represents the coefficient of WPD at jth level and kth sample. Twenty-five sub-bands were used for WPD as the frequency of useful EEG signal is lower than 50 Hz. Therefore, the dimensions of feature vector for average coefficients are 200.

Wavelet packet energy in each sub-band: In the perspective of wavelet packet energy, WPD decomposes signal energy on different time-frequency plain; the integration of square amplitude of WPD is proportional to signal power. The sub-band entropy is defined as in (4.2):

$$E(j,n) = \int |S(t)|^2 dt = \sum_k \left(d_j^n(k)\right)^2 \tag{4.2}$$

where $n = 0, 1, 2, \ldots, 2^j$. As eight channels were selected in this research, the dimensions of feature vector for wavelet packet energy was 200.

4.4.2.2 Hjorth parameter

Hjorth parameter is essential to analyze EEG signals in both time and frequency domains. It can extract the property of EEG signals efficiently [33]. Hjorth parameters are used to compute the quadratic mean and the dominant frequency of EEG signals on each side of the brain: we used the first two Hjorth descriptors in 1970 and 1973, namely activity and mobility. From the activity and mobility in the EEG signals, it reflects the global trend of a signal, for visual analysis. Hjorth parameters were used in various online EEG analyses, such as in sleep staging in order to compute the amplitude and the main frequency of a signal. These descriptors are chosen because they have a low calculation cost [34].

Let us consider the spectral moment of order 0 and 2:

$$m_0 = \int_{-\pi}^{\pi} S(w)dw = \frac{1}{T}\int_{t-T}^{t} f^2(t)dt \tag{4.3}$$

$$m_2 = \int_{-\pi}^{\pi} w^2 S(w)dw = \frac{1}{T}\int_{t-T}^{t} \left(\frac{df}{dt}\right)^2 dt \tag{4.4}$$

where $S(w)$ represents the power density spectrum and $f(t)$ represents the EEG signal within an epoch of duration T. The first two of Hjorth parameters are given by

$$\text{Activity} : h_0 = m_0 \tag{4.5}$$

$$\text{Mobility} : h_1 = \sqrt{\frac{m_2}{m_0}} \tag{4.6}$$

where h_0 is the square of the quartic mean and h_1 reflects the frequency of dominant. These quantities are in discrete forms, where $h_0(k)$ and $h_1(k)$ at a sampled time of k are calculated within a sliding window of 1s length using the open source software library BioSig.

Besides that, Hjorth parameter has also used the fourth-order spectral moment m_4 to define a measure of the bandwidth of the signal called complexity.

$$\text{Complexity: } h_2 = \sqrt{\frac{m_4}{m_2} - \frac{m_2}{m_0}} \tag{4.7}$$

The first parameter is Activity, which represents the signal power; Mobility represents the mean frequency; and Complexity represents the change in frequency.

4.4.2.3 Coherence

Coherence is a feature used to measure the degree of linear correlation between two signals. The correlation between two time series at different frequencies can be uncovered by coherence. Coherence is normally used for analyzing the condition of different cognitive disorders. It has been proved that EEG-based coherence analysis can be used in biometrics [15]. The range value for the magnitude of the squared coherence estimate is between 0 and 1, which quantizes how well x corresponds to y at each frequency. The value of 0 for the coherence function means the independence between two signals. The value of 1 for the coherence function means the complete linear dependence. The formula of coherence is given as follows:

$$C_{xy}(f) = \frac{\left|P_{xy}(f)\right|^2}{P_{xx}(f)P_{yy}(f)} \tag{4.8}$$

where $C_{xy}(f)$ is a function of the power spectral density $\left(P_{xx} \text{ and } P_{yy}\right)$ of x and y, and the cross-power spectral density P_{xy} of x and y.

4.4.2.4 Cross-correlation

The main idea of the cross-correlation, also known as sliding dot product, is to measure the similarity of two channels. Cross-correlation is used to find occurrences of a known signal in unknown one [35]. Additionally, it is a function of the relative delay between the signals, which can be applied in pattern recognition and cryptanalysis. Two input signals will be used to compute the cross-correlation:

- Channel 1 with itself: ρ_X
- Channel 2 with itself: ρ_Y
- Channel 1 with channel 2: ρ_{XY}

The correlation ρ_{XY} between two random variables x and y with expected values, μ_x and μ_y, and standard deviation, σ_x and σ_y, is given as:

$$\rho_{X,Y} = \frac{\operatorname{cov}(X, Y)}{\sigma_X \sigma_Y} = \frac{E((X - \mu_X)(Y - \mu_Y))}{\sigma_X \sigma_Y} \tag{4.9}$$

where $E(X)$ is the expectation operator and $\operatorname{cov}(X)$ is the covariance operator.

4.4.2.5 Mutual information

In information theory and probability theory, the mutual information is used to measure the relationship between two signals that are sampled simultaneously. In other words, mutual information measures how much the information is communicated in one input signal about another. The common unit of mutual information measurement is the bit when we used logarithms of base 2 in its computation [30].

4.4.2.6 Mean of amplitude

Mean, also known as average, is the sum of all EEG potential value and divided by the number of samples. The expression of the mean is given in (4.10):

$$\overline{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \tag{4.10}$$

where n is the number of data and x_i is the value of data.

In our earlier work in [36], we have compared the performance of three feature extraction methods (coherence, cross-correlation, and mean of amplitude) and six feature extraction methods (WPD, Hjorth parameter, mutual information, coherence, cross-correlation, and mean of amplitude). The six feature extraction methods are good to extract important attributes for person authentication.

4.4.3 Feature selection

The WPD method tends to induce large vector set especially when the selected EEG channels increase. Thus, the feature selection process is important to reduce the features set before combining the significant features with the other small feature vectors set. Feature selection plays an important role especially for the large dataset. Three common models for feature selection are the filter model, the wrapper model, and the embedded model. Filter methods investigate the prior knowledge among features to select the best discriminating subset. Therefore, understanding the data features is important to produce a good filter model. On the other hand, wrapper methods employ a predetermined induction algorithm to find a subset of features with the highest evaluation quality by searching through the feature subsets space. The wrapper method is more time consuming than the filter method because it is strongly coupled with an induction algorithm. It calls the induction algorithm repetitively to evaluate the performance of each feature's subset [37] during the performance evaluation process.

The Correlation-based Feature Selection (CFS) often referred as cfsSubsetEval in WEKA is a correlation-based feature selector. CFS is a good feature selection method that is able to reduce dimensionality without affecting accuracy [37]. It is a fast and correlated-based filter algorithm that is applicable in discrete and continuous problems. The CFS algorithm evaluates the feature subset according to the correlation-based heuristic merit. A good feature subset contains high correlation between features and the class [38]. In our earlier work in [36], the experiments were designed in two levels, i.e., select the attributes from WPD feature vectors using CFS algorithm before combining with other feature vectors; and to apply the CFS feature selection across all feature vectors at the same time. The experiment results showed that the feature selection applied on the WPD only gained better classification accuracy and AUC.

4.4.4 Classification

Fuzzy-Rough Nearest Neighbor (FRNN) classifier was proposed in our previous work [36,39] and used to evaluate the performance for person authentication. It is a fuzzy-rough version of WEKA data mining tools. FRNN classifier was first introduced by Jensen and Cornelis [40], which combined the strength of fuzzy sets, rough sets, and nearest neighbors classification approach motivated by human decision making. In FRNN algorithm, the nearest neighbors are used to construct the fuzzy lower and upper approximations to quantify the membership value of a test object to determine its decision class, and test instances are classified based on their membership to these approximations. FRNN algorithm follows the fundamental of fuzzy-nearest neighbors approach in classifying objects into the most probable decision class. However, instead of using the fuzzy membership function, FRNN capture the uncertainty with the fuzzy-rough approximations. FRNN classification approach used in [36] and [39] have gained good results for person authentication using EEG signals.

Fuzzy logic connectives play important role in the development of fuzzy-rough set theory. A triangular norm (t-norm), T is any increasing, commutative, and associative $[0,1]^2 \rightarrow [0,1]$ mapping, satisfy $T(1, x) = x$, for all x in [0,1]. On the other hand, an implicator is any $[0,1]^2 \rightarrow [0,1]$ mapping $\mathscr{F}$ satisfying $\mathscr{F}(0,0) = 1$, $\mathscr{F}(1, x) = x$, for all x in [0,1]. In [40], they have used Kleene–Dienes implicator for x, y in [0,1].

Various types of performance measurements such as accuracy, recall, precision, and area under receiver operating characteristics curve (AUC) are used to evaluate the efficiency of the results. Accuracy and AUC were selected based on literature review. Although accuracy is commonly used to analyze results, it is not a good performance measurement at all the times because it provides less meaningful information by omitting false positives in its measurement. False positives provide useful information on tolerance up to a certain extent. In addition, AUC is gaining more popularity for judging classifier properties by providing a graphical method. It is a very useful performance measure by calculating AUC learning curves for very large datasets. It cannot be denied that AUC curves are provided very meaningful of both theoretical and empirical justification. AUC is found to have a more discriminating value and statistically consistent compared to the accuracy.

4.5 Results and discussion

A EEG dataset from UCI Machine Learning and EEG dataset from UCI Machine Learning Repository were used in the experiments. Large dataset was used in this research and it consists of 10 subjects with 64 channels electrode placement. Each individual is completed with a total of 60 trials and sampled at 256 Hz. Due to many redundant trials in one of the subjects; it was replaced by another subject from the full dataset. This is necessary to ensure that the prediction ability is not biased due to the redundant data in both training and testing phase. Instead of treating the classification as a ten-class problem, the classifier was trained with only two outputs, i.e., the client and the imposter. The data were split into 80% of training and 20% of testing. In this study, we have considered the electrodes at occipital area. The eight electrodes are PO7, PO3, POZ, PO4, PO8, O1, OZ, and O2 as suggested in [7].

Table 4.3 shows the classification performance of FRNN in person authentication modeling. The classification accuracy and AUC obtained in the experiment were 92.67% and 0.951, respectively. From the results shown in Table 4.3, we can conclude that the FRNN model is suitable for EEG signals classification for person authentication modeling.

Table 4.3 Classification performance of FRNN in person authentication modeling

Person	True positive rate (TPR)	False positive rate (FPR)	Accuracy (%)	AUC
Person 1	0.967	0.226	96.67	0.976
Person 2	0.917	0.157	91.67	0.954
Person 3	0.908	0.381	90.83	0.950
Person 4	0.900	0.604	90.00	0.894
Person 5	0.992	0.075	99.17	1.000
Person 6	0.875	0.458	87.50	0.921
Person 7	0.900	0.530	90.00	0.926
Person 8	0.950	0.302	95.00	0.981
Person 9	0.900	0.307	90.00	0.928
Person 10	0.958	0.301	95.83	0.981
Average	0.927	0.334	92.67	0.951

4.6 Conclusion

In this chapter, we discussed the different types of person authentication models. All the mentioned person authentication models have their strengths and shortcomings. Therefore, the EEG signal was proposed to overcome the shortcomings. The EEG signals are unique but highly uncertain, noisy, and difficult to analyze. VEPs can be found in the past literature and showed that the VEPs are suitable for person authentication modeling. Thus, feature extraction such as WPD, Hjorth parameter, coherence, cross-correlation, mutual information, and mean of amplitude are proven good to extract the relevant information or characteristics from the EEG signals. Different features provide different discriminative power for different subjects. On the other hand, feature selection also plays an important role in reducing the dimensionality of feature vectors. FRNN acts as classifier was implemented to measure the performance of uncertainty modeling in EEG signals analysis. The experimental results showed that FRNN is able to be used for person authentication modeling.

References

[1] S. Marcel and J. D. R. Millán, "Person Authentication using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation.," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 743–752, 2007.

[2] K. Fladby, "Brain Wave Based Authentication," Gjovik University College, 2008.

[3] A. H. Lashkari, S. Farmand, D. O. Bin Zakaria, and D. R. Saleh, "Shoulder Surfing Attack in Graphical Password Authentication," *Int. J. Comput. Sci. Inf. Secur.*, vol. 6, no. 2, pp. 145–154, 2009.

[4] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An Identity-Authentication System using Fingerprints," *Proc. IEEE*, vol. 85, no. 9, pp. 1365–1388, 1997.
[5] T. K. Neela and K. S. Kahlon, "A Framework for Authentication using Fingerprint and Electroencephalogram as Biometrics Modalities," *Int. J. Comput. Sci. Manag. Res.*, vol. 1, no. 1, pp. 39–43, 2012.
[6] M. Ekinci and M. Aykut, "Human Identification Using Gait," *2006 IEEE 14th Signal Process. Commun. Appl.*, vol. 14, no. 2, pp. 267–291, 2006.
[7] A. Zuquete, B. Quintela, and J. P. Silva Cunha, "Biometric Authentication using Brain Responses to Visual Stimuli," in International Conference on Bio-inspired Systems and Signal Processing, 2010, pp. 103–112.
[8] Y.-N. Shin, M. G. Chun, and W. Shin, "A Reproducible Performance Evaluation Method for Forged Fingerprint Detection Algorithm," in International Conference on Information Science and Applications (ICISA), 2010, pp. 1–8.
[9] V. Matyáš Jr and Z. Riha, "Biometric Authentication Systems," Czech Republic, 2000.
[10] A. Babich, "Biometric Authentication. Types of biometric identifiers," 2012.
[11] A. Bera, D. Bhattacharjee, and M. Nasipuri, "Hand Biometrics in Digital Forensics," in *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, 2014, pp. 145–163.
[12] J. Lehtonen, "EEG-based Brain Computer Interfaces," Department of Electrical and Communications Engineering, Helsinki University of Technology, Espoo, 2002.
[13] E. H. Chudler, "Functional Divisions of the Cerebral Cortex." [Online]. Available: https://faculty.washington.edu/chudler/functional.html. [Accessed: 02-Feb-2018].
[14] I. Svogor and T. Kisasondi, "Two Factor Authentication using EEG Augmented Passwords," in 34th International Conference on Information Technology Interfaces, 2012, pp. 373–378.
[15] H. Olesen, J. Klonovs, and C. K. Petersen, "Development of a Mobile EEG-Based Feature Extraction and Classification System for Biometric Authentication," Aalborg University: Copenhagen, 2012.
[16] M. Teplan, "Fundamentals of EEG Measurement," *Meas. Sci. Rev.*, vol. 2, no. 2, pp. 1–11, 2002.
[17] C. R. Hema, M. P. Paulraj, and H. Kaur, "Brain Signatures: A Modality for Biometric Authentication," in 2008 International Conference on Electronic Design, 2008, pp. 1–4.
[18] J.-F. Hu, "Multifeature Biometric System Based on EEG Signals," in Proceedings of the 2nd International Conference on Interaction Sciences Information Technology, Culture and Human - ICIS '09, 2009, pp. 1341–1345.
[19] M. J. M. Alexandra, P. Fonaryova Key, and G. O. Dove. "Linking Brainwaves to the Brain: An ERP Primer," *Dev. Neuropsychol.*, vol. 27, no. 2, pp. 183–215, 2005.
[20] R. B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles', "The Electroencephalogram as a Biometric," in Canadian Conference on Electrical and Computer Engineering 2001, 2001, vol. 2, pp. 1363–1366.

[21] J. Thorpe and P. C. Van Oorschot, "Pass-Thoughts: Authenticating With Our Minds," in Proceedings of the 2005 *W*orkshop on New *S*ecurity Paradigms, 2005, pp. 45–56.

[22] R. Palaniappan, "Two-Stage Biometric Authentication Method using Thought Activity Brainwaves," *Int. J. Neural Syst.*, vol. 18, no. 1, pp. 59–66, 2008.

[23] R. Palaniappan and K. V. R. Ravi, "A New Method to Identify Individuals Using Signals from the Brain," in International Conference Proceedings of the 2003 Joint Conference of the Fourth, 2003, pp. 1442–1445.

[24] R. Palaniappan and D. P. Mandic. "Biometrics from Brain Electrical Activity: A Machine Learning Approach," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 738–742, 2007.

[25] K. Malinka, "Usability of Visual Evoked Potentials as Behavioral Characteristics for Biometric Authentication," in 2009 *Fourth International Conference on Internet Monitoring and Protection*, 2009, pp. 84–89.

[26] J. G. Snodgrass and M. Vanderwart, "A Standardized Set of 260 Pictures: Norms for Name Agreement, Image Agreement, Familiarity, and Visual Complexity," *J. Exp. Psychol. Hum. Learn. Mem.*, vol. 6, no. 2, pp. 174–215, 1980.

[27] H. J. Lee, H. S. Kim, and K. S. Park, "A Study on the Reproducibility of Biometric Authentication Based on Electroencephalogram (EEG)," in *2013 6th International IEEE/EMBS Conference on Neural Engineering (NER)*, pp. 13–16, 2013.

[28] X. L. Zhang, H. Begleiter, B. Porjesz, W. Wang, and A. Litke, "Event Related Potentials during Object Recognition Tasks," *Brain Res. Bull.*, vol. 38, no. 6, pp. 531–538, 1995.

[29] "10/20 System Positioning Manual," Hong Kong, 2012. Trans Cranial Technologies Idt. Hong Kong. Manual.

[30] H. Jian-feng, "Biometric System Based on EEG Signals by Feature Combination," in International Conference on Measuring Technology and Mechatronics Automation, 2010, pp. 752–755.

[31] W. Ting, Y. Guo-zheng, Y. Bang-hua, and S. Hong, "EEG Feature Extraction Based on Wavelet Packet Decomposition for Brain Computer Interface," Measurement, vol. 41, no. 6, pp. 618–625, 2008.

[32] D. Y. Hu, W. Li, and X. Chen, "Feature Extraction of Motor Imagery EEG Signals Based on Wavelet Packet Decomposition," in The 2011 IEEE/ICME International Conference on Complex Medical Engineering, 2011, pp. 694–697.

[33] S.-H. Oh, Y.-R. Lee, and H.-N. Kim, "A Novel EEG Feature Extraction Method Using Hjorth Parameter," *Int. J. Electron. Electr. Eng.*, vol. 2, no. 2, pp. 106–110, 2014.

[34] T. Cecchin, R. Ranta, L. Koessler, O. Caspary, H. Vespignani, and L. Maillard, "Seizure Lateralization in Scalp EEG using Hjorth Parameters.," *Clin. Neurophysiol.*, vol. 121, no. 3, pp. 290–300, 2010.

[35] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive Biometric System Based on Electroencephalogram Analysis," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 1, pp. 1–8, 2008.

[36] S. H. Liew, Y. H. Choo, Y. F. Low, Z. I. Mohd Yusoh, T. B. Yap, and A. K. Muda, "Comparing Features Extraction Methods for Person Authentication using EEG Signals," in *Pattern Analysis, Intelligent Security and the Internet of Things*, 2014, pp. 196–205.
[37] K. M. Te Shun Chou, K. K. Yen, J. Luo, and N. Pissinou, "Correlation-Based Feature Selection for Intrusion Detection Design," in Military Communications Conference, 2007. MILCOM 2007. IEEE, 2007, pp. 1–7.
[38] X. Lu, X. Peng, P. Liu, Y. Deng, B. Feng, and B. Liao, "A Novel Feature Selection Method based on CFS in Cancer Recognition," in 2012 IEEE 6th International Conference on Systems Biology (ISB), 2012, pp. 226–231.
[39] S. H. Liew, Y. H. Choo, and Y. F. Low, "Fuzzy-Rough Nearest Neighbour Classifier for Person Authentication using EEG Signals," in Proceedings of 2013 International Conference on Fuzzy Theory and Its Application, 2013, pp. 316–321.
[40] R. Jensen and C. Cornelis, "Fuzzy-Rough Nearest Neighbour Classification and Prediction," *Theor. Comput. Sci.*, vol. 412, no. 42, pp. 5871–5884, 2011.

Index

EEG Signal Processing

Feature extraction, selection and classification methods

Electroencephalography (EEG) is an electrophysiological monitoring method used to record the brain activity in brain-computer interface (BCI) systems. It records the electrical activity of the brain, is typically non-invasive with electrodes placed along the scalp, requires relatively simple and inexpensive equipment, and is easier to use than other methods.

EEG-based BCI methods provide modest speed and accuracy which is why multichannel systems and proper signal processing methods are used for feature extraction, feature selection and feature classification to discriminate among several mental tasks. This edited book presents state of the art aspects of EEG signal processing methods, with an emphasis on advanced strategies, case studies, clinical practices and applications such as EEG for meditation, auditory selective attention, sleep apnoea; person authentication; handedness detection, Parkinson's disease, motor imagery, smart air travel support and brain signal classification.

About the Editor

Wai Yie Leong is a Professor at MAHSA University, Malaysia, where she specializes in biomedical signal and image processing, medical signal processing and telecommunications, smart control, and wireless sensor networks. She has been actively involved in Women In Technology and received the Smart-State-Smart-Women Award from the Queensland Government, Australia, in 2005. She is currently the Chairman of the Women Engineers Section, Malaysia (IEM-WE) and Chairman of Women Engineers – AFEO (WEAFEO). She has participated in National and International Wushu Tournaments winning more than 30 awards, including traditional Taichi, Taichi sobre, Taichi fan and Taichi sword.

IET Book Series on e-Health Technologies

Series Editor: Professor Joel P. C. Rodrigues, the National Institute of Telecommunications (Inatel), Brazil and Instituto de Telecomunicações, Portugal

Demographic shifts in populations trigger opportunities for innovations in e-Health, m-Health, precision and personalized medicine, robotics, sensing, the Internet of Things, cloud computing, Big Data, Software Defined Networks, and network function virtualization. The integration of these technologies is however associated with many technological, ethical, legal, and social issues. This new Book Series aims to disseminate recent advances in the e-Health Technology field to help improve healthcare and wellbeing.

ISBN 978-1-78561-370-8

9 781785 613708

Healthcare Technologies
Computing

The Institution of Engineering and Technology • www.theiet.org
978-1-78561-370-8