

*Brain Signal as a
New Biometric Authentication Method*

Fares Yousefi

*A thesis submitted in partial fulfilment of the requirements of
Liverpool John Moores University for the degree of
Doctor of Philosophy*

Feb 2022

Acknowledgment

Firstly, I would like to express my sincere gratitude to my supervisor Dr. Hoshang Kolivand for the continuous support of my PhD study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my PhD study.

Besides my advisor, I would like to thank the rest of my thesis committee: Dr. Wasiq Khan, Dr. Asma Patel, for their insightful comments and encouragement, but also for the hard questions which helped me to widen my research from various perspectives.

My sincere thanks also goes to the staff at Liverpool John Moores University within the Faculty of Engineering and Technology who helped me to prepare all the requirements for the project.

I would specifically like to thank and Dr. Atif Waraich within the School of Computer Science and Mathematics and Tricia Waterson in faculty research. Without their precious support it would not have been possible to conduct this research.

Last but not least, I would like to thank my family: my parents and to my brothers for supporting me throughout my education, this project, writing this thesis and my life in general.

Fares Yousefi

Abstract

Security authentication defines the process of verifying the identity of a person. For many years, authentication technology has played a crucial role in terms of data security. Existing typical biometric authentication technologies have some limitations. Progress in technology has produced several specific devices with ability to reproduce human biometrics that are currently used, mainly because they are mostly visible and touchable. Therefore, a new biometric method is required to overcome the limitations of current biometric authentication systems. Human brain signals are one of the biometric characteristics that has recently been utilised in diverse Brain-Computer Interface (BCI) applications. Brain-based authentication is achieving more popularity among researchers where research studies have reported considerable accuracy using different BCI methods for authentication purposes. However, there are some limitations in terms of usability, time efficiency, and most importantly the permanency of the method through time. The proposed research suggests two different brain-based authentication methods using picturing patterns and deep breathing patterns as brain states. This process starts with signal acquisition using the above-mentioned brain patterns as user strategies to capture the raw EEG data from the participants, followed by the pre-processing stage for data cleansing and standardisation. For noise removal, filtering techniques and the Independent Component Analysis (ICA) algorithm are utilised to make data ready for the feature extraction. Fast Fourier Transform (FFT), Power Spectrum Density (PSD), and Discrete Wavelet Transform (DWT) are used for the feature extraction from the time-frequency domain data representation. The extracted features are then forwarded to classification methods that include Linear Discriminant Analysis (LDA), Support Vector Machines (SVM), and Artificial Neural Network (ANN). The proposed picturing and deep breathing methods indicate 88% and 91% accuracy respectively when evaluated over pure unseen data. The results show that the picturing pattern method improves the security level according to invisibility and changeability of the brain-ID using images; and deep breathing patterns method improves the usability and permanency of the system because this pattern can be used anywhere and at any time.

Table of Contents

ACKNOWLEDGEMENT.....	II
ABSTRACT.....	III
TABLE OF CONTENTS.....	IV
LIST OF TABLES.....	VI
LIST OF FIGURES.....	VII
CHAPTER 1. INTRODUCTION.....	X
1.1 INTRODUCTION	1
1.2 PROBLEM BACKGROUND.....	3
1.3 PROBLEM STATEMENT	6
1.4 RESEARCH AIM.....	6
1.5 RESEARCH OBJECTIVES	6
1.6 JUSTIFICATION	7
1.7 REQUIREMENTS (FUNCTIONAL, NON-FUNCTIONAL)	8
1.8 RESEARCH CONTRIBUTION	8
1.9 RESEARCH SCOPE AND LIMITATIONS.....	9
1.10 THESIS ORGANISATION.....	9
CHAPTER 2. BACKGROUND/LITERATURE REVIEW.....	11
2.1 INTRODUCTION	12
2.2 BIOMETRICS.....	13
2.2.1 <i>Physiological and Behavioural Biometrics</i>	13
2.2.2 <i>Biometric Authentication and Identification</i>	14
2.2.3 <i>Biometric Authentication Types, Advantages and Disadvantages</i>	15
2.2.4 <i>Biometrics Test and Evaluation</i>	16
2.2.5 <i>Brainwaves as a new biometric authentication</i>	17
2.2.6 <i>Neural oscillations (Brainwaves)</i>	18
2.3 BRAIN-COMPUTER INTERFACE (BCI):	20
2.3.1 <i>BCI Types</i>	21
2.3.2 <i>BCI System process</i>	26
2.4 BRAIN-BASED BIOMETRIC AUTHENTICATION.....	29
2.4.1 <i>Brain-Based Authentication Methods</i>	30
2.4.2 <i>Signal acquisition protocols</i>	32
2.4.3 <i>Mental Visualization</i>	34
2.4.4 <i>Alpha brainwaves and deep breathing</i>	36
2.5 SUMMARY.....	37
CHAPTER 3. RESEARCH METHODOLOGY.....	39
3.1 INTRODUCTION	40
3.2 RESEARCH FRAMEWORK	41
3.3 PHASE 1: INVESTIGATION.....	44
3.3.1 <i>Security Authentication Methods</i>	44
3.3.2 <i>Brain-Based Biometric Authentication</i>	46
3.3.3 <i>Literature</i>	47
3.4 PHASE 2: SIGNAL ACQUISITION	47
3.4.1 <i>User Signal Strategy</i>	47
3.4.2 <i>Acquiring EEG From Participants</i>	48
3.4.3 <i>Recorded EEG Raw Signals</i>	50
3.5 PHASE 3: PRE-PROCESSING (ENHANCEMENT).....	50
3.5.1 <i>Visual Inspection</i>	51

3.5.2	<i>Removing Artifacts and Bad Channels</i>	51
3.5.3	<i>Signal Filtering</i>	52
3.5.4	<i>ICA Technique</i>	52
3.6	PHASE 4: FEATURE EXTRACTION	52
3.6.1	<i>Fast Fourier Transform (FFT)</i>	52
3.6.2	<i>Power Spectrum Density (PSD)</i>	53
3.6.3	<i>Log-Bandpower</i>	53
3.6.4	<i>Discrete Wavelet Transforms (DWT)</i>	53
3.6.5	<i>Extracted Features</i>	54
3.7	PHASE 5: CLASSIFICATION	54
3.7.1	<i>Linear Discriminant Analysis (LDA)</i>	55
3.7.2	<i>Support Vector Machine (SVM)</i>	55
3.7.3	<i>NN Classifier</i>	56
3.8	PHASE 6: RESULTS & EVALUATION	57
3.9	CONCLUSION	57
CHAPTER 4. METHODS		58
4.1	INTRODUCTION	59
4.2	SAS-BCI METHOD.....	59
4.2.1	<i>SaS-BCI Stages</i>	60
4.2.2	<i>Pre-Processing (Enhancement)</i>	64
4.2.3	<i>Feature extraction</i>	73
4.2.4	<i>Classification</i>	78
4.3	DEEP BREATHING (DB) METHOD	83
4.3.1	<i>DB Brain Pattern</i>	84
4.4	SUMMARY.....	88
CHAPTER 5. RESULTS AND EVALUATION		89
5.1	INTRODUCTION	90
5.2	SAS-BCI METHOD.....	90
5.3	DEEP BREATHING METHOD	96
5.4	SUMMARY.....	98
CHAPTER 6. CONCLUSION.....		99
6.1	OVERALL CONCLUSION	100
6.2	LIMITATIONS AND PROBLEMS	103
6.3	FUTURE WORKS	104
REFERENCES		106

List of Tables:

TABLE 2.1. BIOMETRIC METHODS ADVANTAGES AND DISADVANTAGES.....	15
TABLE 2.2. THE METHODOLOGY OF BRAIN IMAGING TECHNIQUES AND THE WAYS THAT THEY WORK.....	19
TABLE 2.3. TYPES OF BRAINWAVES AND THEIR FREQUENCY RATES AND MENTAL STATE SITUATION.	20
TABLE 2.4: TYPES OF SOME POPULAR NON-INVASIVE WIRELESS HEADSETS TO CAPTURE EEG DATA.	24
TABLE 2.5. COMPARISON OF SOME BIOMETRICS WITH BRAINWAVE BIOMETRICS.....	29
TABLE 5.1. IMAGE RECALL SUCCESS PERCENTAGE FOR BOTH 2D AND REAL OBJECT PICTURES	91
TABLE 5.2. THE RESULTS OF THE CLASSIFIERS FOR PICTURISING PATTERN.....	93
TABLE 5.3. THE AVERAGE RESULTS FOR THE PERFORMANCE SVM & LDA CLASSIFIERS.....	94
TABLE 5.4. COMPARISON OF THREE DIFFERENT EXPERIMENTS WITH DIFFERENT STRATEGIES AND CLASSIFIERS ...	95
TABLE 5.5. THE AVERAGE RESULTS OF BOTH SVM AND NN CLASSIFIERS FOR BREATH-HOLDING PATTERN	97
TABLE 5.6. THE AVERAGE PERFORMANCE OF THE CLASSIFIERS FOR <i>RECALLING</i> BREATH-HOLDING VS <i>NOT</i> <i>RECALLED</i>	97
TABLE 5.7. A COMPARISON BETWEEN THIS PAPER AND PREVIOUS WORKS	97

Table of Figures

FIGURE 2.1. PHYSIOLOGICAL & BEHAVIOURAL BIOMETRIC TYPES	14
FIGURE 2.2. BRAIN SIGNALS BESIDE THE MOST PRACTICAL BIOMETRIC AUTHENTICATION TECHNIQUES.	17
FIGURE 2.3. BCI TYPES TO CAPTURE THE ELECTRONIC SIGNALS	21
FIGURE 2.4. PHOTOS OF AN INVASIVE BCI IMPLANT ON HUMAN BRAIN	22
FIGURE 2.5. A PARTIALLY INVASIVE BCI ON HUMAN BRAIN	22
FIGURE 2.6. A TYPE OF NON-INVASIVE BCI DEVICE.	23
FIGURE 2.7. THE WAY THAT BCI CAPTURES THE SIGNALS FROM THE HUMAN BRAIN	23
FIGURE 2.8. EMOTIV EPOC + BCI HEADSET DEVICE	25
FIGURE 2.9. ILLUSTRATION OF LOCATION OF EMOTIV EPOC + ELECTRODES ON THE SCALP [66]	25
FIGURE 2.10. BRAIN-COMPUTER INTERFACE PROCESS	26
FIGURE 2.11. BRAIN SIGNAL ACQUISITION METHODS.	27
FIGURE 2.12. BCI APPLICATION FIELDS.....	28
FIGURE 2.13. POTENTIAL SYSTEM DEPLOYMENT FLOWCHART [14].....	31
FIGURE 3.1: THE SIX PHASES OF THE METHODOLOGY PROPOSED IN THIS PROJECT.....	43
FIGURE 3.2: EMOTIV EPOC + WITH ITS COMPONENTS THAT WAS USED FOR DATA ACQUISITION.....	49
FIGURE 3.3: EMOTIV PRO SOFTWARE INTERFACE FOR CONTACT QUALITY	49
FIGURE 3.4: EMOTIV PRO SOFTWARE INTERFACE.....	50
FIGURE 3.5: DIFFERENT TYPES OF ARTIFACTS THAT ARE VISIBLE IN EEG DATA [127]	51
FIGURE 3.6. EEG FEATURES BEFORE AND AFTER USING THE LDA CLASSIFIER	55
FIGURE 3.7. SVM CLASSIFICATION PROCESS VISUALISATION.....	55
FIGURE 4.1. NEW SIGNAL ACQUISITION STRATEGY USING BRAIN-COMPUTER INTERFACE.....	60
FIGURE 4.2. THE 20 DIFFERENT 2D AND 3D IMAGES THAT WAS USED IN THE EXPERIMENT	62
FIGURE 4.3. THE USER-STRATEGIES AND SIGNAL ACQUISITION FROM THE PARTICIPANTS IN TWO SESSIONS.....	63
FIGURE 4.4. A SCREENSHOT FROM THE EMOTIV SOFTWARE WHILE RECORDING THE DATA WITH 14 CHANNELS. 63	
FIGURE 4.5. EMOTIV EPOC CHANNEL LOCATION DETAILS.....	64
FIGURE 4.6. CHANNEL LOCATIONS ON THE SCALP BY NAME AND BY NUMBER	65
FIGURE 4.7. A VISUALISATION OF EACH CHANNELS INCLUDING THE SIGNALS THAT RECORDED BY THEM.....	65
FIGURE 4.8. PLOTTING CHANNEL POWER SPECTRAL DENSITY OF THE RECORDED EEG	66
FIGURE 4.9. CONTINUES DATA REJECTION BY EYES IN EEGLAB	67
FIGURE 4.10. AN EXAMPLE OF TWO BAD CHANNELS IN A PART OF THE RECORDED DATA	67
FIGURE 4.11: COMPARISON OF A BAD CHANNEL AND A GOOD CHANNEL	68
FIGURE 4.12: THE ORIGINAL POWER SPECTRUM IN FREQUENCY	69
FIGURE 4.13: THE FILTERED DATA WITH HIGH-PASS FILTER TECHNIQUE	69
FIGURE 4.14. ICA COMPONENT PLOTS FOR ALL 14 CHANNELS IN A DATASET.....	70
FIGURE 4.15. ICA COMPONENTS PROPERTIES PLOT FOR CHANNEL 3 OF A DATASET	70
FIGURE 4.16. SERIES OF COMPONENTS THAT DETECTED BY ICA ALGORITHM WHICH CAN BE REJECTED AFTER INVESTIGATION.....	71
FIGURE 4.17. APPLYING EEGDATA ON EEGLAB	72
FIGURE 4.18. THE RESPECTIVE MARKERS ON THE EEG DATA.....	73
FIGURE 4.19. A SCREENSHOT OF THE DARBELIAI TOOL ON EEGLAB IN MATLAB SOFTWARE TO DETERMINE THE BRAINWAVES IN TERMS OF THE FREQUENCY RATES.	74
FIGURE 4.20. POWER SPECTRUM IMAGE IN AN EEG DATASET.....	75
FIGURE 4.21. ABSOLUTE POWER IMAGE FROM AN EEG DATASET	75
FIGURE 4.22. RELATIVE POWER IMAGE FROM AN EEG DATASET	75
FIGURE 4.23. THE ILLUSTRATION OF THE CONCAVITY OF SPECTRAL DEFINITION	76
FIGURE 4.24. THE PROCESS OF THE CONVEXITY OF POWER SPECTRAL FOR FREQUENCIES AND POWER SPECTRAL VALUES.....	77
FIGURE 4.25. THE FUNDAMENTAL IDEA OF LINEAR SVM CHARACTERIZED BY THE OPTIMAL HYPERPLANE	79
FIGURE 4.26. A SCREENSHOT OF THE CLASSIFICATION LEARNER APPLICATION IN MATLAB SOFTWARE	80
FIGURE 4.27. CONFUSION MATRIX RESULT OF THE EEG DATASET AFTER TRAINING THE MODEL	81
FIGURE 4.28. UPLOADING THE DATA ON BCILAB	81
FIGURE 4.29. APPLYING THE LOG-BANDPOWER PARADIGM AND CREATING MODEL ON BCILAB	82
FIGURE 4.30. THE PARADIGM CLASSIFIER RESULTS FROM BCILAB	83

FIGURE 4.31. THE METHODOLOGY OF THE DB EXPERIMENT	84
FIGURE 4.32. AN EXAMPLE OF A CLEANED DATA AFTER FILTERING	85
FIGURE 4.33. DECOMPOSITION OF EEG DATA IN FOUR LEVELS	86
FIGURE 4.34. THE ANN DIAGRAM FOR EEG BRAINWAVE SEGMENTS	87
FIGURE 5.1. A COMPARISON BETWEEN THE REAL OBJECT PICTURES IN TERMS OF DIFFICULTY TO REMEMBER THE DETAILS	92

Table of Abbreviations

ANN : Artificial Neural Networks	56
BCI : Brain-Computer Interface	2
BP : Backpropagation.....	5
BSS : Blind Source Separation	27
CAR : Common Average Referencing.....	27
CAS: Common Access Card	1
CL : Classification Learner.....	80
CNN : Convolution Neural Networks	56
CSP : Common Spatial Patterns	27
CSSD : Common Spatial Subspace Decomposition	27
CSSP : Common Spatio-Spatial Patterns.....	27
CSV : Comma-Separated Values.....	63
DWT : Discrete Wavelet Transform.....	28
ECoG : Electrocorticography	22
EDF : European Data Format	63
EEG : Electroencephalogram	3
EER : Equal Error Rate	16
EMG : Electromyography.....	23
ERP : Event Related Potentials.....	5
FAR : False Acceptance Rate	16
FFT : Fast Fourier Transform	41
FIR : Finite Impulse Response	68
fMRI : Functional Magnetic Resonance Imaging.....	35
FNR : False Negative Rates.....	81
FRR : False Rejection Rate.....	16
HP : High Power.....	85
ICA : Independent Component Analysis	7
k-NN : k-Nearest Neighbour	4
LAT : Local Averaging Technique.....	27
LDA: Linear Discriminant Analysis.....	3
LJMU : Liverpool John Moores University.....	6
LP : Low Power	85
MEG : Magnetoencephalography	35
NIRS : Near-Infrared Spectroscopy.....	35
PCA : Principal Component Analysis	27
PET : Positron Emission Tomography	35
PIV : Personal Identity Verification	1
PSD : Power Spectral Density	4
RKF : Robust Kalman Filtering.....	27
RNN : Recurrent Neural Networks.....	56
RSVP : Rapid Serial Visual Presentation	3
SaS : Signal acquisition Strategy	60
SCOH : Spectral Coherence	4
SL : Surface Laplacian	27
SNR : Signal-to-Noise Ratio	33
SOM : Self Organizing Maps	27
SVD : Single Value Decomposition	27
SVM : Support Vector Machine	53
TPR : True Positive Rates.....	81
WT : Wavelet Transform.....	52

Chapter 1

Introduction

1.1 Introduction

In the past, when computer technology had not been invented and there were no personal computers, smart mobile technologies, and especially the internet, the word “security” meant the preservation of personal property, personal safety and occupational safety, and many related issues. Nowadays, with the advancement of technology, especially the internet and the presence of advanced computers and gadgets that record data and save them, information security is one of the most important security concerns, which in many cases encompasses all the security implications [1].

In our computerized world, technological terms are changing on a daily basis with a variety of technologies being introduced to make human life easier and safer. However, most of the time, such technology deals with data (and information) requiring high security. Information security in many sectors of the population including the general public, companies, organizations, and governments, plays a vital role. The stakeholders have been demanding more appropriate, reliable, secure, and practical ways to keep their information safe.

Authentication is the method of allowing individuals access to an application or system based on their identity [2]. Today, with more users engaging technology in their everyday lives particularly smartphone/mobile devices where a lot of sensitive information is stored and used, security and accurate authentication methods have become a top priority within information security [3]. In the past, individuals used to have a briefcase to keep their keys, money and important documents like bank account booklets, letters, photos, etc. which could be locked to keep them secure. But today, individuals can keep all of that information on their personal computers, mobile devices, social networks, and cloud storage. In this case, security and data protection plays a crucial role. Authentication is necessary as it allows companies and users to keep their systems and devices protected by authorizing only authenticated users to use important resources [4].

There are multiple techniques in authentication [5] such as *Something you know* (password or PIN) *Something you have* (such as a smart card, Common Access Card (CAC) [6], Personal Identity Verification (PIV) [7], or RSA token [8]), and recently *Something you are* (e.g., using biometrics).

Password or PIN authentication and different kinds of smart cards and tokens are easy to implement, and the risk of them getting lost or being stolen is high in both of them. In contrast, biometrics is a new technological alternative to solve this problem [9] that uses the unique biological or behavioural characteristics of a person.

Biometric authentication has multiple advantages that can deliver highly accurate and secured access to resources. This can be accomplished very quickly and consistently, with a minimum training and the person's identity can be proven without access to the information that may be stolen, lost or changed [10].

There exist several biometrics technologies such as fingerprints, face detection, voice recognition, Iris, etc. which have been used for personal identification [11]. Each one of the different biometric identification methods has their own strengths and particular uses. Some methods require less invasive techniques while others can be accomplished without the familiarity of the topic and some are very difficult to replicate. Two major properties within biometrics that are useful for authentication purposes include: a) Physical biometrics comprising fingerprints, retina scans, DNA, facial recognition, hand geometry biometrics, and iris scan; b) Behavioural biometrics, which contains speech recognition and handwritten signatures [12].

These typical biometric authentication technologies have some advantages such as stronger security, improved quality of experience, reliability. However, there are several drawbacks associated such as environment and usage can affect measurements (e.g., the condition of your fingerprint at the time of scanning such as wet, oily or dirty hands which may produce unclear patterns). Considering such problems, these systems are not very reliable [13].

The current biometric methods are suffering from some three main disadvantages; firstly, they are visible and can be recorded and replicated by some specific software and technologies, secondly, they are not replaceable which it means the features cannot be changed if it were ever compromised and finally, they are not usable for some disabled individuals who are not able to use their hands or move their bodies. Therefore, a new biometric method needs to be produced to reduce the number of disadvantages that are within current systems.

Brain signal on the other hand, is an invisible human characteristic which is replaceable (e.g., allows us to change the pattern), and might be most appropriate for disabled individuals (e.g., users with physical disabilities). Brainwave is one of the characteristics that currently has been receiving much attention from researchers working on Brain-Computer Interface (BCI) within diverse application domains.

In the past, individuals always desired to understand the non-verbal behaviours (including brain/mind), or to control their environments or replace objects with their brainpower [14]. The technological revolution has made this practical such as visualised transferring signals straight to someone else's brain allowing them to experience new sensory inputs like sight, hearing or feeling

[15]. One of the potential outcomes of the future brain related technologies could be the manipulation of computers and associated devices with the simple transferring of a thought. Considering this potential, BCI will be a significant breakthrough within technology. BCIs are becoming increasingly popular in medical and non-medical areas as a way for communication to be conducted between humans and machines. “A major goal of BCI is to decode intent from the brain activity of an individual, and signals representing the decoded intent are then used in various ways to communicate with an external device” [16]. BCI is the interaction between humans and computers, and it is the most recent development and research area of Human-Computer Interface (HCI) [17]. It can lead to many applications for gamers, social interactions, capture feelings and emotions, disabled individuals in different ways, and understand brain activities and human/animal neural activities [18].

To sum up, the significant factors in any biometric authentication method are Privacy and Security, Universality, Uniqueness, Permanency and Collectability. Privacy and permanency are big challenges in any brain-based authentication technique. Thus, they require more improvements in the case of the stability of the brain pattern and the security level of the method. In this research, two different strategies are proposed using the picturising method to improve the security level and the deep breathing method to improve the stability of any brain state over time, which could help to use brain signal as a new biometric authentication method.

1.2 Problem background

Recent biometric user authentication techniques have some problems and limitations. To cover the recent biometric limitations, we need a new biometric Brainwave based authentication, which is another technique to the extensive range of authentication systems. Electroencephalogram (EEG) signals are the most popular method to investigate brain signals in this process. A couple of different approaches were presented in different studies to capture EEG signals and classify them with different BCI methods to find the unique signals and use them as an authentication method with a high accuracy rate.

Chen et al.[19], proposed a system within authentication, which is centred on Rapid Serial Visual Presentation (RSVP) stimulus. A brain amplifier was used to obtain EEG signals and Linear Discriminant Analysis (LDA) to classify them. A specific association constant calculated the important features. According to the author’s notation, a password can be hidden effectively in certain compulsive situations.

Chuang et al.[20], presented a new approach which used the MindWave to obtain data. Seven tasks were executed, including sports activity, breathing, audio listing, simulation of finger

movement, colour, reciting and identifying music with singing, and pass-thoughts. The classification process is done with the k-Nearest Neighbour (k-NN) algorithm. The most accurate strategies were for colour, audio, and sport. The most difficult one was for the pass-thought task according to the results of the questionnaire that determined for user-friendliness with different tasks. Breathing, audio, and colour were the straightforward tasks.

La Rocca et al.[21], presented an approach centered on connectivity within EEG spectral coherence. In this method, data samples were gathered from 108 participants during open resting and closed-eyes positions. EEG data was captured using a system consisting of 64 different channels with a rate of 160 Hz. Data was filtered to 50 Hz via a low-pass anti-aliasing filter. Spectral Coherence (SCOH) and Power Spectral Density (PSD) analysis techniques were used to extract mental features. To calculate uniqueness, two different algorithms were used separately in this process which were Mahalanobis classifiers that were based on distance and match-score fusion system. This technique is strong and very accurate for user identification. The performance of classification has the possibility of not functioning properly if this classification was used for a larger group of users on traditional hardware and it is less reliable.

Ruiz-Blondet et.al.[22], presented a protocol known as CEREBRE with a band-pass filtering between 1 and 55 Hz and based on normalized cross-correlation, a simple discriminant function was used for classification. The nominal (4 categories, 3 channels) classifier showed the highest accuracy when all the patterns were used but both maximum and minimum classifiers showed 100% accuracy. The results presented that the most accuracy was for the oddball (a stimulus that occurs infrequently relative to all other stimuli, and has distinct characteristics) and food. The resting pattern had reduced performance in terms of classification. Authentication centered on a memory-evoking task (also known as “pass-thoughts” in other studies) [23] also indicated unreliable outcomes mainly because of inconstant time that was consumed to allow thinking.

In general, the EEG-based authentication process has four main steps that include: signal acquisition, pre-processing (data cleansing and standardisation), feature extraction, and classification. Acquiring the brain signals and EEG data appropriately, is the crucial step which can influence the outcomes directly. There are three main protocols for EEG data recording: tasks with an external stimulus, mental tasks, and resting states. It is important to select an appropriate protocol for authentication purposes as it has significant impact on the accuracy of the results.

Resting state protocols are very popular in EEG signal recording especially for authentication purposes [24]. In this protocol, the individuals should sit in as quiet or less noisy area as possible

for recording the EEG data. Resting states make the alpha band the dominant brainwave among others [25]. The simplicity of this protocol makes it more useful because it can be done without using any extra equipment other than a brain device in comparison to other protocols; however, it should be done in a quiet environment.

Tasks with external stimuli cover a wide range, for example, reading different types of texts [26], recognizing different types of images [27], recognizing different geometric figures [28], moving and static substances [29]. Tasks with external stimuli have the advantage of permanency condition over time but their disadvantage is their need for external equipment. Another EEG recording protocol is mental tasks, which includes imagining body movements, mental activities. For example, images of moving hands, head, or feet and sometimes doing both movements and imagining the movements [30]. According to different studies, imaginary tasks have achieved better results in comparison to physical activities. There are other experiments such as counting in mind [31], picturing patterns by imagining 2D and 3D images [32].

Some studies achieved high accuracy results using multiple EEG recording protocols and tasks for authentication purposes. Armstrong et al. [33] used a text reading task while Event Related Potentials (ERP) were collected from participants and applying SVM and non-SVM classifiers which achieved 89% accuracy as results. Patel et al. [34] used self-photo and non-self-photo as visual stimulation. They used a Backpropagation (BP) neural network classifier on the extracted features based on fuzzy entropy and achieved an average success rate of 92%. Zhendong et al. [35] used visual/audio stimuli for their experiment to recall some specific subjects including water bottle, handle, screwdriver, which achieved 87.3% accuracy as the result of their work. Abo-Zahhad et al. [36] proposed a multi-level EEG system using eye blinking, which by applying the data on an LDA classifier from the band power spectral features achieved a high accuracy rate of 98.56% for their experiment. The main problem in most studies in this area is the stability of the method through time that is important to cover the permanency set for any authentication process. Human brain signals can change over time by experiencing different events in life. The brain cannot function properly in some specific moments to create a stable pattern for a task. It could be for some reason like being sick, anxious, drunk, stressed, etc. [37].

Considering the aforementioned factors, there are several limitations in existing research studies mainly related to usability, time efficiency, and most importantly the permanency of the method through time. We need a better approach to acquire and utilise brain signals as a new biometric authentication method which is more reliable, usable for different aspects of technology, and permanent in time.

1.3 Problem statement

Brain-based authentication techniques have some limitations, and they suffer from some critical downsides, such as:

- *Brain Situation:* Brain signal is different to other types of biometrics, which use only one simple pattern. Brainwaves can be very difficult to classify in different situations, for example, the brain signal power is in a low frequency rate in sleeping time or could be in a high frequency rate in stressing times, which makes it harder to find a stable pattern through time [38] [39].
- *Weakness of the signals:* Brainwaves are very low frequency rate electromagnetic waves. The human scalp is a strong shield for the brain, which makes the created waves even weaker to be acquired and recorded by non-invasive devices [40] [41].
- *BCI Authentication methods:* Regarding complexity and the weakness of the brainwaves, the current BCI methods are not reliable. Their used strategies to acquire brain signals are very time consuming and complex, the brain-IDs are not stable through time and have lower level of security [42] [43].

Human brain signal is altering every day according to different events that happen in life which, can change the stability of the brainwaves through time. On the other hand, brainwave is a type of electromagnetic wave that is very weak while producing and it is hard to capture which, might create noisy data full of artifacts. Recent BCI authentication methods struggle with these problems and do not have reliable results that could make the system more practical to cover the current issues.

1.4 Research Aim

The ultimate goal of this study is to propose a new framework to process the EEG signal for the identification of unique patterns to be used as a reliable biometric authentication signature.

1.5 Research Objectives

To achieve the aim the following objectives need to be addressed

- To investigate different biometric authentications, brain-computer interfaces and brain-based authentication techniques in previous studies.
- To propose new strategies to acquire and record the EEG signals from participants using BCI devices.
- To capture a primary dataset following the appropriate ethical procedures from the Liverpool John Moores University (LJMU).

- To apply filtering techniques and Independent Component Analysis (ICA) algorithm for noise removal.
- To extract the features needed according to proposed strategies, which can be used as the authentication signature.
- To utilise multiple classification algorithms using extracted features to validate the proposed biometric authentication technique
- To evaluate the results for the permanency of the brain pattern, usability and security level of the method

1.6 Justification

This research has proposed two BCI approaches with newly introduced methodologies to use brain signal as an authentication technique. These methods address multiple problems such as security, usability and stability facing any brain-based authentication. Researchers can use proposed strategies and methods to build a secure and permanent authentication technique using brain signal. The first strategy using the picturing pattern can be used for any type of authentication process that needs a higher level of security. In this method, the user can use a specific image in the mind as a security ID. It does not need any body movements or extra equipment and most importantly, it is not visible. The results obtained from this research (and this method) are poised to become a basis for the much-needed industrial standard in computer and any mobile and smart gadget security. Furthermore, it might be useful for vulnerable users who can utilize the proposed method as reliable brain-based authentication for smart devices. It is also believed to have an advantage from the usability perspective producing ease of use on the authentication process.

In the case of stability and permanency of any brain pattern for authentication purposes, the second method using the deep breathing strategy would revolutionize the whole process of authentication using brain signals. Deep breathing can stabilize the brain state in any brain situation. In this method the user takes deep breaths in three parts of inhale, breath-holding and exhale. The breath-holding part itself is a brain-ID that can be used for a stable authentication pattern. Researchers can integrate this strategy to their method and make it stable through time. The human brain can be distracted and be out of its normal state according to the way of living. Stress, anxiety, sadness, excitement, sickness, drunkenness and many other things can affect the brain to not produce the necessary frequency rate signals to create a pattern.

The proposed method and dataset would be of enormous help mainly to researchers, academics (e.g., tutors, students), software developers using biometric methods, and industry related to security tech creators including computers, mobile phones, smart home devices, technologies for disabled individuals, etc.

1.7 Requirements (Functional, Non-functional)

There are some requirements and resources for this project as follows:

- *Related works and research papers:* To start the project we need to gather enough information about the subject from other research papers and related works. For this matter, some books in Liverpool John Moores University's library and online resources websites like IEEE Xplore Digital Library, Scopus, Web of Science, Google Scholar, and some other reliable websites are used. (functional)
- *A high-performance computer device (PC-Laptop):* To do the investigation and searching, data processing and machine learning, and writing up. A high-performance computer system is needed for which the university computer systems and a personal laptop (Apple MacBook Pro) will be used. (functional)
- *Internet connection:* The university high-speed internet connection is used. (functional)
- *A BCI device to capture the signals:* To investigate brain signals an Emotiv EPOC+ device is needed which the university prepared and provided for this project. (functional)
- *An Emotiv SDK software:* To transfer the captured brain signals via Emotiv device to the computer and record the signal data, special software was needed which the university prepared and provided a licence to use it for the period of the project experiments and tests. (functional)
- *Research ethical approval:* To demonstrate that we adhere to the accepted ethical standards of a genuine research study and to protect participants.
- *Programming platforms and software:* To process the recorded signals, apply the proposed method and use the classification algorithms to acquire the results (non-functional)
- *High speed internet connection:* To use online platforms and live tests on the data and research different experiments. (non-functional)

1.8 Research Contribution

- The first and main contribution is systematic collection of primary data set, investigation, and listing of the strengths and shortcomings of the existing techniques and strategies in biometric authentication methods specifically the BCI authentication process that could help use brain signal as a new biometric technique and cover the disadvantages of the recent biometric methods.
- The two methods proposed in this research are the contributions to improving the security level of any brain-based authentication method and its stability over time. The first method is based on a picturising pattern that heightens the security level, and the second method is based on a deep breathing strategy that improves the permanency of the brain pattern during the authentication process.

- We introduced SaS-BCI algorithm to improve the security level of the brain-based authentication process by using a specific picture as a security pattern when imagined in mind. This method does not need any external stimuli or any body movement, which makes the technique more secure because it will not be visible. On the other hand, another picture as a security pattern can replace the previous pattern if needed.
- The deep breathing pattern was introduced to improve the stability of any brain pattern that could be used for authentication purposes. This method, regardless of any situations of human life that can change the brain functionality, could bring back the brain to its normal state, which can produce the brainwaves in the frequency rate needed to create a specific pattern.

1.9 Research Scope and Limitations

Decide how we can acquire brain signal that can improve the level of security, permanency of the pattern through time and usability for authentication processes to see if we can gain better results to use brainwave as a biometric authentication method.

Any BCI-based experiment needs a brain device to record the brain data and analyse it. At the time this research is done, there is still a big lack of stronger brain devices that can acquire the data from the brain. Brain signals are very weak and hard to capture without noises which makes the experiment harder to achieve the appropriate results. In this research an EEG-based EMOTIV Epoc + BCI device were used to do the experiments. It took a lot of time and effort to clean the data from the noises made by the device and in some cases some of the electrodes weren't recording the data properly which forced us to redo the experiment and spend more time on it. The number of participants were another limitation in this research especially in the COVID-19 situation. In this kind of experiment the more participants involved the more accurate the result will be.

1.10 Thesis Organisation

Chapter 1 includes the statement of the thesis. It starts with the introduction and following that the problem background, problem statement, aim, objectives, requirements, contribution, scope and limitations. The structure of thesis is outlined at the end of the chapter.

Chapter 2 provides an in-depth literature review of all the three major areas: biometric authentication methods, brain-computer interface, and brain-based authentication methods. Emphasis is laid on the various contributions and limitations of the proposed algorithms and techniques in all three relevant areas.

Chapter 3 presents the research methodology in six phases. Phase 1 investigates different types of authentication methods, biometric authentication techniques, brain-computer interfaces their process steps, brain-based or EEG authentication methods in different research and their strengths and weaknesses. All of these investigations together complete the literature of the project. Phase 2 is the first step of the presented methods, which is the brain signal acquisition. In this phase, two signal-acquiring user strategies are presented; the first one is SaS-BCI using the picturing pattern and the second one is the deep breathing technique. It explains the way a user's brain signal is acquired by a brain device named Emotiv EPOC+ and its software to record the raw EEG data and store them in the computer system. The signal pre-processing and enhancement of the raw EEG data is done in Phase 3. This phase explains the techniques were used for noise, artifact and bad channel removal by different techniques and algorithms. Phase 4 shows different methods and algorithms used for the feature extraction step of the main method. The extracted features will be selected and classified using different classifiers in Phase 5. Finally Phase 6 presents the results, evaluation and conclusion.

Chapter 4 discusses the realization of the second to fifth objectives of this research by presenting two new methods. It starts with the SaS-BCI method using the picturing pattern to improve security and usability of the brain-based authentication process. It has three main steps of signal acquisition, feature extraction and classification using different strategies and techniques of the BCI system. It is followed by the second method using the deep breathing pattern to improve the stability and permanency of a brain-based authentication process. This method also includes three main steps of a BCI system like the previous method using different strategies and techniques.

Chapter 5 presents results emanating from the two presented methods. Testing, evaluation and validation of all contributions are employed in this chapter. The results achieved by different classifiers in each method are presented separately. It starts with the result and evaluation of the first method and follows with that of the second method. The last part of this chapter is a comparison of each presented method's result with some other high-level experiments done by other researchers previously, which compares the security level, usability, stability and permanency of the presented methods in this research with others.

Chapter 6, the thesis ends with a conclusion and suggestions for further research which may provide directions in which future researchers of brain-based authentication methods may proceed.

Chapter 2

Background/Literature Review

2.1 Introduction

There is a growing demand for different types of user authentication technologies for both online and physical systems. The motivation to authenticate users ranges from access control reasons to business development purposes like adding e-commerce elements. Organizations need to understand that passwords are not the only way to authenticate users. There is a wide variety of authentication technologies and an even greater range of activities that require authentication methods.

Authentication is the process of identifying users that request access to a system, network, or device. Access control often determines user identity according to credentials like username and password. Other authentication technologies like biometrics and authentication apps are also used to authenticate user identity.

User authentication is a method that keeps unauthorized users from accessing sensitive information. For example, User (A) only has access to relevant information and cannot see the sensitive information of User (B). Cybercriminals can gain access to a system and steal information when user authentication is not secure. The data breaches companies like Adobe, Equifax, and Yahoo faced are examples of what happens when organizations fail to secure their user authentication. Hackers gained access to Yahoo user accounts to steal contacts, calendars and private emails between 2012 and 2016. The Equifax data breach in 2017 exposed credit card data of more than 147 million consumers. Without a secure authentication process, any organization could be at risk.

Cybercriminals always improve their attacks. As a result, security teams are facing plenty of authentication-related challenges. Therefore, companies are starting to implement more sophisticated incident response strategies, including authentication as part of the process. Some common authentication methods used to secure modern systems are 1. Password-based authentication which is the most common method of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. 2. Multi-factor authentication which is an authentication method that requires two or more independent ways to identify a user. 3. Certificate-based authentication technologies which identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's licence or a passport. 4. Biometric authentication which is a security process that relies on the unique biological characteristics of an

individual. This type of authentication is one of the most secure methods in comparison to others which are always improving and changing depending of the human biological and physiological characteristics. In this case, human brain signal is one of the human biometrics that has attracted researchers and scientists to use for authentication proposes.

Authentication technology is always changing. Businesses have to move beyond passwords and think of authentication as a means of enhancing user experience. Authentication methods like biometrics eliminate the need to remember long and complex passwords. As a result of enhanced authentication methods and technologies, attackers will not be able to exploit passwords, and a data breach will be prevented.

Overall, this chapter provides an overview of popular and well-known authentication methods, biometric methods comparisons, Brain-Computer interface (BCI), brain-based authentication techniques and investigates previous works and experiments of other researchers in this area, which covers the first objective of this project.

2.2 Biometrics

The word Biometrics is a combination of two Greek words. “bios” (life) and “metrikos” (measure). It is the arithmetical analysis of humans’ unique behavioral and physical characteristics. Thus, biometric recognition of individuals is for identity verification or identification. This technology is mostly used for access control and identification, or for identifying users who are under investigation [44]. Biometrics is a technique to verify a person using his/her behavioural or physiological characteristics [45]. A good definition of biometric technologies is “automated methods of verifying or recognizing the identity of a living person based on physiological characteristics or behavioural characteristics” [46].

There are two different concepts in biometrics that we should concentrate on, which are behavioural/ Physical Biometrics and Authentication/Identification.

2.2.1 Physiological and Behavioural Biometrics

Any human physiological or behavioral characteristic, which is quantifiable, and can be found in everybody (Fig 2.1). These characteristics have unique specific differences that will not change over time [47].

Behavioural Biometrics concentrates on analysing the non-physiological or non-biological structures of any human. It studies the unique psychological characteristics of humans like

signature, voice, gait, keystrokes. Physical Biometrics is doing the opposite, which is focusing on analyzing the physiological and biological structures of the human. These unique characteristics include fingerprints, the shape of the hand, face, and the construction of the eye (iris/retina) [48].

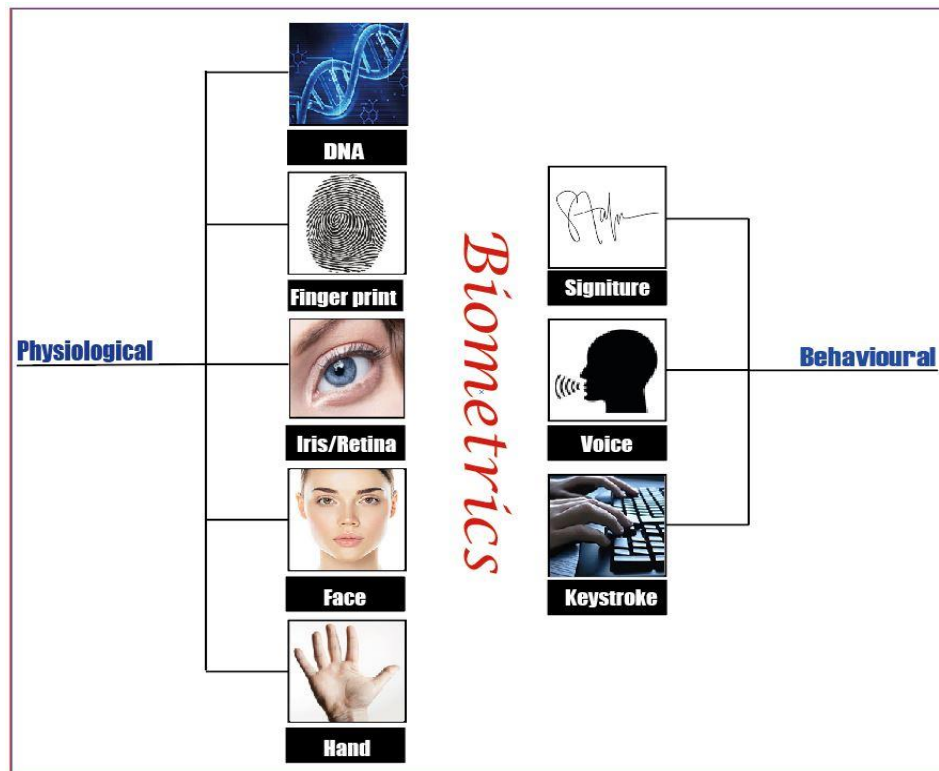


Figure 2.1. Physiological & Behavioural Biometric types

2.2.2 Biometric Authentication and Identification

A biometric technique can work in two modes: authentication or identification [49]. These two concepts are at the heart of the biometric science.

The Biometric system's authentication is trying to determine the real person who is trying to authorise him/herself. For instance, when individuals are trying to access their own computer, smartphone or network using fingerprint or retina scan, they are demanding to be somebody and the question "Am I really whom I claim to be?" is trying to be answered. The Biometric system's identification is trying to determine the person who wants to access. Therefore, if individuals are trying to log into their computer, network or smartphone another time, and they do not claim to be anybody, the biometric technology is trying to check and find out who really that person is and the question "Who am I?" is trying to be answered [50].

2.2.3 Biometric Authentication Types, Advantages and Disadvantages

As mentioned before, there are two different concepts in biometrics that we should concentrate on, which are Behavioural/Physical Biometrics and Authentication/Identification. Behavioural Biometrics concentrates on analysing the non-physiological or non-biological structures of any human. It studies the unique psychological characteristics of humans like signature, voice, gait, keystrokes. Physical Biometrics is doing the opposite, which is focusing on analysing the physiological and biological structures of the human [9].

Biometric authentication is one of the most popular ways to provide personal identification because these characteristics of a human are specific and unique. Most of these specific features are so hard to duplicate and accurately produce. In terms of information security, physiological biometric traits appear more practical. The most popular physiological biometric techniques are Face detection, Fingerprint identification and Iris/Retina scan. The current biometric techniques have some advantages and disadvantages. Table 2-1 shows advantages and disadvantages of recent biometric methods [10].

Table 2.1. Biometric methods advantages and disadvantages.

<i>Biometric Advantages and Disadvantages</i>	
<i>Advantages</i>	<i>Disadvantages</i>
<p>Security: Biometric technology brings different types of solutions, which are nearly impossible to hack unlike passwords.</p> <p>Accuracy: Biometric works with individual's physical traits such as fingerprints, face, retina amongst others that will always serve you accurately anywhere, anytime.</p> <p>Convenient: Your credentials are with you forever, so it does not require you to memorize or note down anything.</p> <p>Flexibility: You have your own security credentials with you so you do not need to bother memorizing awkward alphabets, numbers and symbols required for creating a complex password.</p> <p>Trustable: Reports claim that the young generations trust biometric solutions more than other solutions.</p> <p>Scalability: Unlike other solutions, biometrics are highly scalable solutions for all types of projects. It is possible for any kinds of projects because of the scalability of its solutions.</p> <p>Save Time: Biometric solutions are highly time conserving.</p> <p>Save Money: With a little money, any company can track their employees and reduce the extra costs they are paying for years.</p>	<p>Physical Traits Are Not Changeable: We can reset a password, but we never can change our fingerprints or retina, these are fixed.</p> <p>Error Rate: Usually, biometric devices make two types of errors, False Acceptance Rate (FAR) and False Rejection Rate (FRR). When the device accepts an unauthorized person, it is known as FAR and when it rejects an authorized person, it is known as FRR.</p> <p>Delay: Some biometric devices take more than the accepted time and a long queue of workers form waiting to be enrolled in large companies.</p> <p>Unhygienic: In contact-based biometric techniques, a biometric device is used many times by an enormous number of people. Everyone is actually sharing his or her germs with each other via the device.</p> <p>Physical Disability: Some individuals are not fortunate enough to be able to participate in the enrolment process. They might have lost or damaged body parts such as fingers or eyes.</p> <p>Environment And Usage Matters: Environment and usage can affect the overall measurements taken.</p>

2.2.4 Biometrics Test and Evaluation

There are two fundamental aspects that must be tested in biometric systems: system effectiveness and user acceptance. Jorgensen and Yu [51] suggested that biometric systems should measure FAR, FRR, and EER as key effectiveness metrics. The first two establish whether the system accurately identifies the user while the last specifies the error rate where FAR and FRR are equal. These values are determined as follows:

$$FRR = \frac{\text{False Rejections}}{\text{Unauthorized Attempts}} \times 100\% \quad (2.1)$$

$$FAR = \frac{\text{False Acceptances}}{\text{Unauthorized Attempts}} \times 100\% \quad (2.2)$$

EER is defined as the point where FAR equals FRR. A lower EER indicates a more accurate system. The evaluation of the user acceptance aspect involves a set of factors. They include operational, technical, manufacturing, and financial possibilities. El-Abed et al. [52] recommended a thorough evaluation of the individual's entire interaction with the system. This evaluation includes any thoughts, feelings, and outcomes of the individual experiences. The overall effectiveness of the approach can be calculated by leveraging a number of metrics, including FAR, FRR, and EER. The evaluation of these values combined with the amount of data required will determine the effectiveness of the solution [53] [54]. A lower EER (i.e., FAR=FRR) indicates a more accurate system. Additionally, Revett et al. [55] described how the current state of EEG-based authentication can reach classification accuracy between 80% and 100% with an EER of just 5.5%, and a true acceptance rate (TAR) of 95+%. These values, as expected with physiological characteristics-based biometrics, are superior to behavioural based biometrics [54]. Based on these values, an acceptable level of effectiveness for this work can be defined by an EER equal to or smaller than 5.5%, an accuracy of at least 80%, and a TAR of 95+%. Although the values above are accepted for defining a reliable biometrics system, it is important to note that a biometric technique's performance depends on the features it is based on (i.e., genotypic or phenotypic). Matyas et al. [56] discussed how genotypic features do not change over time, allowing FRR to remain low. However, in the case of monozygotic twins, such a system will not be able to distinguish them.

When systems rely on phenotypic variation, a lower limit on the FRR may be required. A key aspect of any research is the confidence interval, which is determined by the confidence level, the variability of the sample, and the sample size [57]. The confidence level is typically set at 95% while the variability is estimated using the standard deviation from the sample. As discussed by Sauro and Lewis, the sample size is the key factor a researcher can control in affecting the width of a confidence interval. Since this interval and the sample size have an inverse square root relationship, the sample size has to be quadrupled in size to reduce the margin error by 50%.

2.2.5 *Brainwaves as a new biometric authentication*

The potential for using brain waves as human biometric identification has risen to the surface once again. The password is not secure enough to stay at the universal standard forever. There are different types of biometric techniques (Fig 2.2) that have some limitations and disadvantages. An idea presented as a way to distinguish humans from thoughts, before becoming a method of security, could be the measuring standard for biometric identification in the near future, but it needs more time and work on it. It is an uncommon form of identification, but such imperceptible biometric methods are being discovered progressively. Brainwave authentication might sound like the stuff of science fiction right now, but it is obviously a possible technique of identification and in terms of security, it could have a big role to play in the future.

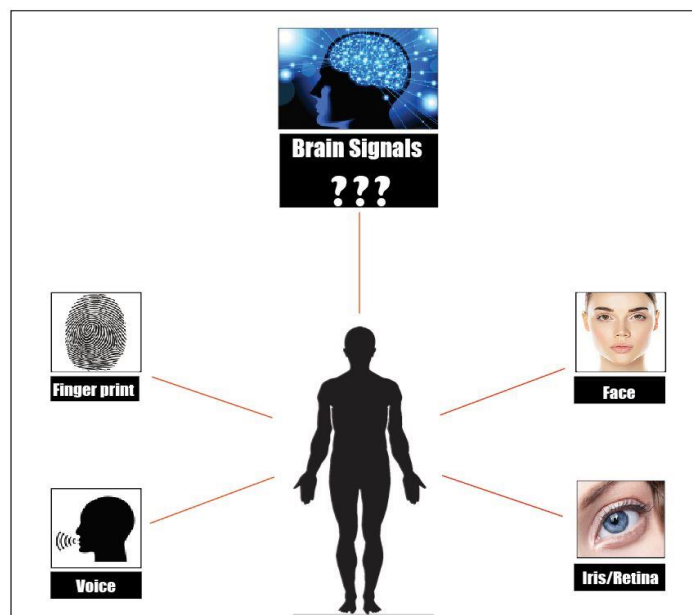


Figure 2.2. Brain signals beside the most practical biometric authentication techniques.

2.2.6 Neural oscillations (Brainwaves)

Neural oscillations, or brainwaves, are an essential mechanism to enable the synchronization of neural activity inside and around brain areas and help the accurate temporal organisation of neural processes underlying memory, cognition, behaviour, and perception. They occur during activation of large clusters of neurons, though they can occur with a single neuron as well [58]. Neural tissue can generate oscillatory activity in a couple of different ways, by either, interactions between neurons, or driven by mechanisms within separate neurons. “The interaction between neurons can give rise to oscillations at a different frequency than the firing frequency of individual neurons” [59].

2.2.6.1 History

Hans Berger was a German psychiatrist who observed the first human neural oscillations as early as 1924. He invented electroencephalography (EEG) for the recording of "brain waves" by measuring electrical activity in the brain of a patient in his hospital who had suffered skull damage [60]. At first, he got some disappointing results in trying to discover the physiological basis of psychic phenomena in his early work; Berger decided to try to discover the electrical activity of the brain. He discovered the alpha wave and documented these waves along with the beta activity. He found that when we are fully awake, the alpha waves decrease and beta waves become dominant. As he was the discoverer of the alpha brainwave rhythm, it is known as "Berger's wave". “More than 50 years later, intrinsic oscillatory behaviour was encountered invertebrate neurons, but its functional role is still not fully understood”. There even became conjecture that maybe humans could control the devices, by using these signals without specific supplies of muscles and nerves; all of this remained speculation for some time [61].

2.2.6.2 Electroencephalography (EEG)

EEG is one of the techniques for brain imaging. Different types of brain imaging methods allow researchers and doctors to view problems or activity inside the human brain, without invasive neurosurgery. A few safe imaging techniques are accepted in use today in hospitals and research facilities throughout the world. Table 2.2 shows these techniques [62].

Table 2.2. The methodology of brain imaging techniques and the ways that they work.

<i>Brain Imaging Techniques</i>		
<i>Methodology</i>	<i>What is imaged?</i>	<i>How?</i>
<i>Electroencephalography (EEG)</i>	<i>Changes in electrical brain current</i>	<i>Electrodes placed on scalp measure electrical brain waves</i>
<i>Computed (Axial) Tomography Scan (CT or CAT)</i>	<i>X-ray images of the brain</i>	<i>Multiple images (tomograms) are taken by rotating X-ray tubes. Doesn't image function</i>
<i>Position Emission Tomography (PET)</i>	<i>Emissions from radioactive chemicals in the blood</i>	<i>Radioactive isotopes injected into the blood are detected like X-ray</i>
<i>Magnetoencephalography (MEG)</i>	<i>Changes in electrical brain current</i>	<i>Similar to EEG but magnetic brain waves are measured instead of electrical brain waves</i>
<i>Functional Magnetic Resonance Imaging (fMRI)</i>	<i>Blood flow; oxyhemoglobin to deoxyhemoglobin ratio</i>	<i>Relies on the magnetic properties of blood. Shows brain function spatially and temporally</i>

Electroencephalography (encephalon = brain), or EEG is an electrophysiological observing technique to capture electrical activity generated by the brain from electrodes placed on the scalp surface. “EEG refers to the recording of the brain's spontaneous electrical activity over a period of time, as recorded from multiple electrodes placed on the scalp” [63]. In comparison to other imaging methods, EEG has some benefits. It is an excellent tool for studying the neurocognitive processes underlying a person’s behaviour for a number of reasons: 1) EEG has very high time resolution and captures cognitive processes in the time frame in which cognition occurs. 2) EEG directly measures neural activity. 3) EEG is inexpensive, lightweight, and portable. 4) EEG monitors cognitive-affective processing in the absence of behavioural responses [64]:



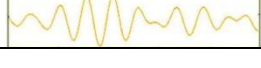
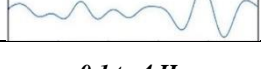

One of the fastest available imaging methods is EEG, which can take thousands of snaps per second. EEG time course 100 years ago was a plot on paper. The data displays as a continuous flow of voltages on a screen in the current systems. “It measures electrical activity generated by the synchronized activity of thousands of neurons (in voltage) and provides excellent time resolution, allowing you to analyse which brain areas are active at a certain time – even at sub-second timescales” [65].

2.2.6.3 Brainwave Types (Frequencies)

Brainwaves are produced by synchronized electrical pulses from masses of neurons communicating with each other. Thinking of brainwaves as musical notes is a useful metaphor. For example, the low-frequency waves are like an intensely powerful drumbeat and on the other hand, the higher-frequency waves are more like a delicate high-pitched

flute. “Like a symphony, the higher and lower frequencies link and cohere with each other through harmonics” [66]. The brainwaves are changing according to what the human is feeling and doing. When weaker brainwaves are dominant, we can feel lazy, tired, dreamy or slow. The higher brainwaves are dominant when we feel hyper-alert or wired. In terms of frequency, we all have five types of brainwaves (Gamma, Beta, Alpha, Theta, and Delta). “Each frequency is measured in cycles per second (Hz) and has its own set of characteristics representing a specific level of brain activity and a unique state of consciousness” [67]. This is represented in Table 2.3.

Table 2.3. Types of brainwaves and their frequency rates and mental state situation.

<i>Wave</i>	<i>Frequency</i>	<i>Mental State</i>
<i>Gamma</i>	<p><i>Above 40 Hz</i></p> 	<i>Thinking, integrated thought</i>
<i>Beta</i>	<p><i>13-40 Hz.</i></p> 	<i>Alertness, focused, integrated, thinking, agitation, aware of self and surroundings</i>
<i>Alpha</i>	<p><i>8-12 Hz.</i></p> 	<i>Relaxed, non-agitated, conscious state of mind</i>
<i>Theta</i>	<p><i>4-7 Hz</i></p> 	<i>Intuitive, creative, recall, fantasy, dreamlike, drowsy and knowing</i>
<i>Delta</i>	<p><i>0.1 to 4 Hz</i></p> 	<i>Deep, dreamless sleep, trance, and unconscious</i>

2.3 Brain-Computer Interface (BCI):

There is a big question in people’s minds nowadays; is there any technology to help the mind to communicate with robots, artificial intelligence and other minds directly through technologies? In the period of the last 50 years, researchers have made impressive progress toward achieving such a dream with BCI technology. “Brain-computer interface is a method of communication based on neural activity generated by the brain and is independent of its normal output pathways of peripheral nerves and muscles” [68]. BCIs are developed by the research community with some applications in mind for the generation of new assistive devices [69]. “They have facilitated re-establishing the movement ability for physically challenged users and replacing lost motor functionality” [70].

The predicted future for BCI and the research community is to study the participation of BCI in the life of disabled individuals through medical applications. Some recent studies have targeted normal individuals by exploring the use of BCIs as an input device and examining the generation of hands-free applications [71].

Brain-computer interface technology is a powerful communication tool for both users and systems. There is no need for any external devices or muscle involvement to issue instructions and complete the communication. Normal individuals have been targeted in most recent studies by exploring the use of BCIs as an input device and exploring the generation of hands-free applications [72]. It translates the specific features of the brain signal that indicate the intent of the user into computer readable commands. To control an electronic device these commands can be exerted [73].

2.3.1 BCI Types

The BCI can be separated into invasive, partially invasive and non-invasive types as shown in Figure 2.3. BCI has a couple of different types [74], but the main purpose of all types is to acquire the electrical signals which communicate nerve cells in the brain and turn them into a signal that can be detected by another external device.

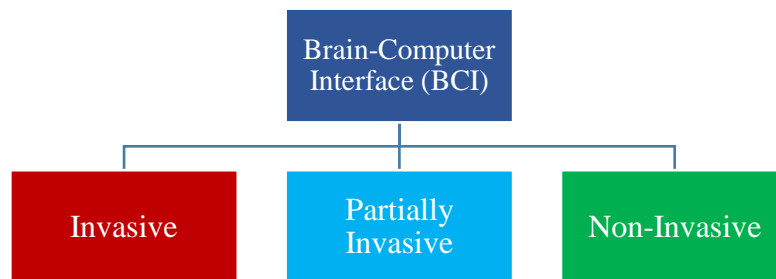


Figure 2.3. BCI types to capture the electronic signals

2.3.1.1 Invasive BCI

Invasive BCI: recording the signals that occurs when electrodes enter brain tissue. This is a permanent basis method that buries electrodes within the brain. They require complex surgery to implant and usually involve a permanent hole in the skull (Fig 2.4). A better signal quality, a higher range of frequency, and spatial resolution can be captured from this method typically. This technique records neural activity from an assembly of single brain cells.

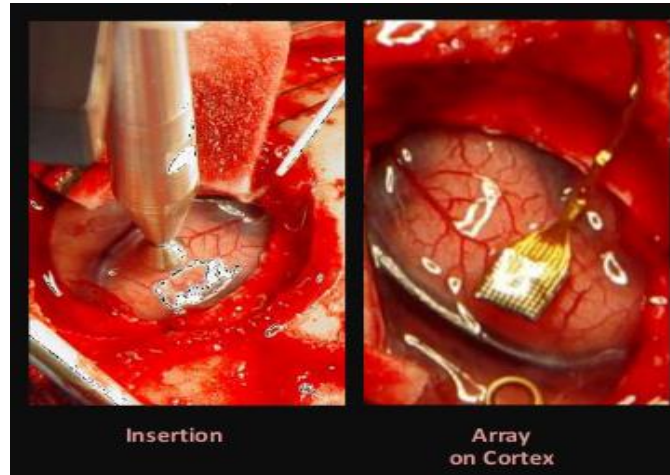


Figure 2.4: Photos of an invasive BCI implant on human brain

2.3.1.2 Partially Invasive

In BCI Partially-Invasive the electrodes are placed inside of the skull but rest outside the brain rather than within the grey matter above the brain's surface (Fig 2.5). A good example of partially invasive BCI is Electrocorticography (ECoG). ECoG is a type of monitoring that uses electrodes placed directly on the bare surface of the brain to record brainwaves from the cerebral cortex. Electroencephalography (EEG) electrodes monitor the same activity from outside of the skull. "Recent studies have shown that ECoG amplitudes in certain frequency bands carry substantial information about the task-related activity, such as motor execution and planning, auditory processing, and visual-spatial attention" [75].

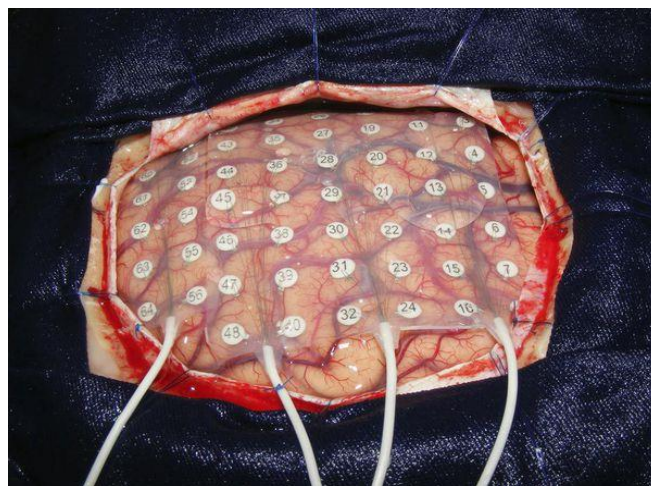


Figure 2.5. A partially invasive BCI on human brain

2.3.1.3 Non-Invasive BCI

No surgery is needed in this type of BCI. Instead, the sensors or electrodes are placed over the head or (via a hat, belt, patch or a headset) (Fig 2.6) to measure Electroencephalography (EEG), which reads the rhythm of brain activities.



Figure 2.6. A type of non-invasive BCI device.

Non-invasive BCI produces weak signal quality because the skull bone reduces signals and brain waves produced by the neurons. These kinds of signals, which are recorded in a non-invasive way, have been used to control muscles and restore limited movements.

Electromyography (EMG) is an analytical process to measure muscles and the nerve cells which are controlling them. “EMG results can reveal nerve dysfunction, muscle dysfunction or problems with nerve-to-muscle signal transmission” [76].

The following image (Fig 2.7) shows the different layers of the brain and where the signal is taken from.

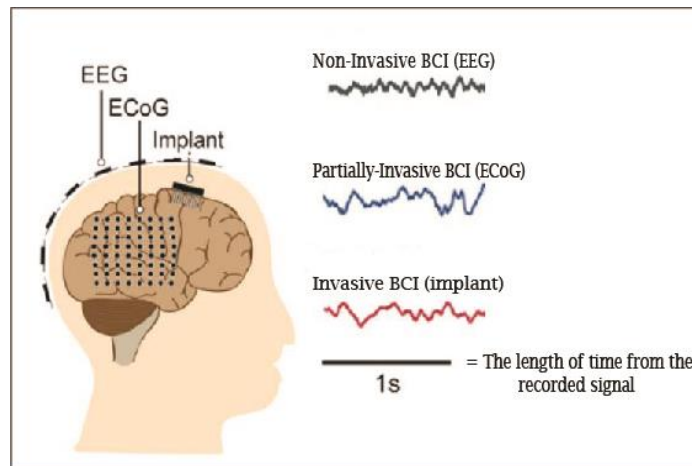


Figure 2.7. The way that BCI captures the signals from the human brain

When looking at other brain devices like partially invasive and invasive, EEG devices feature ease of calibration and use. Table 2.4 given below shows some popular wireless EEG devices that are available to consumers [77].

Table 2.4: Types of some popular non-invasive wireless headsets to capture EEG data.

<i>Name of Device</i>	<i>Electrode</i>	<i>Number of Channels</i>
<i>Cognitionics Mobile-72</i>	<i>Dry</i>	<i>64</i>
<i>ENOBIO 32</i>	<i>Dry</i>	<i>32</i>
<i>mBrainTrain</i>	<i>Wet</i>	<i>24</i>
<i>OpenBCI</i>	<i>Dry</i>	<i>16</i>
<i>EMOTIV Epoc+</i>	<i>Wet</i>	<i>14</i>
<i>EMOTIV Insight</i>	<i>Dry</i>	<i>5</i>
<i>Muse</i>	<i>Dry</i>	<i>2</i>
<i>NeuroSky Mindwave</i>	<i>Dry</i>	<i>1</i>

2.3.1.3.1 *The Emotiv EPOC+*

Emotiv EPOC+ [Fig 2.8] is a brain-computer interface device, providing high resolution and full spatial resolution. “It is a 14-channel wireless EEG, designed for contextualized research and advanced BCI applications” [78].

In 2013, Emotiv Inc. released EPOC+, which is a research-oriented wireless headset that records 14-channel EEG. It uses saline-based wet sensors instead of other conventional EEG systems that use sticky gels. Emotiv EPOC+ is a 14-channel wireless EEG, designed for contextualized research and advanced BCI applications. The EPOC+ provides access to the dense array, high quality, and raw EEG data using our subscription-based software which records EEG signals. The electrodes are placed on the scalp according to an extended 10-20 system for EEG measurement. Users can wear EPOC in everyday life as it is wireless, lightweight, and battery-powered. “The EPOC+ measures both EEG and 9-axis motion data. Data is transmitted wirelessly through Bluetooth. The 14 channel wireless EPOC+ is designed for research and brain-computer interface used, and EEG can be obtained with an Emotiv Pure” [79].



Figure 2.8. Emotiv EPOC + BCI headset device

The EPOC+ is designed to provide good coverage of the frontal and prefrontal lobes and also provides coverage of the temporal, parietal and occipital lobes. This device has two electrode arms each containing 9 locations (7 sensors + 2 references). Two sensor locations (M1 / M2) already have rubber sensors fitted because they are the alternative positions for the default references (P3 / P4) (Figure 2.9). Channel names based on the International 10-20 locations are AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, and AF4.

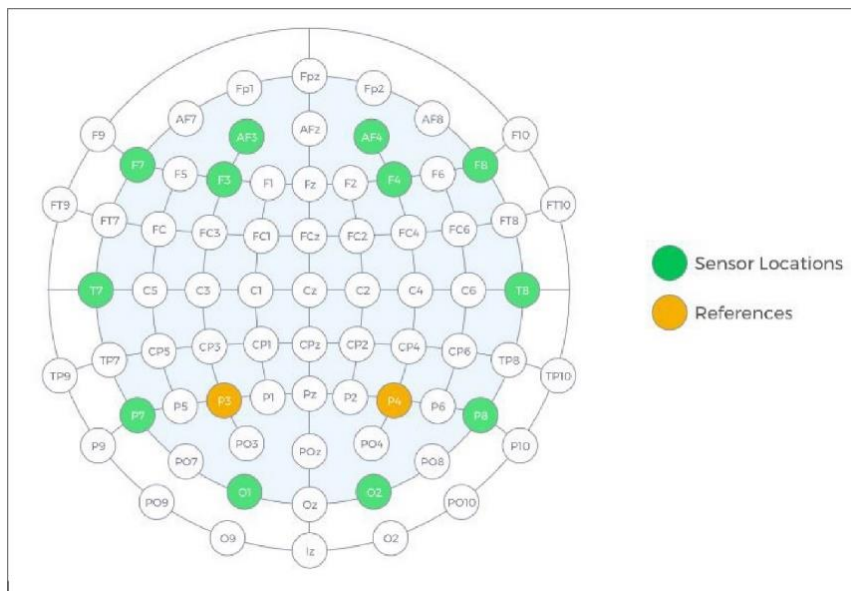


Figure 2.9. Illustration of location of Emotiv EPOC + electrodes on the scalp [66]

2.3.2 BCI System process

A BCI is a system that can distinguish a definite set of forms in brain signals following five sequential stages (Figure 2.10): signal acquisition, pre-processing (signal enhancement), feature extraction, classification, and the application interface [80]

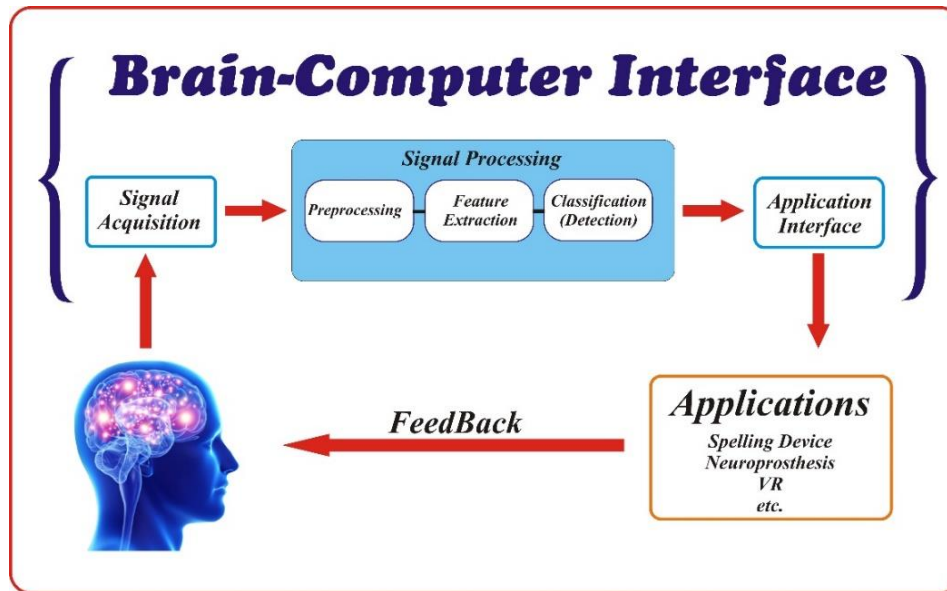


Figure 2.10. Brain-Computer Interface process

2.3.2.1 Signal acquisition

Signal acquisition is a considerable challenge in the field of BCI. Some methods focus on EEG signals; however, other methods exist that can capture neurological activity. There are some weaknesses and strengths in each method for acquiring different types of signals from the brain. End use is a factor that was intended by the designer which filters out which method you should use for capturing specific signals [81]. These electrical signals can be recorded as non-invasive or invasive. Captured signal strength is usually low, they are required to be augmented and digitized to be ready for use in different computer applications.

One of the main components of any BCI system is evaluating brain oscillations. Different methods for signal capturing are presented in studies. As shown in Figure 2.11, there are two general classes of brain acquisition methods: invasive and non-invasive methods. “In invasive technology, electrodes are neurosurgically implanted either inside the user’s brain or over the surface of the brain, while in non-invasive technologies; the brain activity is measured using external sensors” [82].

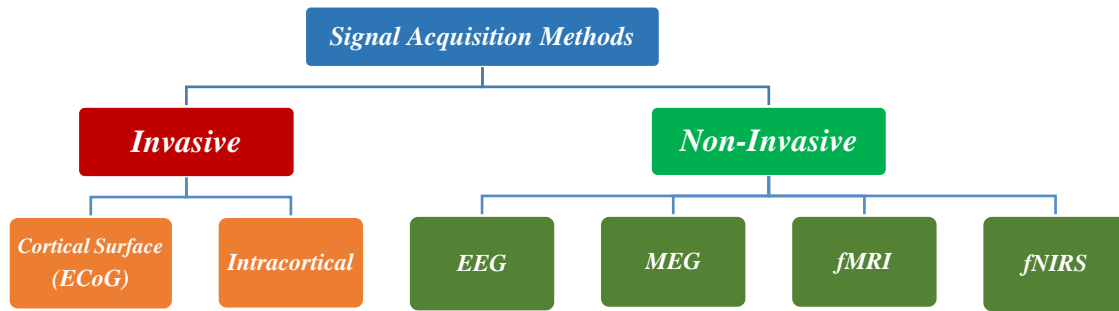


Figure 2.11. Brain signal acquisition methods.

2.3.2.2 Pre-processing or signal enhancement

After the signal acquisition part, signals are going to be pre-processed. Signal pre-processing is also called Signal Enhancement [83]. In general, the acquired brain signals are made unclear by noise and artifacts. The artifacts are eye blinks, eye movements, heartbeat. In addition to these, muscular movements and power line intrusions are also mixed with brain signals [84]. A couple of different methods are used for artifact removal which “the most frequently used methods are Common Average Referencing (CAR), Surface Laplacian (SL), Common Spatial Patterns (CSP), Independent Component Analysis (ICA), Principal Component Analysis (PCA), Common Spatio-Spatial Patterns (CSSP), Single Value Decomposition (SVD), Frequency Normalization (FreqNorm), Robust Kalman Filtering (RKF), Local Averaging Technique (LAT), Common Spatial Subspace Decomposition (CSSD), etc. The most frequently used methods are CAR, SL, CSP, ICA, PCA and Adaptive Filtering” [85]. Overall, these techniques have specific purposes that could match each objective of experiments conducted [86].

2.3.2.3 Feature extraction

After pre-processing and filtering, the EEG signals will pass through the feature extraction process and select particular features by some feature selection methods. Some researchers used “a hybrid BSS-SVM system to extract the movement-related features from the EEGs” [87]. The authors used a Blind Source Separation (BSS) algorithm to separate the EEG and measured EOG into statistically independent sources and SVM classifier to extract the features. Another method was “feature extraction methods based on Self Organizing Maps (SOM) using auto-regressive spectrum” [88]. The SOM consists of a regular, generally two-dimensional, network of map neurons. The neurons are linked one to another according to the map topology. This topology is taken into account through a neighbourhood function to

extract the needed features. The other feature extraction method is the combination of time-frequency and Linear Discriminant Analysis (LDA) technique [89]. Discrete Wavelet Transform (DWT) feature extraction method has been working to control the pointer movement via EEG. In another study, db40 wavelet packet decomposition was another feature selection method which was used to select features of EEG signals to control the four-direction movement of a ball on the computer screen [90].

2.3.2.4 Classification

Different brain activity forms must be produced by the user in order to control a BCI that will be translated into commands and identified by the system. This identification relies on a specific classification algorithm. Using classification algorithms is the most popular tactic for this purpose. These procedures are used to identify “patterns” of brain activity [91]. “Classification algorithms are divided into five different categories: linear classifiers, neural networks, nonlinear Bayesian classifiers, nearest neighbour classifiers and combinations of classifiers” [92].

A large type of classifiers has been tried in BCI research. The decision trees [93] and the whole category of fuzzy classifiers [94] have not been attempted in BCI research, which are the two most relevant classifiers. There are several other efficient and well-known classifiers that can be found in the literature such as Bagging or Arcing [95]. These types of algorithms could prove useful as they all succeeded in several other pattern recognition problems.

2.3.2.5 Application interface

There are many different BCI applications (Fig 2.12), especially for disabled individuals. “It reads the waves produced by the brain and translates these signals into actions and commands that can control the computer(s)” [96]. Remote communication and Mind reading have their uniqueness in numerous fields such as self-regulation, marketing, production, educational, security, games, and entertainment. It makes a joint connection between users and the nearby systems [97].

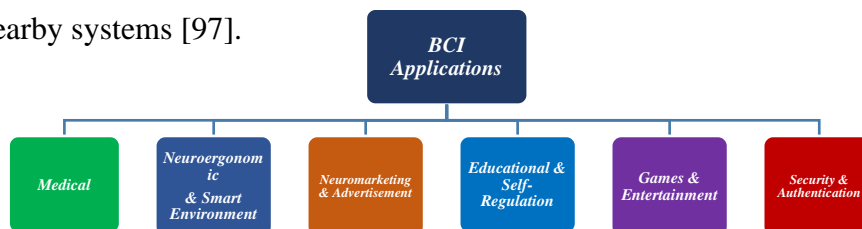


Figure 2.12. BCI Application Fields

2.4 Brain-Based Biometric Authentication

Currently, biometrics, such as voice, fingerprint, iris, face, have been widely studied in literature and especially in real-life situations. However, there are some weaknesses in these biometrics [98]. For example, Fingerprints can be faked through latex milk, plastic mould and wood glue [99]; a fingerprint made by a 2D picture from a normal printer [100]; and maybe a high-resolution photography [101]. Face, fingerprints, retina and iris are all non-cancellable. This means that, they cannot be replaced, and a new eye or finger cannot be grown again or face volitionally cannot be changed. We need a biometric more secure than any of these, which would be more difficult to replicate, and it would be cancellable. Brain electrical activity may meet these criteria. It is not visible to replicate, and the security pattern could be an image in the mind or a brain function that could be changed anytime.

There are a couple of unique advantages in brain signal compared with other biometrics. First, in order to record EEG, the person must be alive [102]. Fingerprint and Face can be maintained even from a dead human body, or the iris, after death, is still valid for recognition for a few hours after death [103]. According to this matter, the user has to be alive and in a conscious state to produce EEG data. Second, brain signal voltage will fall off dramatically with distance from the brain.

Despite the many advantages of brain-based biometric, it is still not extensively adopted because considerable research still must be done. To evaluate how reasonable a biometric is as an authentication method, there are seven universal factors including universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention [104]. Table 2.5 compares five biometrics including brainwaves in terms of the seven factors mentioned [98].

Table 2.5. Comparison of some biometrics with brainwave biometrics

Biometric Identifier	Universality	Uniqueness	Permanence	Collectability	Performance	Accessibility	Circumvention
<i>DNA</i>	High	High	High	Low	High	Low	Low
<i>Face</i>	High	Low	Medium	High	Low	High	High
<i>Fingerprint</i>	Medium	High	High	Medium	High	Medium	Medium
<i>Iris</i>	High	High	High	Medium	High	Low	Low
<i>Brainwave</i>	High	High	High	Medium	High	Medium	High

Recently, scientists and researchers have been carrying out many attempts to observing the unique patterns of the brain signal. Several different methods have been used to analyse EEG signals. Regarding the recent progression of EEG signal acquisition devices, the capability of providing better results is going higher and these processes are getting simpler.

2.4.1 Brain-Based Authentication Methods

There are different studies using different tasks, extracted features, and classifiers for doing their experiments to get higher accuracy rates of brainwaves to use them for authentication purposes.

An authentication system proposed by Riera et al.[105], used a combination of ECG and EEG signals, for discriminating the situation. The achieved accuracy for this study was higher than others even for the relaxation task. This is due to the added ECG channel. A different approach proposed by Jayarathne et al.[106], tested the possibility of person authentication by thinking about a specific number. Yeom et al.[107] presented a method to extract unique signals using “self- and non-self” face pictures. In response to self-face, each subject has their own characteristic, so EEG patterns must be unique in regard to this subject. The accuracy rate for each system mostly depends on the mentioned aspects.

Chen et al.[19] proposed an authentication system, which is based on Rapid Serial Visual Presentation (RSVP) stimulus. The test was on 29 individuals who participated, and a brain amp was used to obtain EEG signals. For data collection in this process, both dry and wet electrodes were used separately. Three signs were used as targets, and participants should count the samples among some randomly generated trials. 600 targets were shown to record EEG signals. The specific features were considered by a special correlation constant. Following the flowchart (Fig 2.13) is the deployment of a potential system. “During registration, the user chooses a password, consisting of three symbols. These symbols are displayed in random order together with 22 other non-password symbols in fast progression (i.e. RSVP). The EEG data is evaluated and a model estimated. During the login process, all symbols are displayed in RSVP fashion and the login decision is based on the classifier’s output of the EEG data”.

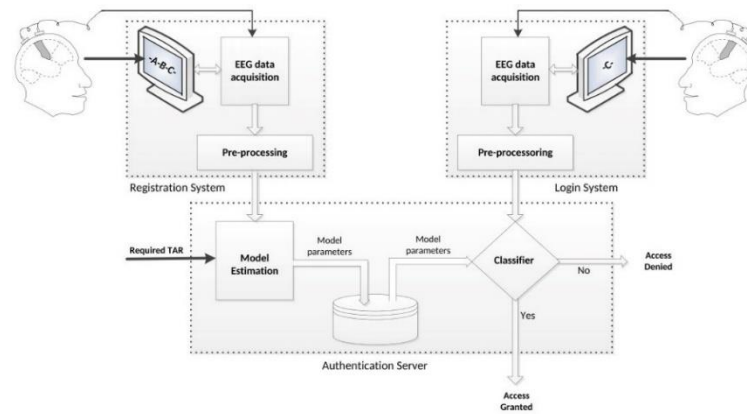


Figure 2.13. Potential system deployment Flowchart [14]

The average accuracy, in the single trial classification process using 16-channel configurations that all were wet, was 87.8%; and for the 16-channel configurations which all were dry, it was 78.2%. Both different types of dry and wet processes presented 100% accuracy with 27.0s and 10.7s average login times respectively. There was no confident response for the older one after training the system for a new password.

A new approach presented by Chuang et al.[20] is one of the best-performing methods in terms of security and usability. 15 subject were recruited and the MindWave was used to obtain data. From the performance of seven different tasks such as sports activity, breathing, audio listening, simulated finger movement, colour identification, singing recitation, and pass-thought. The only extracted frequencies were Alpha and Beta. The signals were compacted in the timestamps to make the data a single measurement. To count the similarity between pairs of signals, the Cosine similarity method was used. The similarities of signals were checked between different subjects and within each subject separately. The classification process is done with the k-nearest Neighbour (k- NN) algorithm.

The best classification accuracies were for colour, audio, and sport. However, 99% accuracy has been shown via the proposed method. The most difficult one was for the pass-thought task according to the results of the questionnaire that determined for user-friendliness with different tasks. In terms of complexity of the user strategy, breathing, colour, and audio tasks were the simplest and less time consuming which made the system more practical.

An approach was presented according to EEG spectral coherence connectivity by La Rocca et al.[21] for finding the uniqueness of signals. Using information swapped from different areas of the brain was the main idea of this approach to finding uniqueness. The brain signals

of 108 users were collected during open resting and eyes-closed state conditions. The captured EEG data was from using a 64-channel device with 160 Hz sampling rate. High-pass band filtering was used to clean the data. Spectral coherence (COH) and power spectral density (PSD) analysis techniques were used to extract mental features. “COH quantifies the level of synchrony between two stationary signals at particular frequencies. PSD is the frequency response of a random or periodic signal, demonstrating average power spread as a function of frequency”. To calculate uniqueness, two different algorithms were used separately in this process, which were Mahalanobis classifiers, and another algorithm named match-score. The accuracy rate of 100% was acquired for COH features of eyes-closed and 90.49% for PSD eyes closed data. This method showed a strong and high accuracy for user identification. The better accuracy was for COH features with the Match-score algorithm. However, it requires static EEG signals, and the duration of the analysis process is long.

CEREBRE protocol which was presented by Ruiz-Blondet et al.[22], uses EEG signals to authenticate a user. 400 different images including 100 celebrity faces, 100 food images, 100 sine gratings, and 100 low-frequency words were used as stimulus. Besides those categories, an oddball stimulus category also was included to further develop the required EEG pattern. 50 individuals participated in this research. Event-Related Potentials (ERP) were cleared with a band-pass filter (1–55 Hz) and based on normalized cross-correlation, a simple discriminant function was used for classification. According to the results, the minimal (3 channels, 4 categories) classification method showed the highest accuracy (all the trials were used) but both minimal and maximal classifiers showed 100% accuracy for all channels and all classifiers. The results showed that the most accuracy was for the single-stimulus classifiers based on food and oddball stimulus. Identity classification which was based on resting state showed a weak performance for EEG. Memory recall authentication task (which some studies call “pass-thoughts” [23]) had weak performance too, because of the changeable thinking time.

2.4.2 Signal acquisition protocols

There are three groups of protocols used for recording EEG in general: mental tasks, resting states, and tasks with an external stimulus. Choosing each protocol can influence the procedure of authentication and the accuracy. For instance, for mental tasks or the resting states an EEG recording device is required; while, external stimuli tasks need devices to

make the appropriate stimulation. Then again, resting states tasks can be effortlessly influenced by artifacts and noisy environment, while a higher “Signal-to-Noise Ratio” (SNR) can be seen in tasks followed by external stimuli and mental tasks. This can be accomplished by recognizing “Event Related Potential” (ERP) [108]. For example, to observe the ERP reactions to the visual stimuli, the visual cortex, occipital lobe and central region are engaging.

According to this and with some compromising, the number of electrodes that have been utilized in this study to record brain signals have been reduced. Many different mental tasks have been tested and good results achieved. However, most of them are very complex and time consuming for authentication process. Tasks like imagining some physical body movements [109], counting numbers in mind, sing a song, and focusing on a desired thought [110], imagining the movement of a given geometric shape around an axis [111], and some other sets of mental tasks that individuals are asked to perform.

EEG as biometric authentication is still one of the popular subjects among researchers and scientists. Many different methods were proposed in different studies. In terms of the authentication process, all biometric methods should have four sets of requirements, which are collectability, universality, uniqueness, and permanency. All of these four requirements are important for any EEG-based method to use brain signal as a biometric authentication technique.

Every EEG-based authentication process has four main steps as follows: signal acquisition, pre-processing (cleaning the data), feature extraction, and classification. Acquiring the brain signals and EEG data recording is very important, which can influence the results directly. There are three main protocols for EEG data recording: tasks with an external stimulus, mental tasks, and resting states. It is important to select an appropriate protocol for authentication purposes as it has a great effect on the accuracy of the results.

Resting state protocols are very popular in EEG signal recording especially for authentication purposes [24]. In this protocol, the individuals should sit in an area as quiet as possible or at least with minimal noise for recording the EEG data. Resting states make the alpha band the dominant brainwave among others [25]. The simplicity of this protocol makes it more useful because it can be done without using any extra equipment other than a

brain device in comparison to other protocols; however, it should be done in a quiet environment.

Tasks with external stimuli cover a wide range, for example, reading different types of texts [26], recognizing different types of images [27], recognizing different geometric figures [28], moving and static substances [29]. Tasks with external stimuli have the advantage of permanency condition over time but their disadvantage is their need for external equipment. Another EEG recording protocol is mental tasks, which includes imagining body movements and mental activities. For example, images of moving hands, head, or feet and sometimes both doing the movements and imagining the movements [30].

According to different studies, imaginary tasks have achieved better results in comparison to physical activities. There are other experiments such as counting in mind [31], picturing patterns by imagining 2D and 3D images [32].

Some studies achieved high accuracy results using different EEG recording protocols and tasks for authentication purposes. Armstrong et al. [33] used a text reading task while ERPs were collected from participants and applying SVM and non-SVM classifiers which achieved 89% accuracy as results. Patel et al. [34] used self-photo and non-self-photo as visual stimulation. They used a backpropagation (BP) neural network classifier on the extracted features based on fuzzy entropy and achieved an average success rate of 92.5%. Zhendong et al. [35] used visual/audio stimuli for their experiment to recall some specific subjects including water bottle, handle, screwdriver, which achieved 87.3% accuracy as the result of their work. Abo-Zahhad et al. [36] proposed a multi-level EEG system using eye blinking, which by applying the data on an LDA classifier from the band power spectral features achieved a high accuracy rate of 98.56% for their experiment. The main problem in most studies in this area is the stability of the method through time that is important to cover the permanency set for any authentication process.

2.4.3 Mental Visualization

It is shown that better results have been achieved from imaginary tasks and protocols in comparison to the physical ones. On the other hand, a popular theory called “dual coding” [112] showed that graphical substances such as images, shapes or pictures are easier to remember in comparison to the number, words and sequences. Basically, this theory explains that these types of objects are determined (memorized) with 2 particular codes

(verbal and pictorial) whereas a number sequence or a word are determined by a single verbal code. It has been recommended in a study that despite the fact that photos and words share indistinguishable semantic meaning, pictures are easier to remember and more memorable because they have more particular codes than words [113]. Many studies concluded in their results that words are more memorable than numbers, and graphical patterns, shapes and images are more memorable than words. These progresses reached out to the long term-memories as appropriate as the short-term memories.

Mental imagery or colloquially “visualizing,” “seeing in the mind's eye,” “hearing in the head,” “imagining the feel of,” resembles imaginary experience, but happens in the lack of the real external stimuli. Mental images are always picturing something or other which appears in the mind, and by this means functioning as a form of mental picture [114]. Some researchers have shown that visual mental imagery is in the control of frontal-parietal regions and can rely on occipital-temporal regions of the brain.

In a memory test experience, participants responded “remember,” “know,” or “new.” “In the imagery test, participants responded “high vividness,” “moderate vividness,” or “low vividness.” Visual memory (old-remember) and visual imagery (old-high vividness) were commonly associated with activity in frontal-parietal control regions and occipital-temporal sensory regions. In addition, visual memory produced greater activity than visual imagery in parietal and occipital-temporal regions” [115]. Regarding the experiments and research about mental imagery, we decided to concentrate on this subject and use it as a brain-ID. A new algorithm was designed to acquire the brain signal for authentication purposes.

As we mentioned before, there are a few of different ways which are designed for acquiring the brain activities, including Magnetoencephalography (MEG), Functional Magnetic Resonance Imaging (fMRI), Positron Emission Tomography (PET), Near-Infrared Spectroscopy (NIRS) and Electroencephalography (EEG). In comparison to other methods, EEG is a non-invasive method, which is not very expensive and allows recording the signals passively. EEG-Based user authentication systems are currently popular in BCI security and authentication applications. Recently, scientists and researchers have been doing many attempts to observing the pattern uniqueness of the brain signal. Several different methods have been used to analyse EEG signals. With regard to the recent progression of EEG signal acquisition devices, the capability of providing better results is going higher and these

Page 35

processes are getting simpler. We are going to review a couple of different tactics of EEG capturing methods to acquire better accuracy and check the applicability of using brain signal for authentication purposes. Human brain signals can change over time by experiencing different events in life. The brain cannot function properly in some specific moments to create a stable pattern for a task. It could be for some reason like being sick, anxious, drunk, stressed, etc.

2.4.4 Alpha brainwaves and deep breathing

The human brain has billions of neurons. The communication between neurons creates electrical signals. All the emotions, behaviours, and thoughts for any human being are based on these electrical pulses, which are called brainwaves. There are five types of brainwaves in general: Delta, Theta, Alpha, Beta, and Gamma. Each of these brainwaves has specific frequency rates, which they would constantly change depending on the human's mental and physical situation. Research and studies showed alpha is the best type of brainwave for authentication purposes in comparison to other types [116].

The brain is experiencing many different situations according to different events that happen to each person in life. It makes the brain to be out of its normal baseline and state. Therefore, it creates some situations like stress, anxiety, sickness. To concur and pass those situations, the brain needs to get back to its normal state.

Research reveals that, deep breathing can be counted as a healing exercise. It can reduce anxiety and helps to respond to stress effectively. It has a psychological effect that can bring calmness and a feeling of peace [117]. Most importantly, deep breathing can improve alpha waves, and therefore, increases feelings of relaxation. The human brain is using nearly 20% of all the oxygen that the whole body needs, which means the brain is very oxygen dependent. Therefore, the deficiency in oxygen could cause fuzziness, being dizzy, distracted, and out-of-focus. Deep breathing is the best way to bring back human brainwaves to a normal state. As mentioned before, deep breathing has a direct connection with alpha waves and the relaxation states of the human brain. It increases the activity of alpha waves, which is helpful for a person to be relaxed by reducing stress and anxiety.

A distracted human brain can go back to its normal relaxed state by improving the alpha waves. It can be done by doing deep breathing, which could stabilize the brain state and improve the permanency of the brain pattern no matter what situation the brain experienced.

2.5 Summary

In this chapter, after an overview of the security authentication methods and biometrics, the research turned to the concept of brain-computer interface (BCI) systems, brain-based authentication methods and current issues associated with these methods. The review presented in this chapter specifically focuses in this area following the objectives of the proposed study. Most importantly, studies related to brain-based authentication processes are reviewed covering different techniques that have been used by other researchers for signal processing, signal enhancement, feature extractions methods, and classifications of their authentication system. Identifying the advantages and shortcomings of the existing methods are the main reason new methods and strategies were devised.

Finally, recommendations about new strategy and BCI methods are proposed to be used in different situations to improve the authentication system. BCI environments are currently an attractive topic in many areas such as healthcare, gaming, education, medical, psychology and most importantly for data security purposes.

There are many different issues influencing the process of the BCI systems in brain-based authentication methods such as weakness of the human brain signal, the BCI devices for recording the data, the environment and the situations of anyone's life which can affect the brain stability through time. A number of these issues have been resolved by using some specific BCI methods but according to the literature in this chapter, there are still shortcomings in the brain-based authentication processes in terms of security level, usability, and most importantly, stability and permanency of the security brain pattern in time. Although some of the previous experiments achieved high accuracy rates for the methods used, the majority of them suffer from the usability of the system according to the security level and how time-consuming the process is, and on the other hand the permanency of the system through time.

The signal acquisition protocols that have been used by most previous studies are very time consuming, need to use an external stimulus and be in a specific environment, otherwise the system would not have an appropriate result. In general, these types of protocols are very time-consuming and impractical and easy to apply. In addition, the level of security goes down according to the use of an external stimuli or a body movement strategy.

Several studies have used protocols following better techniques and methods in the BCI system that have achieved higher accuracy results and their systems are more practical and secure and less time-consuming, but they still suffer from the lack of stability of their system through time. The security pattern that they used in their system is not stable according to the human's life situation that can affect the functionality of the brain and can influence the brain pattern.

As we have shown, to find a suitable technique for each purpose, the target must be considered. There is no specific technique to cover all purposes simultaneously at the moment, but the systems can be improved by using the right signal acquisition protocols and applying the right techniques on the BCI main process including the pre-processing, feature extraction and classification algorithms for authentication purposes. We believe the literature review presented in this chapter can help researchers choose the best protocols and methods to meet their goals in any brain-based authentication system.

Chapter 3

Research Methodology Overview

3.1 Introduction

In the previous chapter, the required research background was investigated in detail. The knowledge gained on open issues makes it possible for the research to design the appropriate methodology to pursue the work. The methodology adopted to achieve the stated objectives is introduced in this chapter. It began with a schematic diagram which is further explained to enable a clearer realization of the process to accomplish the objectives.

This chapter discusses the step-by-step process of completing each objective in the project. The methodology presents six phases which cover the entirety of the research. The first phase is investigating the different biometric techniques and brain-based authentication methods which was done in the previous chapter and covers the first research objective. The second phase is to introduce two coherent strategies for recording the brainwaves from participants by the brain device which covers the second objective of the project. The next three phases are Signal pre-processing, feature extraction and classification methods to cover the other three objectives for the project. These three phases are different for each of the two proposed strategies. The final phase is the results achieved and evaluating them according to the last objective of the project. Each phase has different steps which will be explained separately. The organization of this chapter is as follows: Section 3.1 gives an overview of research methodology. The methodology is illustrated in this section 3.2. The chapter continues with Section 3.3 which is the first phase of the methodology. This section explains the required information about the security authentication methods. Investigation of the recent biometric authentication techniques, brain signal as a new biometric method, and brain-computer interfaces are employed. At the end of this section an accurate investigation was done into different types of brain-based authentication methods, their advantages and shortcomings which gave us enough literature for the main goal of this project. Section 3.4 forms the second phase of the methodology which is signal acquisition. Two new user strategies are proposed in this phase to acquire the brain signals from participants by the BCI device and recording the raw EEG data in the computer system using its SDK software. Section 3.5 is the pre-processing phase of the project which starts with visual inspection of the recorded data, brain signals and brain activities using brain plots. It continues with signal filtering, removing the artifacts and bad channels and ICA algorithm to make the data ready for the phase 4 of the project which is section 3.6 feature extraction. For this part of the project some specific methods and algorithms were used such as Fast Fourier Transform

Page 40

(FFT), Power Spectrum Density (PSD) which was computed by Welch periodogram to extract the features according to the purpose of each method. Section 3.7 is the classification phase which explains different techniques to select and classify the extracted features according to both the proposed methods in the project and acquire the accuracy rates of each method. Section 3.7 presents the results, testing and comparisons with the results from other studies, analysis and evaluation and ended with a conclusion of the proposed methodology. This chapter covers the second objective of this thesis.

3.2 Research Framework

The research effort described in this thesis is geared towards the development of a BCI system to use human brain signal as a new biometric authentication method. To evaluate how reasonable a biometric is as an authentication method, there are four main universal factors such as uniqueness, permanence, collectability, performance. The performance and permanence or stability of the method are two of the main challenging contributors of any brain-based authentications to make the system more reliable to use brain signal as a security biometric technique.

These two factors should be improved to create a reliable brain-based biometric authentication method that is practical which could be implemented in any digital software and hardware as a security method. Because of the instability of the human brain regarding different situations in life and the weakness of the brain signals which makes the process of the system slower and more time-consuming, a system is needed to improve practicality, ease of use and stability of brain security pattern which can also heighten the security level of the method. To create such a system, a coherent user strategy and method is needed to make the process of the authentication faster, easier to use and stable through time by bringing back the distracted brain signals to their normal state that can be used as a permanent security pattern in time.

According to the main objectives of this project, to improve the universal protocols of biometric authentication systems, two new strategies and methods are proposed to improve the performance, security level and the permanency of brain-based authentication systems that could help using human brain signal as a new biometric security authentication method. The research concluded by testing, evaluating and validating the results.

A schematic diagram showing the methodological steps, summary and the contribution of this research is presented in Figure 3.1 which depicts the six phases involved and how the research is going to be implemented conceptually.

In general, the methodology discussed above plans to conduct research based on several factors needed for producing a reliable, stable and practical brain-based authentication method.

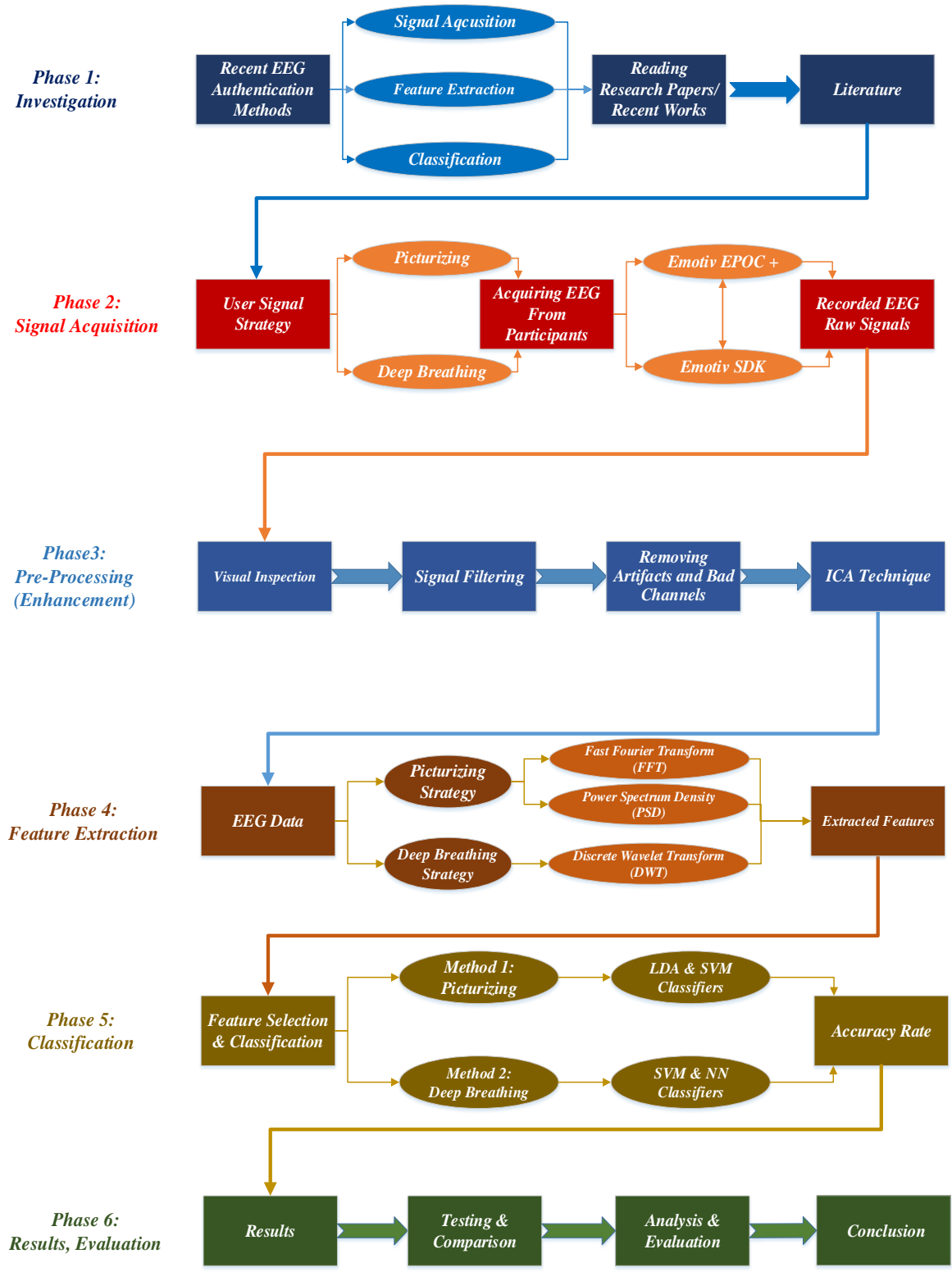


Figure 3.1: The six phases of the methodology proposed in this project

3.3 Phase 1: Investigation

Security authentication methods, biometrics authentication, brain signals, brain-computer interface, and brain-based authentication methods are the main concepts that are investigated in this phase. Gathering all the information investigated in these concepts presents the whole literature of this project.

3.3.1 Security Authentication Methods

It has been found that one of the words we toss around a lot when talking about information security is authentication. In security, authentication is the process of verifying whether someone (or something) is, in fact, who (or what) it is declared to be.

In general, three types of authentication factors are recognized:

- **Something You Know** – includes passwords, PINs, combinations, and code words
- **Something You Have** – includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices.
- **Something You Are** – Biometrics; includes all the behavioural and physiological human characteristics of any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, voice verification, etc.

These three types have been compared. The first two are easy to implement and the risk of being stolen and forgotten is high in both of them. But the third type which is biometrics don't have these issues and they are a most secure type than the other ones.

3.3.1.1 Biometrics

It was investigated that biometrics is the measurement and statistical analysis of a human's unique physical and behavioural characteristics. The basic premise of biometric authentication is that every person can be accurately identified by their intrinsic physical or behavioural traits.

Authentication by Biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics, software and applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry.

Components of biometric devices include the following:

- A reader or scanning device to record the biometric factor being authenticated.
- Software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data; and
- A database to securely store biometric data for comparison.

The two main types of biometric identifiers are either physiological characteristics or behavioural characteristics.

After investigating different types of biometrics and checking their advantages and disadvantages for authentication purposes, it was found that these biometrics have three main disadvantages: 1-they are visible and can be recorded and replicated by some specific software and technologies. 2-they are not replaceable, and the pattern is not changeable. 3-they are not useful for disabled individuals who are not able to use their hand or move their bodies. In this case, we need a new type of biometric that doesn't have these issues, which is human brain signal.

Biometrics has been a great alternative to traditional password authentication for several decades. Biometric authentication methods are such things as a fingerprint, face, iris, voice, and others. These biometrics have shown great positive results in terms of security, but they still suffer from some disadvantages. They are visible and can be recorded and replicated by some specific software and technologies; they are non-replaceable and most importantly they are not useful for some disabled individuals who are not able to use their hands and move their bodies. Therefore, researchers started studying brainwaves and the possibility of using them as a new biometric authentication because it is not visible, the pattern could be changeable, and it would be the best option for disabled individuals.

3.3.1.2 Brain Signal

Brain signal was investigated as another type of human characteristic. Brain signal is another biometric which is not visible, and the security pattern can be changeable and most importantly, it would be the best option for users with specific disabilities who could use their thoughts to identify themselves and manipulate other devices and software.

The average human brain contains about 86 billion nerve cells, called neurons. These are the building blocks of your brain. Neurons communicate with each other by sending

chemical and electrical signals. By capturing and investigating these signals we could understand the way the human brain functions and how we use it to manipulate other machines. It can be done using Brain-Computer Interface (BCI) technologies.

3.3.1.3 Brain-Computer Interface

According to the research and investigation, brain-computer interface (BCI) is a computer-based system that acquires brain signals, analyses them, and translates them into commands that are relayed to an output device to carry out a desired action.

In principle, any type of brain signal could be used to control a BCI system. A BCI system consists of 4 sequential components: (1) signal acquisition, (2) pre-processing, (3) feature extraction, and (4) classification. These 4 components are controlled by an operating protocol that defines the onset and timing of operation, the details of signal processing, the nature of the device commands, and the oversight of performance. The future of BCIs depends on progress in 3 critical areas: development of comfortable, convenient, and stable signal-acquisition hardware; BCI validation and dissemination; and proven BCI reliability and value for many different user populations.

To test the brain signal for authentication purposes we need to use a BCI system to acquire the EEG data, analyse it and try to achieve our goal by processing and classifying the extracted features which could be a brain-based biometric authentication method.

3.3.2 Brain-Based Biometric Authentication

It has been investigated that, basically brain-based authentication is the process of verifying an individual's identity by using their brain signal, and as an approach it offers several distinct advantages over other biometric authentication methods. Since at least the late 1980's [118] neuroscientists have observed that non-invasively measured human brain signals carry personally identifying information [119] [120] that differentiates between family members and across a broad population [121] [122]. Brain signals, unlike many other biomarkers are concealed: an invisible signal that is never exposed in daily life. Second, brain signals are dynamic, non-stationary and extremely complex. They are the result of a unique series of brain waves super positioning in a given brain at any moment, and these waves reflect both personal brain function and anatomy. Taken together, this makes brain signals an ideal candidate for use as a biometric [123] [124] [125] method. Indeed, many groups have attempted to build biometric authentication systems based on brain signals

[33,126,127]. Generally, the process involves a machine-learning classifier to identify if a given brain signal belongs to a genuine identity or to an imposter one. Many research studies were read and different methods have been investigated to find the strengths and the weaknesses in the process of authentication.

3.3.3 Literature

By finishing investigation on all previous sections, the literature of this project completed. In conclusion, biometrics are the best types of security authentication techniques. However, each biometric technique has some advantages and disadvantages. To cover the disadvantages of recent biometric techniques in terms of authentication and identification, we need a new biometric that doesn't have the disadvantages of the others. Brain signal is another human biometric that could be the best option in this case. By developing a specific BCI system we can use brain signal for authentication purposes. Many studies propose different methods and strategies in this area. Some of them achieved very high accuracy rate results for their proposed methods. However, there are still some limitations in their works in terms of security level, performance and permanency of their system through time. We need a system that improves performance, security and stability of the authentication process.

3.4 Phase 2: Signal Acquisition

As mentioned in the literature, acquiring the brain signal is the first step of any BCI system. A good signal acquisition strategy can make a BCI system perform more quickly and easily and more secure specifically for authentication systems. Therefore, according to the previous studies, to acquire the EEG data using mental imagery tasks are the best options for authentication purposes. The majority of the proposed systems by other researchers using mental imagery tasks are less practical and time consuming. Some of them use body movements or involved with some environmental situations.

3.4.1 User Signal Strategy

In this project, two signal acquisition strategies are proposed specifically for authentication purposes that are to cover the shortcomings of previous methods. These two strategies were proposed to complete the second objective of the project.

3.4.1.1 Strategy 1

The first strategy is a mental imagery task using a visualising or picturing pattern by memorising two types of pictures (2D and 3D) as a security ID which improves the security level of the system and the whole process of the authentication will be quicker and more practical.

3.4.1.2 Strategy 2

The second strategy is to improve the stability and permanency of the system through time using the deep breathing pattern. The deep breathing process has three parts of inhalation, breath-holding and exhalation, which in this case, the breath-holding part was picked as a security pattern. As mentioned in the literature, alpha waves are a better option for authentication purposes according to daily's brain situation. To stabilize the alpha wave that could make a permanent brain pattern for the BCI system we used the deep breathing task. Deep breath improves alpha waves and bring back the brain to its normal state.

3.4.2 Acquiring EEG From Participants

To acquiring the signals we will use a special subject strategy, a non-invasive BCI device (Emotiv EPOC +), a computer (Personal Laptop/University PC) and Emotiv SDK Pro software to record the signals and digitize them and make them ready for the other processes.

3.4.2.1 Non-invasive BCI Device

As mentioned in the literature, there are two types of BCI devices, invasive and non-invasive. Invasive devices need surgery to put the electrodes in the scalp, which is dangerous, but non-invasive devices are like a headset and do not need any surgery and it does not have any influence on the human's brain and body. For the project, we decided to use Emotiv EPOC + which is one of the best non-invasive BCI devices in the market at the time of doing this project. "EMOTIV EPOC+ 14 channel mobile EEG is designed for scalable and contextual human brain research and advanced brain-computer interface applications and provides access to professional grade brain data with a quick and easy to use design" [128]. The university prepared an EMOTIV EPOC+ for us and we started to do our project with this device. In the box of the device, there was equipment such as the Emotiv headset with its charger cable, hydrator pack including the electrodes, a hydrator fluid, a Bluetooth USB receiver to connect the device to the computer and an instruction sheet (Fig 3.2).



Figure 3.2: Emotiv EPOC + with its components that was used for data acquisition

3.4.2.2 Emotiv SDK Pro Software

To record and access high-quality raw EEG data we needed the Emotiv SDK Pro software with a PRO license or conduct research leveraging our detections for the project. This product is an online software, which the university prepared the licence for us to activate and use the software.

This software was installed on a MacBook Pro computer and the university computer system. The headset connects to the Emotiv Pro software on the computer via Bluetooth. The quality of the headset signal receiver has been checked by the software. As you can see in Figure 3.3 the green spots are good quality, orange spots are moderate, red spots are very poor quality.

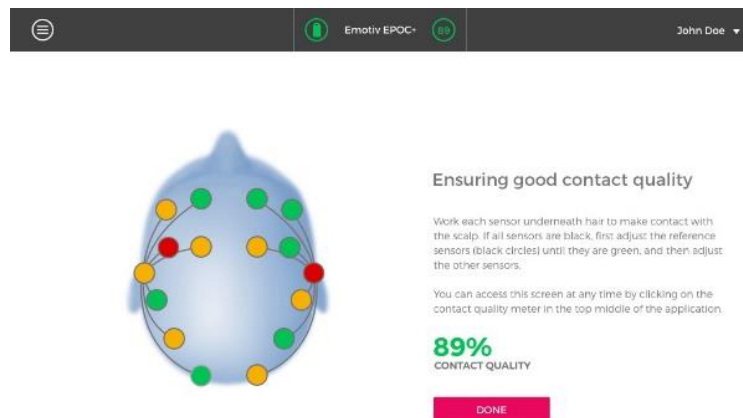


Figure 3.3: Emotiv Pro software interface for contact quality

In the main application display, EmotivPRO has some features (Fig 3.4) of which we used a couple for the project. These features are 1. Raw EEG: view a real-time or recorded data stream from the headset's 14 electric sensors. 2. Performance Metrics: view real-time or

recorded performance metrics for six cognitive states: Stress, Engagement, Interest, Excitement, Focus, and Relaxation. 3. Motion Sensors: view a real-time or recorded data stream from your headset's 9-axis motion sensors. 4. FFT/Band Power: perform a frequency analysis on single channel EEG data in real time or on recorded data. 5. Data packets: view a real-time or recorded data stream of packet loss and capture from your device to your PC. 6. Recordings: open or export previous recordings.



Figure 3.4: Emotiv Pro software interface

3.4.3 Recorded EEG Raw Signals

All EEG data were acquired and recorded on the computer system using the EMOTIV device. The process of the EEG acquisition for each one of the proposed methods was different in terms of the number of the participants, recording time, the environments, time of recording and time of repeating and re-acquiring the data for testing. The raw data was recorded in the system and digitised by the software and got ready for other phases of the project to process and analysis.

3.5 Phase 3: Pre-Processing (Enhancement)

In the process of recording the brain signals, many things could influence the recording and make noises in the recorded data. So the recorded EEG data needed to be checked, filtered and cleaned of any unwanted noises and artifacts. Signal pre-processing is one of the important steps in any BCI system. EEG signals are extremely weak and affected by different types of noises and impairments that need to be carefully eliminated.

The raw EEG data was processed using the EEGLAB and BCILAB Matlab toolboxes. The former is an interactive Matlab toolbox for processing continuous and event-related EEG while the latter is an EEGLAB plug-in for the design, prototyping, testing, experimentation, and evaluation of Brain-Computer Interfaces. EEGLAB incorporates independent component analysis, time/frequency analysis, artifact rejection, event-related statistics, and several useful modes of visualization of the averaged and single-trial data. It provides an interactive graphical user interface to process high-density EEG data. EEGLAB offers a wealth of methods for visualizing and modelling event-related brain dynamics, both at the level of individual EEGLAB data-sets or across a collection of data-sets brought together in a study set. Furthermore, EEGLAB offers a structured programming environment for storing, accessing, measuring, manipulating, and visualizing event-related EEG data.

3.5.1 Visual Inspection

Many types of the artifact and noises in the data are visible and easy to find with eyes in EEG data such as eye movements, muscle movements, high noises, linear trends, and discontinuity. In Figure 3.5, you can see the activity shapes of these types of artifacts.

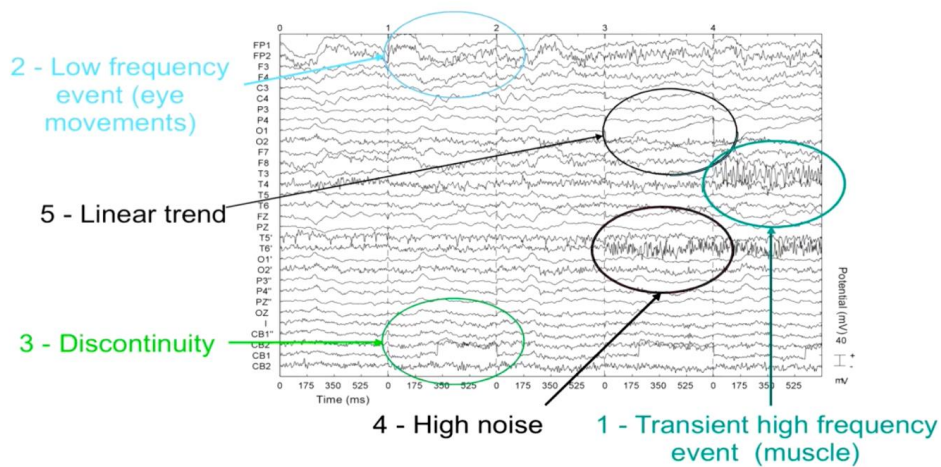


Figure 3.5: Different types of artifacts that are visible in EEG data [129]

3.5.2 Removing Artifacts and Bad Channels

Some of the artifact could happen continually and the reason for this type of artifacts is the problem with the recording electrodes for each channel. These channels which are called bad channels should have been removed from the data if there was any.

3.5.3 Signal Filtering

Filter settings can significantly improve the visibility of a defect signal. The amplitude of artifacts is often larger than the amplitude of the brain data, which potentially decreases the signal/noise ratio, bias data analysis, and potential results. There are different types of filtering methods; in this project the band-pass filtering method was used and following that, the ICA technique.

3.5.4 ICA Technique

“Independent component analysis (ICA) aims to solve the problem of signals separation from their linear mixture. ICA is a special case of blind source separation when separation is performed without the aid of information (or with very little information) about the source signals or the process of signal mixing” [130]. ICA is excellent for identifying and removing blink artifacts because they are large in amplitude, have a discrete source and are extremely reliable from blink to blink.

After the pre-processing step, the EEG data was ready to go to the next step to extract the specific features according to the purpose of any proposed methods.

3.6 Phase 4: Feature Extraction

Feature extraction is a process that identifies important features or attributes of the data. It deals with the problem of finding the most informative, distinctive, and reduced set of features, to improve the success of data storage and processing. In general, there are five of the well-known methods for frequency domain and time-frequency domain methods such as Fast Fourier Transform (FFT) Method, Wavelet Transform (WT) Method, Eigenvectors, Time-Frequency Distributions, Autoregressive Method [131]. The findings indicate that each method has specific advantages and disadvantages which make it appropriate for special types of signals. Considering this, the optimum feature extraction method was used for this project by applying FFT, PSD and DWT on the data.

3.6.1 Fast Fourier Transform (FFT)

This method applies mathematical means or tools to EEG data analysis. It transforms a signal from the time domain into the frequency domain. Basically, any time-dependent signal can be broken down into a collection of sinusoids. In this way, lengthy and noisy EEG recordings can be conveniently plotted in a frequency power-spectrum. By doing so, hidden features can become apparent. By adding all the sinusoids up after FFT, the original signal can be restored, so no information is lost.

3.6.2 Power Spectrum Density (PSD)

Characteristics of the acquired EEG signal to be analysed are computed by power spectral density (PSD) estimation in order to selectively represent the EEG samples signal. FFT is commonly used in EEG to estimate Power Spectral Density (PSD). PSD refers to the spectral energy distribution that would be found per unit frequency. It can be computed by applying FFT directly on the signal or also by transforming the estimated autocorrelation sequence.

3.6.3 Log-Bandpower

Log-Bandpower, was chosen as the desired paradigm after a number of trials to determine best candidates based on the ability to discern differences between AUTH and NOTAUTH marked epochs. In the case of the learning algorithms, SVM and LDA were chosen based on preliminary outcomes with a subset of the data. The logarithmic bandpower (Log-Bandpower) estimates paradigm is based on the design of the original Graz Brain-Computer Interface [132], which used lateralized motor imagery for control. The features exploited by this paradigm in its original form are Event-Related Synchronization and Desynchronization [133] localized in the motor cortex, but the paradigm is not restricted to these applications. Similar measures have also been used in other studies, although without machine learning [134]. Generally, Log-Bandpower can be used as a simple method to operate on oscillatory processes, either in relation to events, or asynchronously. The paradigm is implemented as a standard sequence of signal pre-processing spatial spectral filtering, feature extraction, and machine learning. The defining property of the paradigm is that it extracts, per trial, the per-channel log-variance $\log(\text{var}(X))$ as features of the signal. The resulting feature vectors are then passed along to the learner component. By default, the paradigm uses a non-adaptive spatial filter, the surface Laplacian, and a non-adaptive spectral filter.

3.6.4 Discrete Wavelet Transforms (DWT)

Wavelet transforms are widely used in many engineering fields for solving many real-life problems. A wavelet is a short wave, which has its energy intensified in time to give a tool for the analysis of transient, non-stationary signals or time-varying phenomena [135]. If a signal does not change much over time, we would call it a stationary signal. Fourier transform could be applied to the stationary signals easily and a good result can be taken. However, many signals like EEG have the nonstationary and transient characteristics, in such situations ideally Fourier transform may not be applied directly. But the time frequency methods can be used [136] [137]. We used the Wavelet transform method to extract the

individual EEG sub-bands and reconstruct the information accurately because the wavelet transform has the advantages of time-frequency localization, multi-rate filtering, and scale-space analysis. DWT can expose more details from the signal in both time and frequency domain precisely. This makes it become a robust tool in biomedical engineering, particularly in epileptic seizure detection. In this paper, DWT is utilized to analyse the EEG signals into various frequency bands. The DWT decomposes a specific signal into approximation and detail coefficients at the first level. Then the approximation coefficients are additionally decomposed into next level of approximation and detail coefficients [138].

3.6.5 *Extracted Features*

All the specific features according to the purpose of each proposed method were extracted from the data using FFT, PSD, Log-Bandpower paradigm and DWT techniques. These algorithms were developed in each method in a particular way according to the features needed for each method separately. The feature vectors got ready for the next step which is classification.

3.7 *Phase 5: Classification*

The classification of electroencephalogram (EEG) signals is very important in brain-computer interface (BCI) systems, aiming to achieve intelligent classification of EEG types with high accuracy. There are three methods of learning: supervised, unsupervised, and reinforcement learning. The simplest of these learning paradigms is supervised learning, which is very popular to be used for EEG signal classifications.

Multiple classification algorithms have been used in different studies. In this project, LDA, SVM and NN classifiers are applied on the data to train and test both proposed authentication BCI systems. The software captured biometric traits from the following 14 EEG channels based on the International 10-20 locations: AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, and AF4. These channels are inherently available in the Emotiv headset and cover fundamental locations of each area of the brain. The physiological biometric model followed the standard model presented by Wayman [139]. All the raw data is acquired, then manipulated and sent to a feature extractor. The extracted information is then sent to a classifier where it is decided if the users are who they claim to be.

3.7.1 Linear Discriminant Analysis (LDA)

Linear Discriminant Analysis (LDA) is a well-known method in this research area, which is used for dimensionality reduction problems as a classification algorithm. “The purpose of the LDA classification is to assign observations to the corresponding class based on a set of measurements or predictors by finding an optimal linear transformation that maximizes the class separability” [140]. The discriminant function is the rule of classification in this classifier, and it acts as a linear classification function, which is only in the two-group class (Fig 3.6).

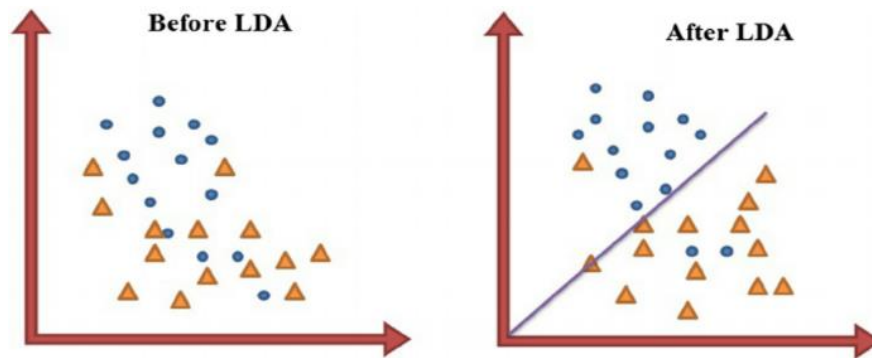


Figure 3.6. EEG features before and after using the LDA classifier

3.7.2 Support Vector Machine (SVM)

SVM is a strong binary classifier, with a large volume of simplification. It is one of the most popular supervised learning algorithms for explaining classification problems, which is based on a linear model [141]. A discriminative classifier is defined by a separating hyperplane. In other words, “given labelled training data (supervised learning), the algorithm outputs an optimal hyperplane which categorizes new examples” [142].

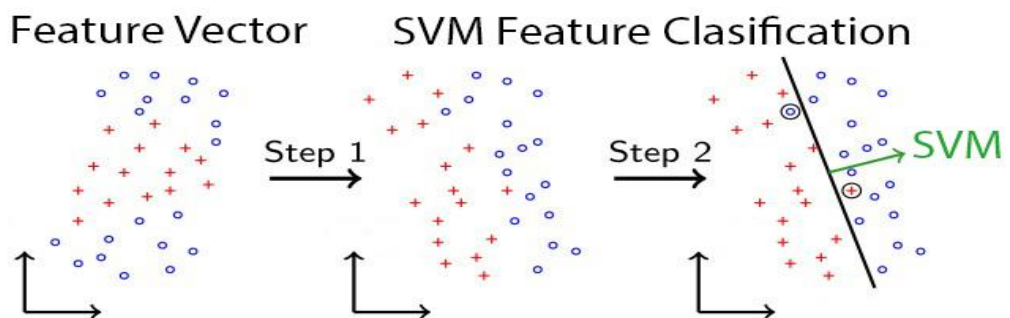


Figure 3.7. SVM classification process visualisation

3.7.3 ANN Classifier

The classification network selects the category based on which output response has the highest output value. Classification neural networks become very powerful when used in a hybrid system with the many types of predictive neural networks. There are three important types of neural networks that form the basis for the classification process: Artificial Neural Networks (ANN), Convolution Neural Networks (CNN), and Recurrent Neural Networks (RNN). In this project, ANN are used for the classification part of the second proposed method. Once the EEG signals were recorded from participants, EEGLAB, BCILAB, Matlab Classification Learner, Wavelet Analysis Toolbox and Neural Network Toolbox were used to process the signals in order to filter, extract features, and develop a classification model. This was all performed to establish what level of accuracy the proposed methods will provide. This was measured by utilizing FAR and FRR as follows:

$$FRR = \frac{\text{False Rejections}}{\text{Unauthorized Attempts}} \times 100\% \quad (3.1)$$

$$FAR = \frac{\text{False Acceptances}}{\text{Unauthorized Attempts}} \times 100\% \quad (3.2)$$

An additional key metric is EER, which is the value where FRR and FAR are equal. The actual processing steps included: load data, specify computational approach, specify parameters, learn a model, visualize a model, and apply the model to a new data set. The recorded EEG file contained corresponding markers (i.e., AUTH and NOTAUTH) reprise. BCILAB used the second data set to evaluate discrepancies and calculate loss measure. As an additional capability, EEGLAB was independently used to pre-process the raw EEG data, including verifying and placing AUTH and NOTAUTH markers, resampling, and appending or deleting content, among other tasks. This enabled the cost-effective validation and enhancement of EEG signals obtained from participants.

3.8 Phase 6: Results & Evaluation

The last phase of the methodology of this project presents all the results from both proposed methods. According to the differences between the algorithms and strategies that were used for each method, there are two sections that include the results, evaluation and conclusion for each method separately. After all, both results are evaluated and compared to other studies and following that is the conclusion, limitations and future works for the whole project.

3.9 Conclusion

This chapter presents proposing two new methods using different user strategies to record the data for signal acquisition phase. The Emotiv EPOC+ brain device and its functions to record human brain signals was explained. Different pre-processing, feature extraction and classification algorithms, techniques and the tools that were used to improve the process of BCI authentication process were all explained. The first proposed method is to improve the security and usability of the process and the second proposed method is to improve stability and permanency of the brain's security pattern. In general, this chapter presents the methodology that we have chosen to achieve all the objectives in this project. In the next chapter, the execution of each method will be presented to achieve the appropriate results.

Chapter 4

Methods

4.1 Introduction

This project proposes two methods to improve the shortcomings in brain-based authentication methods as mentioned in the previous chapters. The first one is an improved brain-based biometric authentication in terms of performance, usability and security level of the process.

The second method is system that improves the permanency and stability of the brain-based security pattern through time. Each method presents a new user strategy for signal acquisition and uses enhanced techniques and algorithms for signal processing, feature extraction and classification of the BCI system. This chapter covers the third, fourth and fifth objectives of this thesis.

4.2 SaS-BCI Method

SaS is for the Signal Acquisition Strategy, which is for a user to register the unique brain pattern on a system for the process of authentication. According to the literature, some research studies achieved results with high accuracy rates for their proposed methods by applying different signal acquisition techniques, feature extraction, and classifications using BCI. One of the important parts of any BCI processes is the way that brainwaves could be acquired and recorded. A new algorithm is presented in this method to acquire the brain signals for the process of authorisation and authentication.

This is to predict image memorability from the user's brain to use mental imagery as a picturing pattern for security authentication. Therefore, users can authenticate themselves by visualising a specific picture in their minds. In conclusion, we can see that brainwaves can be different according to the mental tasks, which it would make it harder using them for authentication process. There are many signal acquisition and signal processing strategies for brain-based authentication that, by using the right techniques, could achieve a higher level of accuracy which is suitable for using brain signal as a biometric security authentication method.

4.2.1 SaS-BCI Stages

SaS-BCI is divided into 4 stages as presented in algorithm 4.1.

Algorithm 4.1: SaS-BCI algorithm

```

Stage 1: Users look at a specific picture and memorise it in their mind
Stage 2: Users Picturise that specific image in their mind
    User Str = Looking at a Specific Picture + Memorising
Stage 3: The brain signal will be recorded in a database as a brain ID.

    Brain ID = User's Unique Pattern Made by Picturing the Specific Image
Stage 4: Users can authorise themselves by picturing the same image in their minds.

    Authentication Method = Receive the Brain ID + Comparing to the Recorded ID in Database
Register the User
    Get User Code
    Get User (Brain ID == Picturized Image Pattern)
Register Successful

System Login
    Login ID == (Get User Code + Get User Brain ID)
If (Login ID == User Code && User Brain ID) Then
    Login Successful
Else
    Login Failed
End If
    
```

The proposed method is divided into three stages. The first stage is to record EEG signals obtained from human participants (Brain ID). In the next stage, these signals will be pre-processed using the data filtering methods for noise removal. The last stage will be classifying the data and testing the user ID to achieve the accuracy of the method for the authentication process (Fig 4.1).

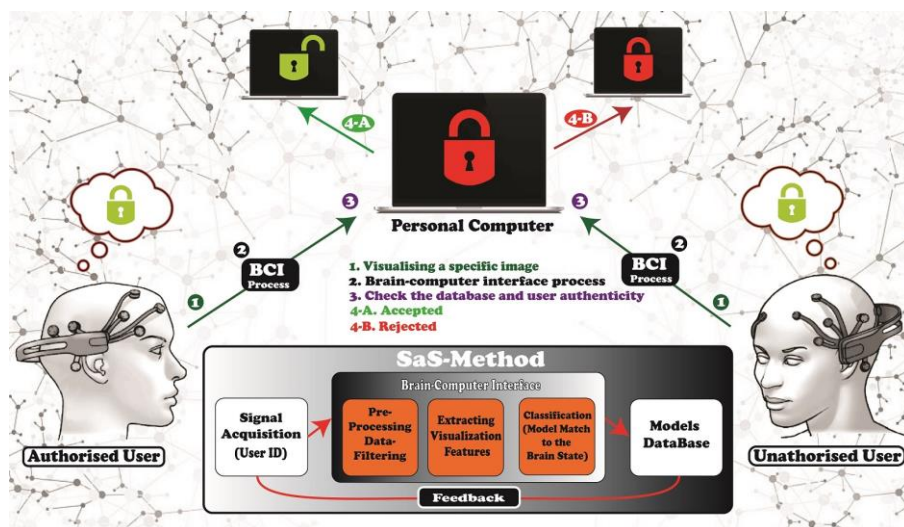


Figure 4.1. New Signal Acquisition Strategy using Brain-Computer Interface

In this method, the acquired data are divided into three portions: training data, cross-validation data and testing. The training data is utilized to ensure the machine perceives image paradigms in the data, and the cross-validation data is utilized to guarantee the effectiveness of the algorithm used and a better accuracy for the trained model. At the end, the test data is utilized to perceive how well the images can be predicted based on its training.

To acquire the EEG data for the purpose of this method, twenty healthy individuals between 25-45 years old participated. This was done by advertising the experiment and asking for participants in the university. As mentioned in the first chapter, the whole ethical protocol to do this experiment were considered and all official works and participation forms signed and received from everyone. This experiment was done in different time periods according to the availability of each participant. All data acquiring was done in the same place with a quiet environment and the same situation for everyone in two different session-days. It took about an hour for each participant to record the EEG data. It included using the brain device and fixing it on their scalps to acquire the strongest signals according to the device's software.

In the first part of the experiment of the first session-day, the participants were asked to sit in front of a white wall and look at it. The EEG data was recorded for 1 minute. Following that, they were asked to look at 10 geometric 2D (Fig 4.2) single colour pictures printed on a paper and attached to the wall separately. The EEG data recorded for 30 seconds per picture. It starts with 2 seconds closed eyes, 5 seconds looking at the picture, and repeating the same process for 5 times. The second part of the experiment was the same process as the first part but looking at 10 colourful 3D geometrics in real life pictures. These two types of pictures were selected according to the memorability of the human mind for different types of pictures. The first group are easy to memorise, and the second group are harder to memorise.

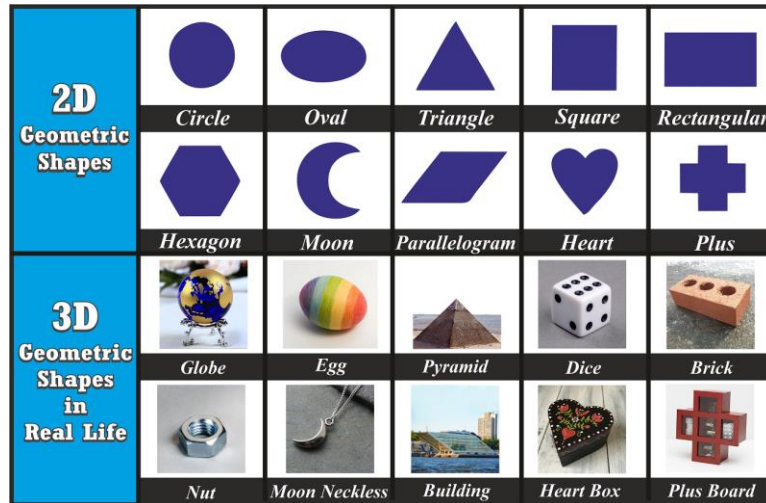


Figure 4.2. The 20 different 2D and 3D images that was used in the experiment

In the final part of the experiment for the first session, participants were asked to picturize each specific image in their minds while looking at the plain white wall. The EEG data recorded for 30 seconds per image in a way that the participants should have picturized the required picture in their mind. This part of the experiment is the prediction of images by picturising them in the mind and counts as the user-ID for the main part in training the system. The second session-day of the experiment was in the same environment and the same situation. The participants were asked to look at the plain white wall and try to picturise the 2D and 3D pictures that they memorised in the first session. They should have picturized and recalled the pictures they were asked to do separately. The EEG data were recorded from each participant from both session-days and saved in the computer system for the next stage of the method for processing.

A data set was provided that contains historical data from which to learn patterns. It needs the outcomes to determine the features that best predict the outcomes. However, the main purpose of this method is testing the picturising paradigm and predicting the pictures by recalling them which can be used as a user-ID biometric authentication.

Measurements were taken by the Emotiv EPOC+ device from the 14 channels that were placed on the participant's scalp. You can see three different positions in two sessions have been exerted as a user strategy for signal acquisition part of the project (Fig 4.3).

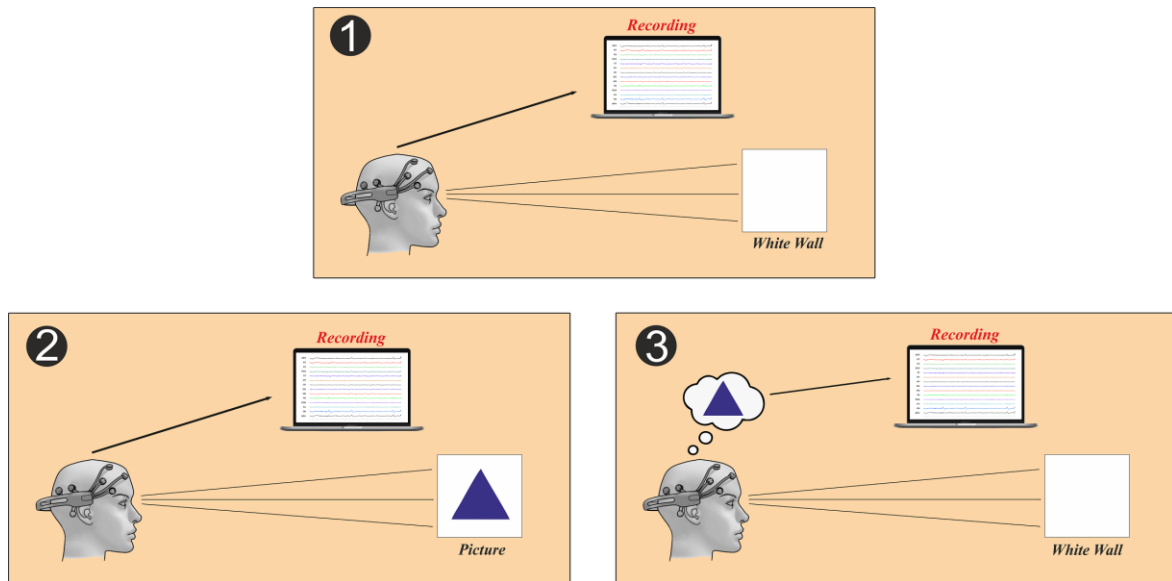


Figure 4.3. The user-strategies and signal acquisition from the participants in two sessions

All the raw EEG data were collected from the participants and saved on the computer by the Emotiv software as EDF files. As you can see in Figure 4.4, the raw data were recorded onto the computer via the Emotiv Pro software. The software allows the user to play the recorded signals, comment on them and save them in two different file types such as EDF and CSV. The EEG data were saved in the computer to start the next part of the project methodology, which is pre-processing.

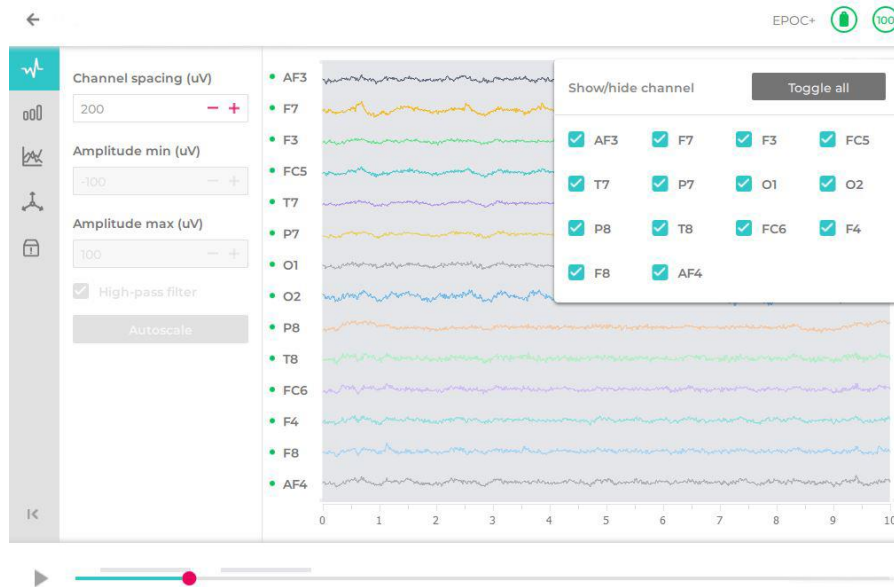


Figure 4.4. A screenshot from the EMOTIV Software while recording the data with 14 channels

4.2.2 Pre-Processing (Enhancement)

The pre-processing section was done for data enhancement and noise removal. The raw EEG data needed to be processed to get closer to the true neural signals and obtain specific features which can be used to train the model. Matlab software was used including EEGLAB and BCILAB toolboxes to process the data. These toolboxes are for the prototyping, designing, experimentation, testing, and evaluation of BCI systems.

4.2.2.1 Visual inspection

At first, the EEG data were imported on EEGLab. Before starting any process, the brainwaves data were visualized to check the differences and the shape of the waves to find out the specific parts and the obvious differences according to the recording time frames. First, we needed to locate the channels used in the EEGLab tool according to the signal acquisition method and the Emotiv device that we used for capturing the raw data.

To do this, the necessary information of each channel was acquired from the Emotiv website that could be added to EEGLab tool to determine the location of all 14 channels on the scalp accurately. Figure 4.5 shows a created CED file that includes all information for each channel to locate them accurately (Figure 4.6) to visualize the brain activities correctly.

Number	labels	theta	radius	X	Y	Z	sph_theta	sph_phi	sph_radius	type
1	AF3	-23	0.411	0.885	0.376	0.276	23	16	1	1
2	F7	-54	0.511	0.587	0.809	-0.0349	54	-2	1	2
3	F3	-39	0.333	0.673	0.545	0.5	39	30	1	3
4	FC5	-69	0.394	0.339	0.883	0.326	69	19	1	4
5	T7	-90	0.511	6.12e-017	0.999	-0.0349	90	-2	1	5
6	P7	-126	0.511	-0.587	0.809	-0.0349	126	-2	1	6
7	O1	-162	0.511	-0.95	0.309	-0.0349	162	-2	1	7
8	O2	162	0.511	-0.95	-0.309	-0.0349	-162	-2	1	8
9	P8	126	0.511	-0.587	-0.809	-0.0349	-126	-2	1	9
10	T8	90	0.511	6.12e-017	0.999	-0.0349	-90	-2	1	10
11	FC6	69	0.394	0.339	-0.883	0.326	-69	19	1	11
12	F4	39	0.333	0.673	-0.545	0.5	-39	30	1	12
13	F8	54	0.511	0.587	-0.809	-0.0349	-54	-2	1	13
14	AF4	23	0.411	0.885	-0.376	0.276	-23	16	1	14

Figure 4.5. Emotiv EPOC channel location details.

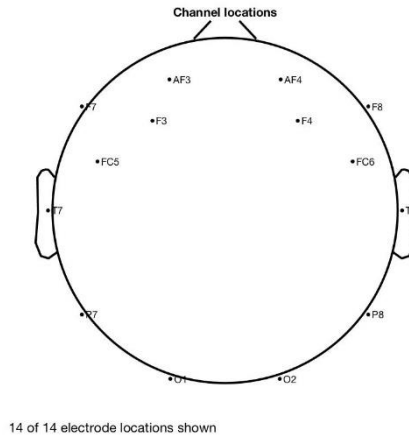


Figure 4.6. Channel locations on the scalp by name and by number

It allowed us to scroll the data received by each channel separately. The channel scrolling helped us to check the activities of signals from the channels and we were able to see the significant signal movement and possible noises in each channel that needed to be removed. In Figure 4.7, you can see the list of all 14 channels in the left side, the signals that were recorded by each channel and the time for recording each signal, which in this figure is per second.

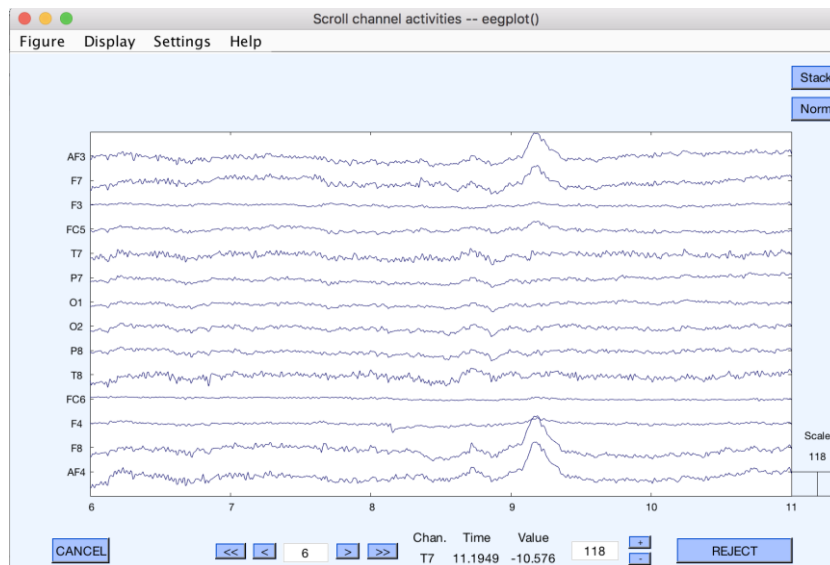


Figure 4.7.A visualisation of each channels including the signals that recorded by them

After checking each channel’s activity, the spectra plotting, and mapping were done to have a clear view of brain activities through the experiment. Figure 4.8 is an example of spectra plotting on EEG data. Each coloured bit signifies the spectrum of the activity of one data

channel. For example, the leftmost scalp map shows the scalp distribution of power at 6 Hz. The other scalp maps indicate the distribution of power at 10, 16, 22 and 60 Hz. Plotting channel spectra and mapping computed the specific time windows in the data. Each channel has a coloured line, which shows their signal characteristics. The characteristics and the distances between each line show that this data needs to be filtered and reject artifacts to be analysed in the further works.

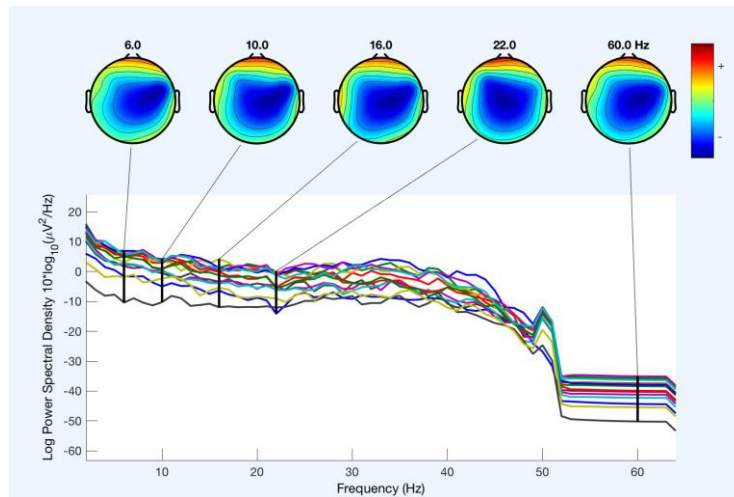


Figure 4.8. Plotting channel power spectral density of the recorded EEG

4.2.2.2 *Removing Artifacts and Bad Channels*

Having a few sensors that are recording values is common during data capturing, which will not be used for data examination. In EEG, sometimes to record anything interesting, the quality of the connection between the electrode and the scalp is too low. It is important to identify the sensors with weak signal quality because the artifact removal will be more efficient. This process started with examining the data visually to reject the abnormal activities of signals. This was done very carefully to not delete the useful information needed for the purpose of the method. Some artifact's frequency rates are very high and abnormal that would not have any specific brain data that could be useful. These types of data were detected visually and removed from the data. In many cases it is better to reject these data manually according to the specific time frame of the recorded data during the experiment. For example, the researcher knows which time in the data includes the important information so they can reject any artifact outside of that timeframe. Regarding to this matter, it might be better to remove artifacts from the data manually by visualising it. Stretches of continuous data were marked for rejection by dragging the left mouse button on them. Figure 4.9 shows

an example of the recorded signal from each channel in the time of the recording per second. You can see that a part of the data selected by the green colour shows some abnormal activities, which are some artifacts and noises that could be rejected by selecting them and taking them off from the data.

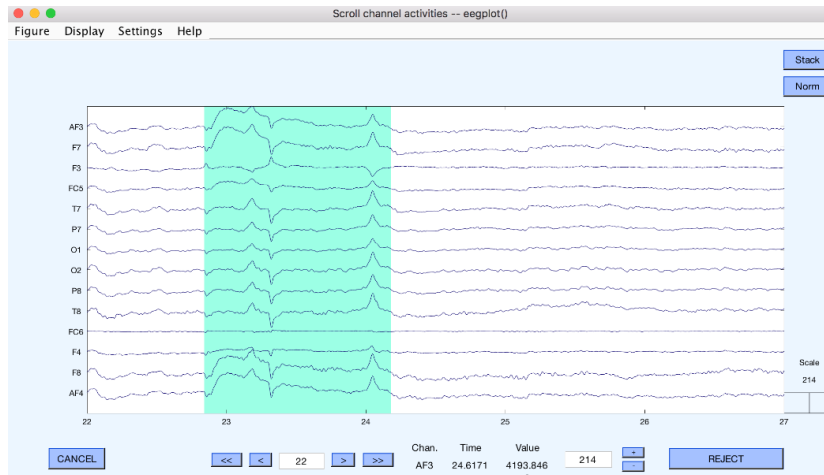


Figure 4.9. Continues data rejection by eyes in EEGLab

Sometimes, the recorded data show that some channels did not record the signals properly which doesn't have any useful data and should be removed. These bad channels were detected by scrolling the data and seeing the characteristics of the recorded signals. Figure 4.10 shows an example of two bad channels in a data set. As you can see channel AF3 recorded a continuous same shape signal noise and channel F7 did not record any data at all.

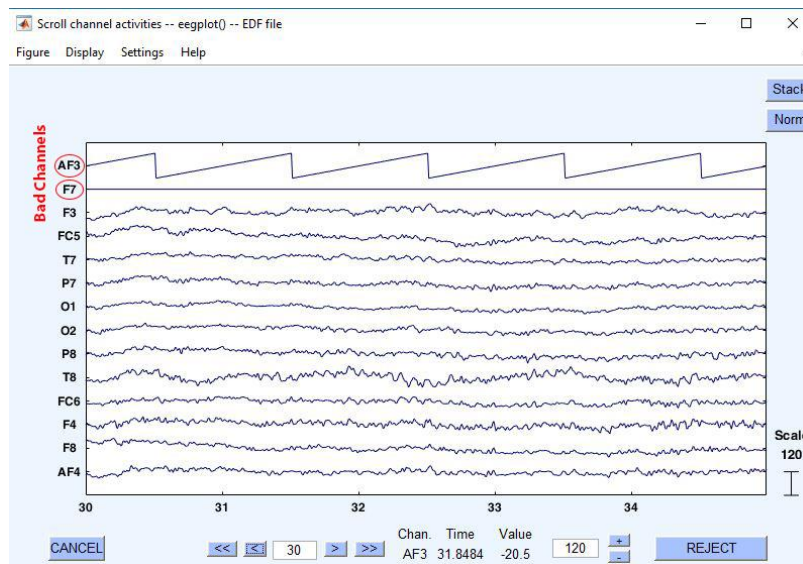


Figure 4.10. An example of two bad channels in a part of the recorded data

Figure 4.11 shows the components of two different channels (Channel 3, Channel 13) in another data set which, in this case, channel 3 identified as a bad channel. You can see three areas that show the differences between a bad channel and good channel. Area number 1 shows the activity power spectrum of each channel which in channel 3 is a smooth line, and it means that it is not a good data. Area number 2 shows the range of continuous data, for which there is no data in channel 3 and nothing is visible but the green background. It means there is about zero range activities, but on channel 13, you can see some information recorded with different colours that are for the range of the continuous data. Area number 3 shows the range amount of the continuous data in which you can see that the range for channel 13 is normal (-38.6 Mv to 38.6 Mv) but channel 3 shows a large number (-3722 Mv to 3722 Mv) that means it is out of range. According to the information above, channel 3 counted as a bad channel and was removed.

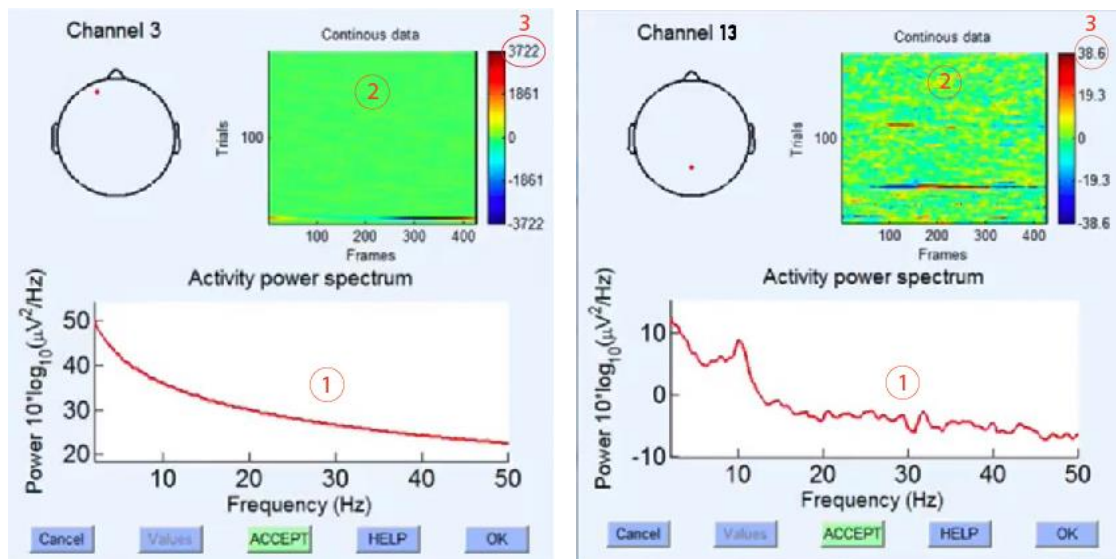


Figure 4.11: Comparison of a bad channel and a good channel

4.2.2.3 Signal filtering

Filtering the continuous EEG data reduces the outline of filtering artifacts at epoch boundaries. A high-pass filter is often necessary to remove linear trends of the data. The reason for using the high-pass filter is removing slow and possibly large amplitude drifts in the signals. In this case, a basic Finite Impulse Response (FIR) filtering technique was used for high-pass filtering. FIR was used to implement almost any sort of frequency response digitally, which is usually implemented by using a series of delays, multipliers, and calculations to create the filter's output. For the lower edge of the frequency passband and

the higher edge of the frequency, 0.5 Hz and 50 Hz was exerted respectively. The amount of 0.5 Hz for lower edge bandpass means everything below that frequency will be removed which is needed for Independent Component Analysis (ICA) that will be exerted in the next step. This analysis algorithm is very sensitive to the lower shifts frequencies. Figures 4.12 and 4.13, show the filter response after applying FIR filtering method on the data recorded by one of the channels in a data set. You can see that it filtered everything lower than 0.5 Hz passband and everything above 50 Hz passband and it removed sharp line noises. This filtering method is doing both the forward and backward phase shift on the signals. As you can see in Figure 4.12 the original signal includes a noise higher than 50Hz which by using the band-pass filter, the noise got removed from the data as shown in figure 4.13.

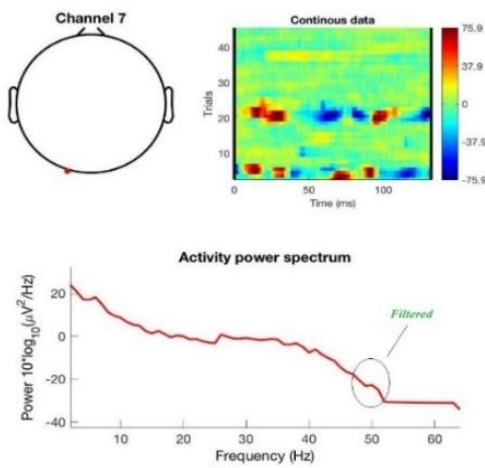


Figure 4.13: The Filtered data with High-Pass filter technique

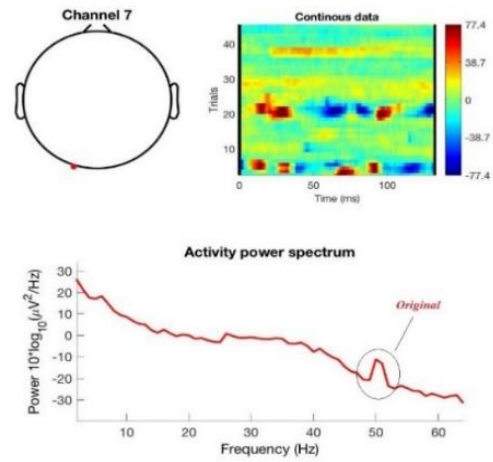


Figure 4.12: The original power spectrum in frequency

4.2.2.4 Independent Component Analysis (ICA)

ICA is excellent for identifying and removing blink artifacts because they are large in amplitude, have a discrete source and are extremely reliable from blink to blink. Blinking is a very common muscle movements which are happening mostly unintentionally by humans. Therefore, it is important to remove the artifacts created in any brain data by blinking which does not include and useful information for the purpose of this study. After filtering the data and removing the artifacts and bad channels for each data set, the ICA technique is applied on each data set. ICA extracted the components in each data set and got ready to plot the component map of the scalp. Figure 4.14 shows the component map of a participant's recorded data set in two dimensions for all 14 channels from IC1 to IC14. The red area on the scalp shows higher frequencies that could be artifacts or a specific brain activity. The

yellow parts are showing brain activities in a lower frequency rate and green is without any specific activities while blue colour shows the frequencies with lower power spectrum range.

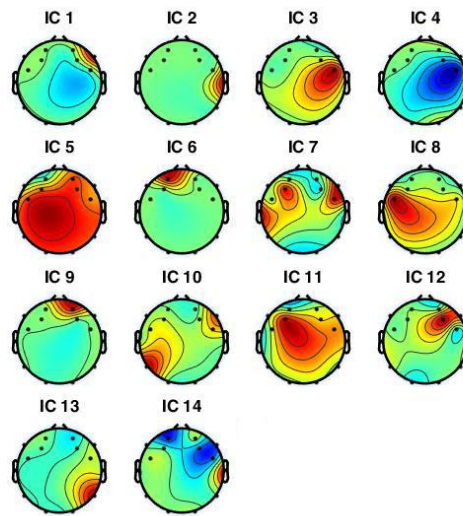


Figure 4.14. ICA component plots for all 14 channels in a dataset

Each component was plotted separately to see the component properties and check 1-scalp topography of the components, 2-spectrum of the components and 3- Event-Related Potential (ERP) images. Figure 4.15 shows the component plot for channel 3 of the data set

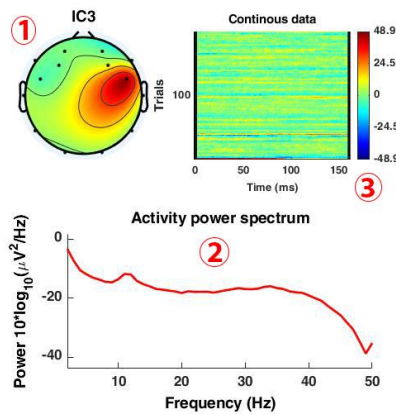


Figure 4.15. ICA components properties plot for channel 3 of a dataset

The decomposition of the components was checked by inspecting and labelling components by maps. There are different components that can be detected by ICA. Components such as eye, muscle, heart (cardiac), bad channels and brain. The ICA algorithm detected different types of components in each data set which allowed us to visualize and reject them from the data. Although the majority of the big artifacts were removed by visualizing and filtering techniques in previous sections, ICA found the unnecessary components in the data which

weren't rejected by previous sections. Figure 4.16 shows an example of the components detected by ICA on the data set.

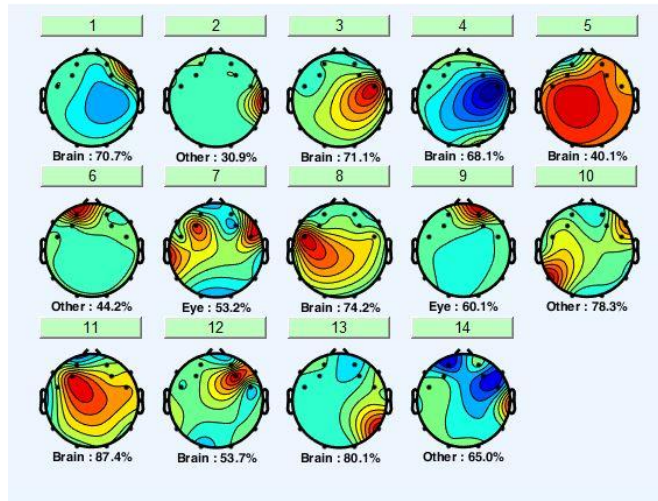
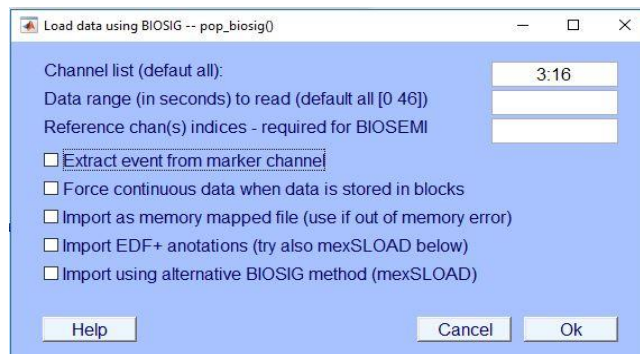


Figure 4.16. Series of components that detected by ICA algorithm which can be rejected after investigation

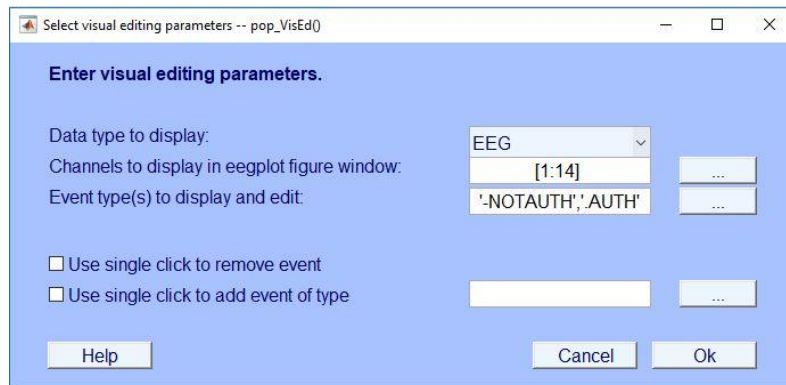
The ICA technique was applied on all data sets to remove artifacts and noises as the last part of EEG data pre-processing. The processed data sets were listed and separated according to each participant and each task that was done in the experiment. The data was prepared to extract the features according to the purpose of the first method in this research.

4.2.2.5 Biometric Data Pre-processing

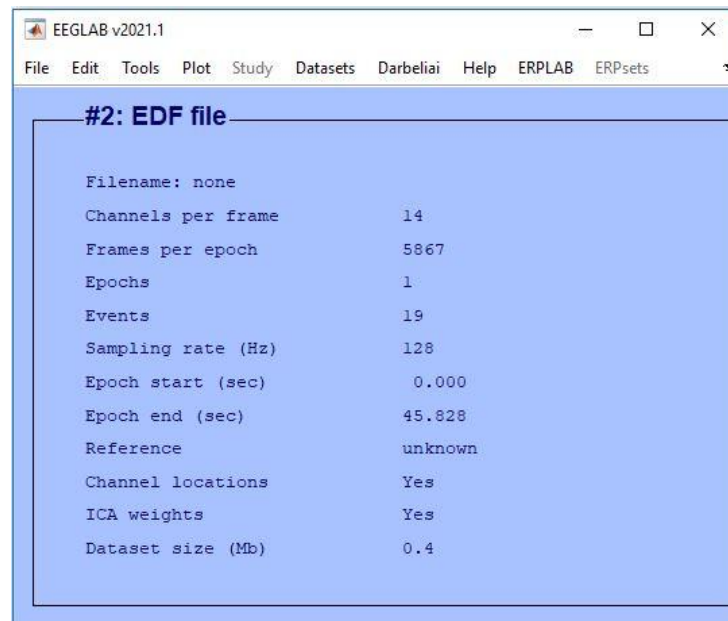
The raw EEG was processed to properly add event markers AUTH and NOTAUTH. AUTH marks an epoch aligning with picturising a specific image (2D/3D) while NOTAUTH aligns with epochs containing closed eyes. Figure 4.17(a) shows the parameters used to perform the initial EEG data loading. Due to Emotiv Research SDK EDF file format, a subset of channels between 3 and 16 was used to capture the 14 available channels. The data range in seconds was kept as the default. After inserting the appropriate markers, as shown in Figure 4.17(b), the full description of the EEG dataset is updated (Figure 4.17(c)).



(a)



(b)



(c)

Figure 4.17. Applying EEGdata on EEGLAB

Finally, after removing the DC offset from the signal, the data scroll view reveals the pre-processed EEG signal ready for feature extraction (Figure 4.18). The resulting processed EEG signal was then saved as a new data set for the next phase, feature extraction and classification.

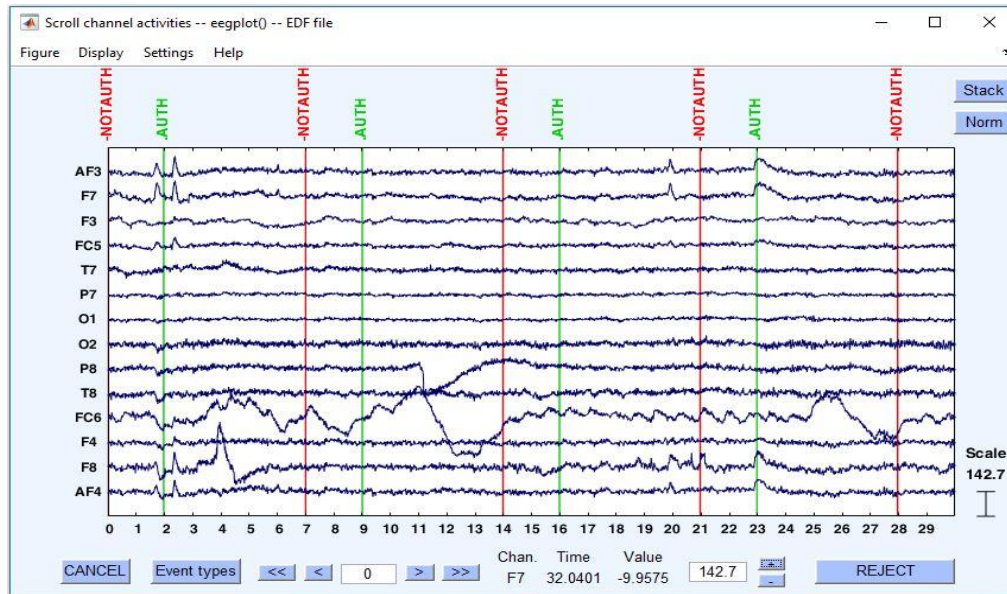


Figure 4.18. The respective markers on the EEG data

4.2.3 Feature extraction

All recorded EEG data were pre-processed and stored as separate data sets and coded for all participants. Each data set was analysed particularly to extract the best possible features. Power Spectral Density (PSD) technique was used to extract feature arrays from the EEG signals. This was done to surge the effectiveness due to a larger number of data points and potential connections between channels across the whole brain. Therefore, it is a significant process in interpreting an input signal to use it as an authentication key.

PSD displays that different mental tasks have different frequency ranges with different powers. It defines the power distribution of a signal over frequency. To calculate the PSD first we needed to convert the time domain to frequency domain by using Fast Fourier Transform (FFT) technique. This process was done in MATLAB software using EEGLab Plugin. The frequency rate for the power spectrum bands was determined according to the types of human brainwaves (Delta, Theta, Alpha, Beta, and Gamma) in their specified frequency rates as Figure 4.19. The pre-processed EEG signals are framed into 1s frame duration with 50% overlap to ensure a smooth trajectory of the features which has proven to be surprisingly effective [143].

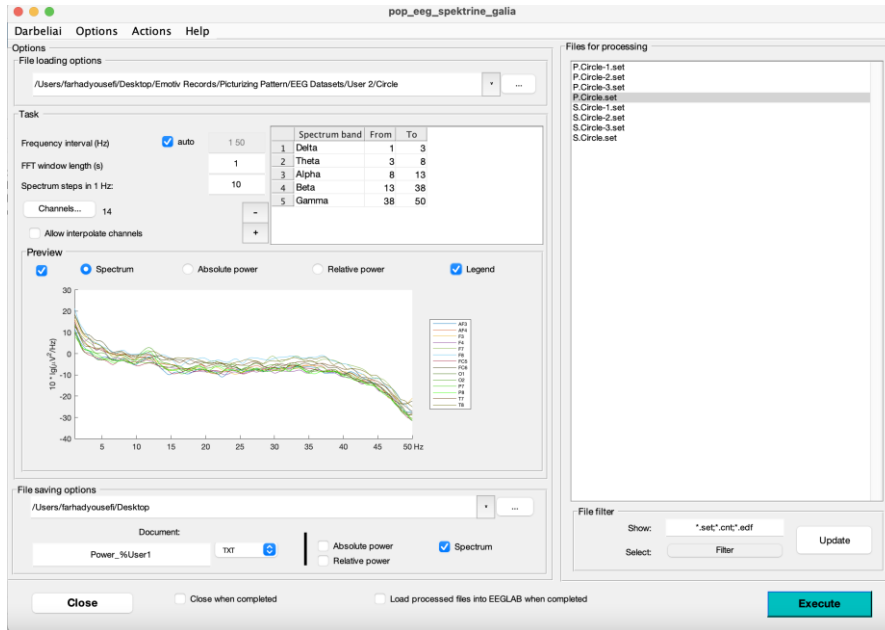


Figure 4.19. A screenshot of the Darbeliai Tool on EEGLab in Matlab software to determine the brainwaves in terms of the frequency rates.

The frequency interval selected was from 4-1 to 50 (Hz) and the FFT method was applied on the data with the length of 1 window and 10 spectrum steps per 1 Hz. This was done to compute spectrum, absolute power and relative power of the signals. If a signal $x(t)$ has Fourier Transform $X(f)$, its power spectral density is $|X(f)|^2 = S_x(f)$. Equation (4.1) shows the absolute spectral power in the band of frequencies from f_0 Hz to f_1 Hz is the total power in that band of frequencies, that is, the total power delivered at the output of an ideal (unit gain) band-pass filter that passes all frequencies from f_0 Hz to f_1 Hz and stops everything else.

$$\text{Absolute Spectral Power in Band} = \int_{-f_1}^{-f_0} S_x(f)df + \int_{-f_0}^{-f_1} S_x(f)df. \quad (4.1)$$

Equation (4.2) is the relative spectral power that measures the ratio of the total power in the band (i.e., absolute spectral power) to the total power in the signal.

$$\text{Relative Spectral Power in Band} = \frac{\int_{-f_1}^{-f_0} S_x(f)df + \int_{-f_0}^{-f_1} S_x(f)df}{\int_{-\infty}^{\infty} S_x(f)df} \quad (4.2)$$

Power spectrum (Fig 4.20) shows in a figure the variation of power across all frequencies, while electrical power shows the power of given measure of EEG like absolute power [Fig 4.21], relative power (Fig 4.22) in a given frequency band, like alpha.

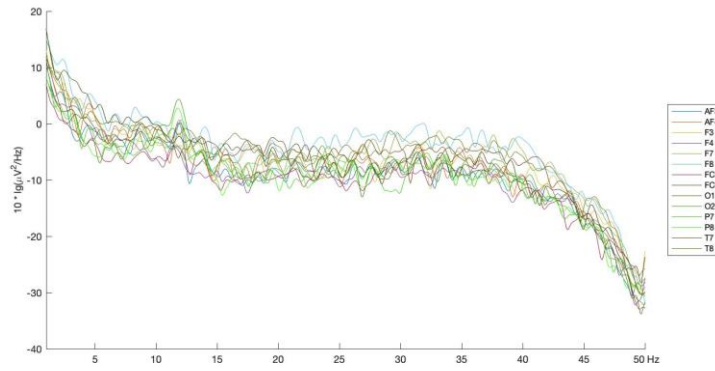


Figure 4.20. Power Spectrum image in an EEG dataset

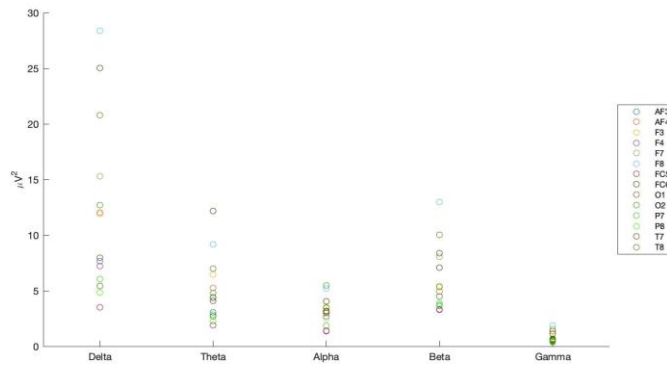


Figure 4.21. Absolute Power image from an EEG dataset

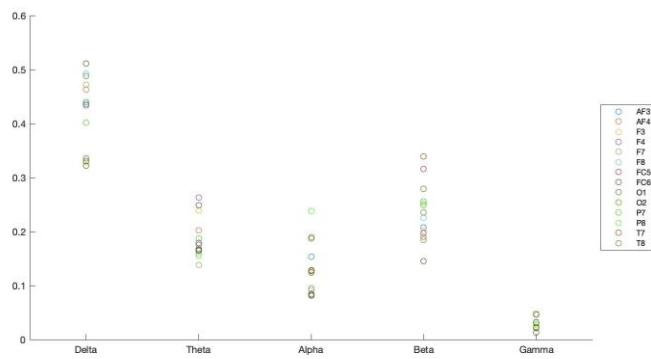


Figure 4.22. Relative Power image from an EEG dataset

PSD function showed the strength of the variations (energy) as a function of frequency. In other words, it showed at which frequencies variations are strong and at which frequencies

variations are weak. The unit of PSD is energy per frequency (width) and energy can be obtained within a specific frequency range by integrating PSD within that frequency range. PSD obtained over squaring of the total value of Fourier-transformed data per segment. Based on that, the non-dominant region of the power spectrum [144] and the concavity of spectral distribution [145] variance of spectral power (Fig 4.23) were considered as EEG features for recognition purposes.

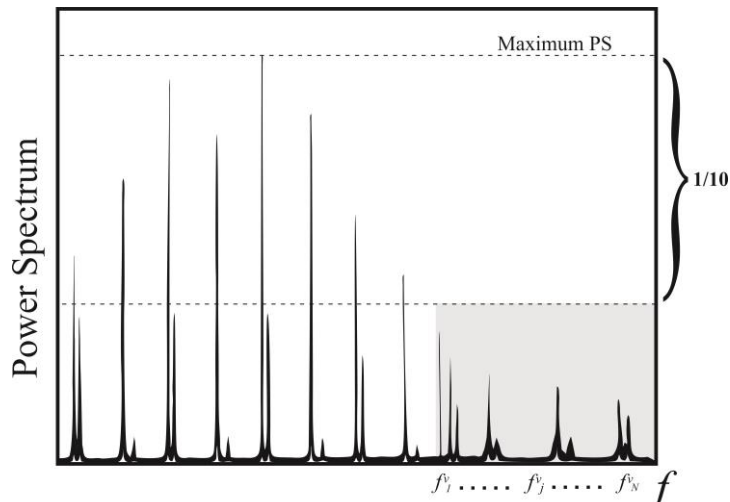


Figure 4.23. The illustration of the Concavity of spectral definition

After spotting the maximum level of the power spectrum, its tenth part was calculated and implemented as a measure. The frequencies values of power spectral that were under the calculated measure squared and then summed (4.3) where, $f_j^u (j = 1, 2, 3, \dots, N)$ is frequency values under the measure. F_u is stated as a feature from the concavity of power spectral distribution. In the alpha band, a feature has been adopted from a power spectral variance which signifies the increase of spectral distribution (4-4)

$$F_u = \sum_{j=1}^N (f_j^u)^2 \quad (4.3)$$

$$\sigma^2 = \frac{1}{L} \sum_{k=1}^L (p_k - \bar{p})^2 \quad (4.4)$$

Where, power spectral values are $p_k (k = 1, 2, 3, \dots, L)$ and the mean value the alpha band is \bar{p} . To distinguish individuals, the convexity of power spectral can be another key feature, which is defined as follows:

In the alpha band, the spectral values have been ranked and afterwards the frequencies of the top three values averaged respectively. This procedure is showed as in Figure 4.24(I). Here, the top three power spectral values and the frequencies are p_1, p_2, p_3 and f_1, f_2, f_3 respectively, the mean values of which are given by formulas 4.5 and 4.6

$$P_m = \frac{p_1 + p_2 + p_3}{3} \quad (4.5)$$

$$F_m = \frac{f_1 + f_2 + f_3}{3} \quad (4.6)$$

As shown in Figure 4.24(II), the power spectral values that are bigger than the mean are $f_i^g (i = 1, 2, 3, \dots, M)$ and their summation is equation (4.7).

$$F_g = \sum_{i=1}^M f_i^g \quad (4.7)$$

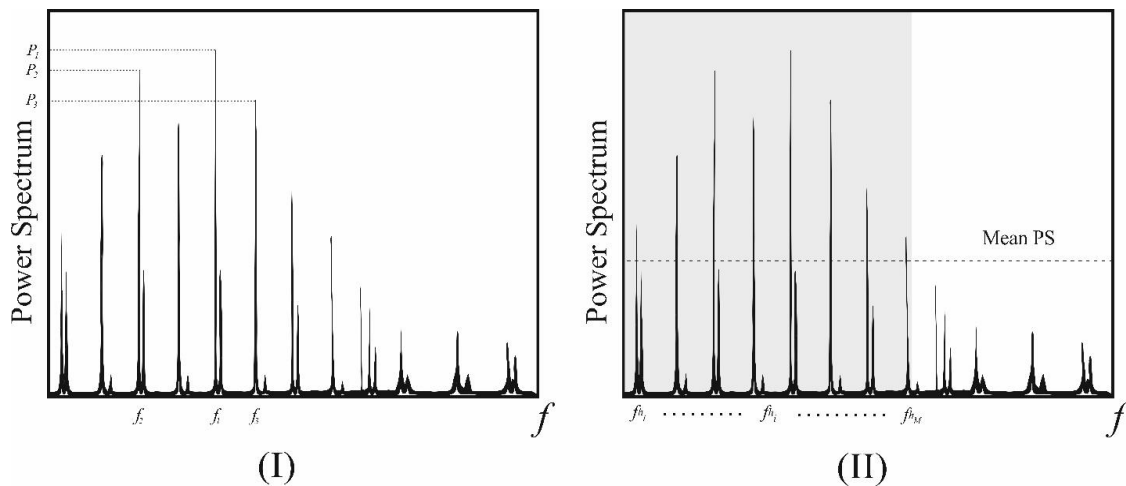


Figure 4.24. The process of the convexity of power spectral for frequencies and power spectral values

In this project, F_m, P_m, F_g from the convexity in power spectral distribution, are extracted as features. The spectral analysis has shown the frequency bands in which amplitude was different between the tasks and normal situation and especially the differences between each task and participants. Based on the classification method using Matlab software, we used the extracted feature obtained using this technique.

4.2.4 Classification

The Classification process was performed based on whether the picturing pattern was successfully recalled or not using Linear Discriminant Analysis (LDA) and Support Vector Machine (SVM) classifiers separately. At this stage, a choice of good discriminative features is very important for getting a better classification result that influences the project's intentions. Because of different environments and different experiment settings, there is no particular method to compare the results between different methods. LDA and SVM techniques are fast and less complex which makes them a good option specifically for authentication processes. LDA is often considered good for real-time BCIs because of its simplicity, speed of execution and low computational cost.

SVM works generally well depending on a clear margin of distinguishing two classes. It will be more efficient in spaces with high dimensions. The main classification technique for this study is the SVM method. LDA has been used separately to check the possible differences in results and accuracy rates. However, many factors such as pre-processing, feature extraction and classification stage are the most important part of any BCI application processes, which has highly influenced the accuracy rate. Therefore, LDA and SVM classification methods have been used to see the differences and compare the results. But the main classifier for the aim of the project is SVM. LDA is one of the most well-known data reduction methods. By utilizing this procedure, the hyperplanes are employed to distinguish the data from various classes. In this process, LDA expect normal distribution of the data, with equivalent covariance framework for the two classes.

The distinguishing hyperplane was obtained by looking for the estimate that maximizes the separation between the means of the two classes and limiting the interclass variance. For an N-class issue ($N > 2$) a number of hyperplanes are utilized in the process. Here, the equation (4.8) can define it, which is expanded over every linear projection, w:

$$J(w) = \frac{|m_1 - m_2|^2}{S_1^2 + S_2^2} \quad (4.8)$$

In equation (4.8), S represents a variance, m represents the mean and the subscripts signify the two classes [146]. LDA technique is used by Matlab software to find a linear transformation that discriminates between different classes. Support Vector Machine (SVM) is a classification technique that creates a hyperplane that separates the data set into classes dependent on kernel functions on a feature space with two dimensions [147] as shown in Figure 4.25.

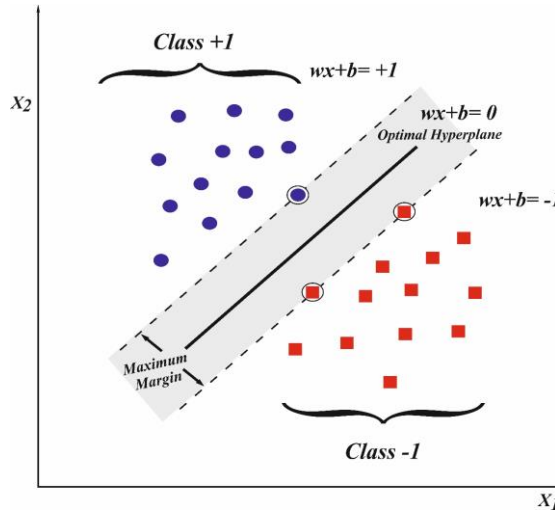


Figure 4.25. The fundamental idea of linear SVM characterized by the optimal hyperplane

(x_i) , which is the training data belonging to two separated classes (y_i) , (4.9) represented with the optimal hyperplane (4.10)

$$\{x_i, y_i\}, i = 1, 2, 3, \dots, N, y_i \in \{-1, +1\}, x_i \in R^n; \quad (4.9)$$

$$(w \cdot x_i) + b = 0; \quad (4.10)$$

In this study, the SVM technique selected the optimal hyperplane with the biggest margin using Equation (4.11) and (4.12), which is equivalent to Equation (13).

$$x_i \cdot w + b \geq +1 \quad \text{for } y_i = +1 \quad (4.11)$$

$$x_i \cdot w + b \leq -1 \quad \text{for } y_i = -1 \quad (4.12)$$

$$\begin{cases} w^T \varphi(x_i) + b \geq +1, & \text{if } y_i = +1 \\ w^T \varphi(x_i) + b \leq -1, & \text{if } y_i = -1 \end{cases} \rightarrow y_i [w^T \varphi(x_i) + b] \geq 1 \quad (4.13)$$

The $\varphi()$ function maps the input space into a greater dimensional space. Support vectors are the closest training data samples to the hyperplane. SVM classification technique was performed using 10-fold cross-validation to find out if the EEG signals formed with a picture

presenting can be used to predict that image's comprehended memorability. This classification was performed based on two labels of least memorable images and most memorable images according to whether correctly and incorrectly recalled as pictured and not pictured. Parameter tuning is performed empirically. The classification process was performed by Matlab. The extracted features from the previous section were imported to Matlab software for classification. The Classification Learner (CL) application in Matlab was used to train the data, creating the classification model to achieve the accuracy rate of the model by applying the test data. CL app is a statistical machine learning toolbox in Matlab platform. This was used to analyse the models to produce the accuracy rate for the given EEG data set. The features file which was prepared after the feature extraction part of the method, was imported to the CL app with 10 folds cross-validation. The number of folds is the number of parts which the training data set will be divided into. One of those parts will be selected for validation randomly. And the remaining parts will be used for training. As mentioned before, two classifiers (LDA, SVM) were used to train the model. Figure 4.26 shows a screenshot from the CL app after importing the feature data and applying the classifiers to train the model. As you can see in the picture, the data classified in two classes of Pictured and Not-pictured and classifiers create the model based on these two classes. It also shows a scatter plot of the data set in the middle of the picture which shows the correctly predicted points as dots and incorrectly predicted as crosses. In the left side of the picture, you can see the result of the performance of the LDA and SVM classifiers on this specific feature data imported for classification.

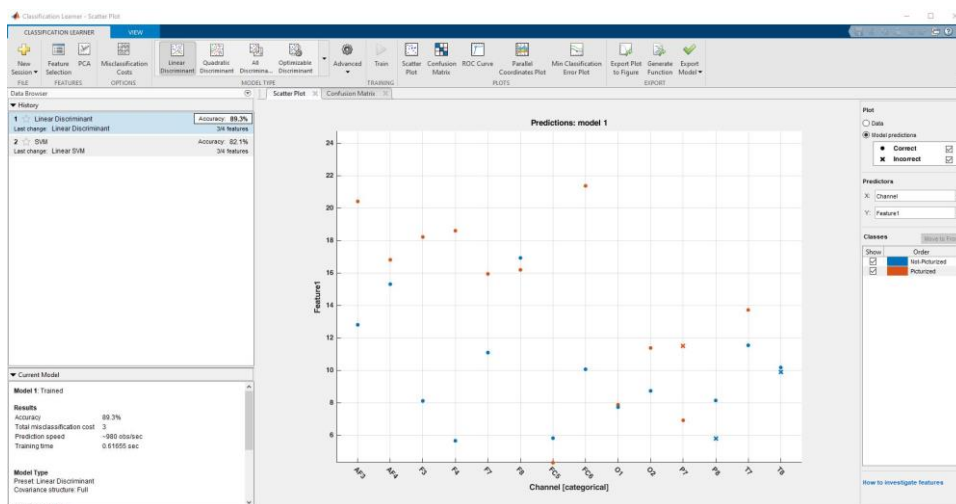


Figure 4.26. A screenshot of the Classification Learner Application in Matlab Software

Figure 4.27 shows the confusion matrix of the classifier’s result and the acquired percentages according to the True Positive Rates (TPR) and False Negative Rates (FNR). In this example you can see that 92% of observations have been classified as Not-Picturized correctly and 14.3% have been classified as Picturized wrongly. On the other hand, 85.7% have been correctly classified as Picturized and 7.1% have been classified as Not-Picturized wrongly.

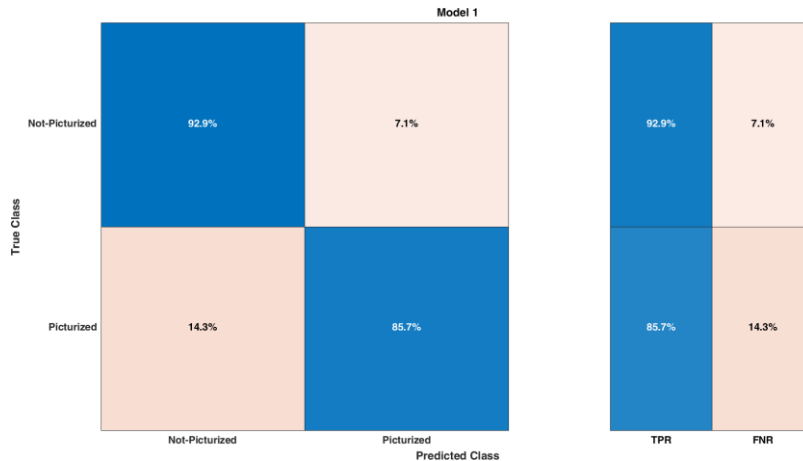


Figure 4.27. Confusion Matrix result of the EEG dataset after training the model

After training the data, the created model was exported as a Matlab code to test the data from the second session of the signal acquisition and achieve the accuracy rate of the picturing pattern method for each specific picture, the system showed that the 2D pictures achieved higher accuracy because they were easier to remember than Real Objects pictures to specify AUTH and NOTAUTH for the biometric authentication. To do this the EEG data set was loaded in BCILAB, a new approach using Log-Bandpower paradigm was selected with the recommended default resampling rate, neighbours per channel, and frequency specification [130] [131]. The epoch time window was added relative to both target markers. The machine learning function was set to SVM and LDA separately (Figure 4.28).

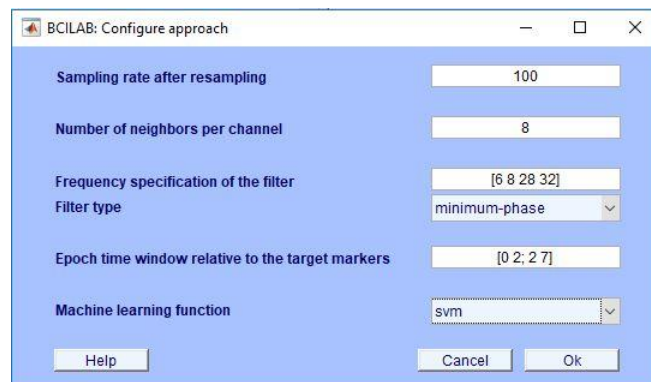


Figure 4.28. Uploading the data on BCILAB

Figure 4.29, shows the advanced BCILAB paradigm parameters view used to define AUTH and NOTAUTH target markers. As you can see, a 10-fold cross-validation is selected to compute loss/performance metric and performance estimates. Once the approach was finalized, a new model was then created.

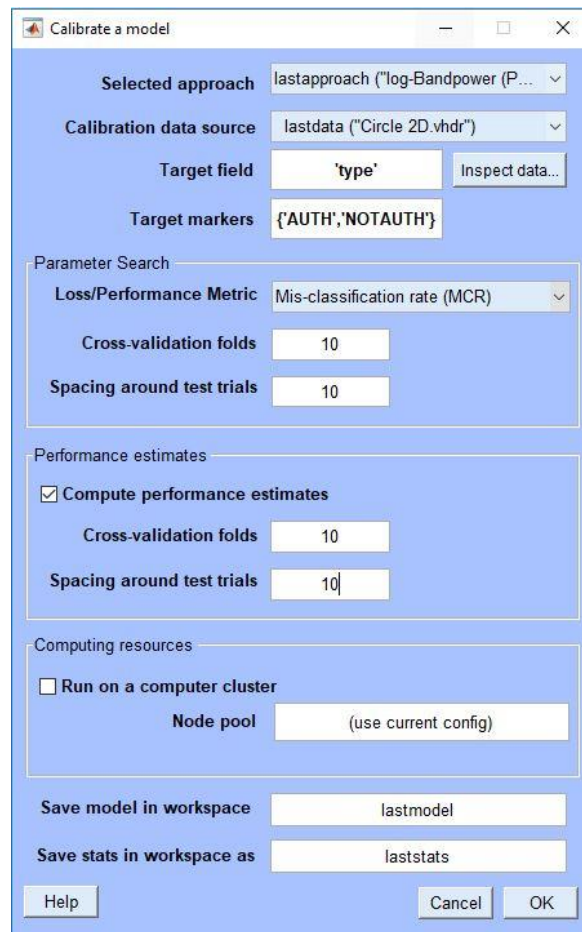


Figure 4.29. Applying the Log-Bandpower paradigm and creating model on BCILAB

Figure 4.30, demonstrates what the classifier results look like in BCILAB. It provides True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR), and Error Rate (ERR). It is important to note that FPR and FNR are equivalent to False Acceptance Rate (FAR) and False Rejection Rate (FRR) respectively.

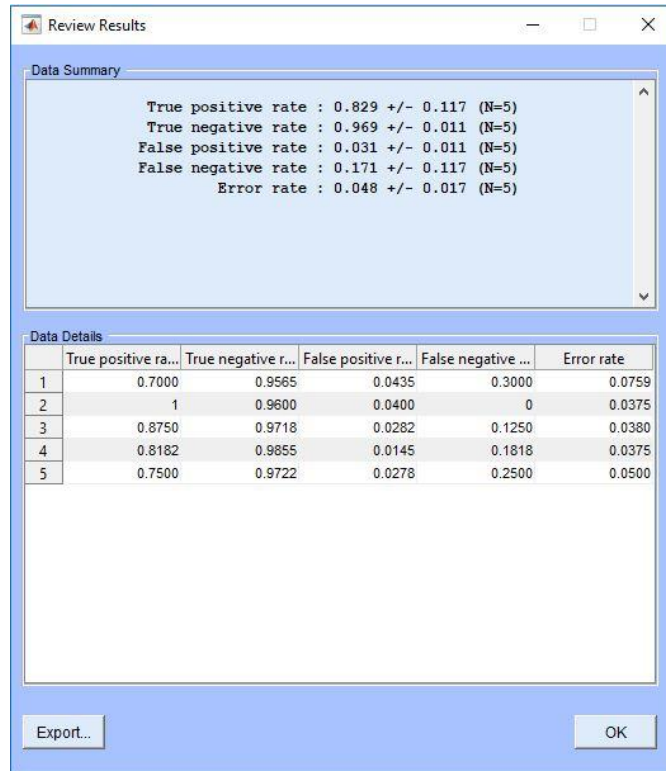


Figure 4.30. The paradigm Classifier results from BCILAB

4.3 Deep Breathing (DB) Method

As mentioned in previous chapters, there are three main EEG acquisition protocols for brain-based authentication methods: mental tasks, resting states, and tasks with external stimulus. Researchers experimented with different types of tasks like finger movement, sports activity, audio listening, colour identification, pass-thoughts, visual stimulus, and multi-tasking. Most of the studies achieved successful results with high accuracy rates but a majority of them are not reliable over a period as the human brainwaves are not stable over time.

Brain state stability or permanency is one of the biggest challenges for any brain-based authentication method. Brain situations can change depending on different events that any human could experience through life. Some events like sickness, addiction to drugs, experiencing high stress, getting mental issues, being drunk from alcoholic drinks, anxiety, and many other situations that can affect the brain functionality. Therefore, a new method is needed to improve the permanency of the brain pattern and the stability of it over time, which could be used in different mental states of the human brain.

Method II in this project is a solution to improve the stability of any brain pattern and cover the permanency challenge using deep breathing, which could be used as a reliable authentication method over time.

4.3.1 Deep Breath Brain Pattern

There are four steps in the proposed method for this project, which started with acquiring the brain signals from individuals for mental tasks including normal breathing, inhale, breath-holding, and exhale; the second step was cleaning the raw data including pre-processing, and filtering by applying FIR high-pass filter and ICA methods. The final step was feature extraction and classification, DWT technique on the data for feature extraction and NN classifier for classification using Wavelet Transform and Neural Network toolboxes in Matlab software. Figure 4.31 shows the whole process of the DB method which includes 4 stages before training and testing the data. This process starts with Signal Acquisition for the deep breathing task and following that pre-processing the data using FIR and ICA methods, Feature Extraction using DWT method, Classification using SVM and ANN classifiers to train and test the data for authentication and verification purposes.

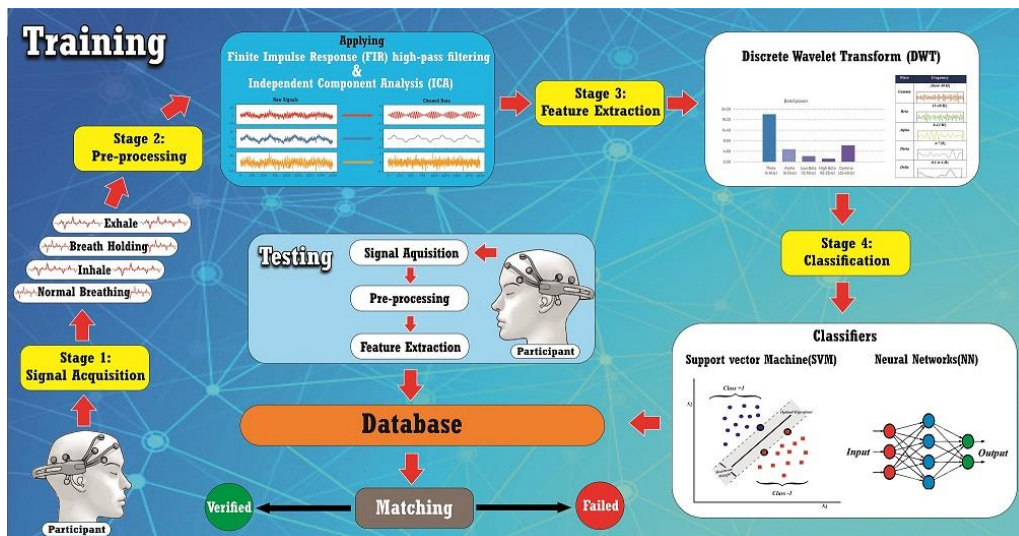


Figure 4.31. The methodology of the DB experiment

4.3.1.1 Signal acquisition

In this method, the data were acquired by the same BCI device as method I (14 channels Emotiv EPOC +) in two different sessions. A period of about 30 minutes per participant was spent in each session. In this experiment, fifty healthy participants from 25 to 45 years old were examined. In the first part of each session, participants were sat on a chair with closed eyes and breathed normally for 2 minutes. In the second part of each session, participants

started doing the deep breathing task at a rate of six breaths per minute. The time for each part of the deep breath was about four seconds for inhalation, two seconds for breath-holding, and four seconds for exhalation. In each session, the EEG data were recorded and stored as the raw data.

4.3.1.2 Pre-Processing

This process was done in the same way as method I in this project, A Finite Impulse Response (FIR) high-pass filtering technique with a band-pass range of 0.5 Hz and 50 Hz was exerted to remove slow and large amplitude drifts and make the data ready for the ICA. And after filtering, the ICA technique was applied to the data. Figure 4.32 shows the data recorded from channel 11 before and after cleaning and filtering.

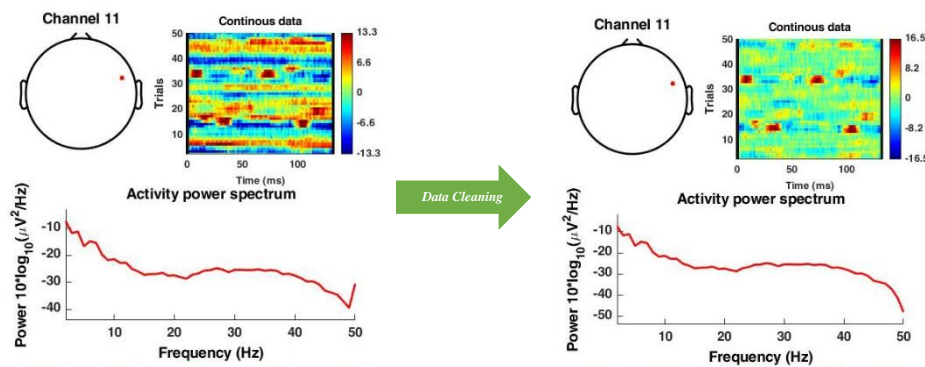


Figure 4.32. An example of a cleaned data after filtering

4.3.1.3 Feature extraction and Classification

In the first stage of the DWT, the signal is concurrently passed through LP and HP filters. The outputs from low and high pass filters are indicated as approximation (A1) and detailed (D1) coefficients of the first level. The output signals holding half the frequency bandwidth of the original signal can be down sampled by two due to the Nyquist rule [148]. The same procedure can be duplicated for the first level approximation and the detail coefficients fetch the second level coefficients.

Through each step of this decomposition process, the frequency resolution is multiple through filtering and the time resolution is split through down-sampling. To achieve better results in feature extraction, wavelet decomposition has been used as a preprocessing level for EEG segments to extract five physiological EEG bands, delta (0-4 Hz), theta (4-8 Hz), alpha (8-13 Hz), beta (13-30), and gamma (30-60 Hz) (Figure 4.33).

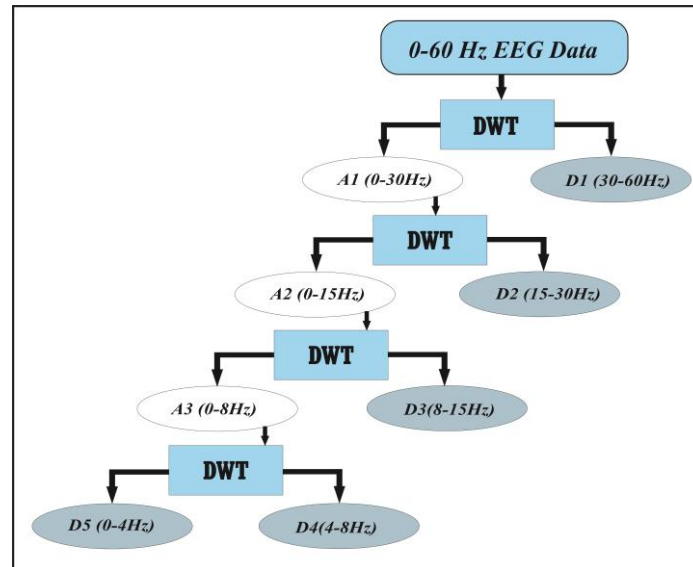


Figure 4.33. Decomposition of EEG data in four levels

For this purpose, four levels DWT with fourth-order Daubechies (db4)[149] wavelet function have been utilized. Since our data set is in the range 0-60 Hz, coefficients D1, D2, D3, D4 and A4 corresponding to 30-60 Hz, 15-30 Hz, 8-15 Hz, 4-8 Hz and 0-4 Hz respectively were extracted, that are almost standard physiological sub-bands. We have extracted the Maximum, Minimum, and Mean of the wavelet coefficients in each sub-band [150] which is obtained by the following Equation

$$\mu_i = \frac{1}{N} \sum_{j=1}^N D_{ij} \quad i = 1, 2, \dots, l \quad (4.14)$$

The last step takes care of analysing the features in order to determine what specific action should be taken based on the given values of the features. The backpropagation neural network algorithm was chosen as a classifier to find out the best accuracy.

4.3.1.3.1 Artificial Neural Network (ANN)

As mentioned, selected features were fed into two classifiers: Neural Network (NN), and Support Vector Machine (SVM) using Matlab. SVM and NN methods are the most commonly used techniques in EEG authentication studies. However, in a simple way, SVM without kernel is a single neuron inside neural networks, nevertheless with diverse cost function. By adding a kernel function, it will be comparable with two layer NNs. Actually, in terms of the model performance, SVMs are sometimes equivalent to a shallow neural network architecture [151][152]. Generally, an NN will outperform an SVM when there is a large amount of data.

Neural networks are complex models precisely in the manner of the human brain, which are designed to recognize different patterns. There are many different neuron layers in a neural net. Each layer receives inputs from previous layers and passes the outputs to further layers. NN methods have become very popular in EEG-based studies for authentication purposes because of the power of this classifier specifically for a larger data set.

Matlab Artificial Neural Network Toolbox was used in this process. The data were applied on the system in 3 layers of input, hidden and output layers. In this process 70% of the data was used for training, 15% for validation and 15% for testing.

Fig. 4.34 presents the ANN diagram performed in Matlab. Fifteen neurons are used in the hidden layer; feedforward back-propagation algorithm was used where the number of outputs was kept as five possible outputs for each part of the task (inhale, breath-hold, and exhale).

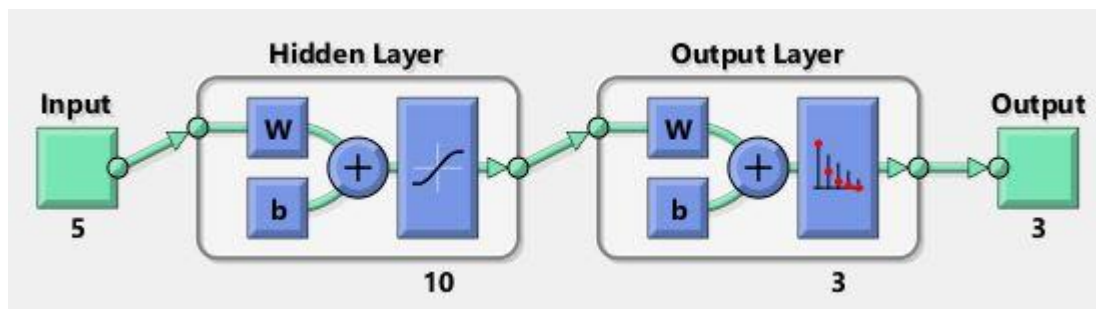


Figure 4.34. The ANN diagram for EEG brainwave segments

This results in five values of frequency spectrum in Decibels, provide the inputs of ANN. Next, the results are computed using the same weights as obtained in the training stage. Finally, the output is classified as 3 classes of inhalation, breath-holding and exhalation. During the training phase, the neural weights in ANN are calculated and they are used in the testing phase. The output from the testing phase is obtained and was used to find the biometric authentication decision ID from the values of (0 and 1); the decision parameter determines whether the EEG signal segment is authenticated or rejected. Specifically, if $ID = 0$, the signal segment is authenticated, and if $ID = 1$ indicates the segment is rejected.

The data set was separated into two approaches of training and testing. Two main measures were calculated for the proposed method analysis and performance: accuracy (Acc), and F-Score measure. These are formulated in equations (4.15) and (4.16) respectively:

$$Acc = \frac{TA+TR}{TA+FR+TR+FA} \times 100 \quad (4.15)$$

$$F - Sc = \frac{2TA}{FA+FR+2TA} \quad (4.16)$$

Where FA and FR represent False Acceptance, and False Reject respectively. TA and TR represent True Acceptance, True Reject respectively. A confusion matrix represented the classification results by its tabulating into one of four mentioned categories: TA, TR, FA, and FR.

This process was done in Matlab using neural network toolbox. First, the network was created and configured by choosing the number of layers and the algorithms that were used to configure the network, following that, the weights and biases were initialized for the network to start training and testing the data.

4.4 Summary

This chapter covers the three main parts of the BCI authentication process including pre-processing the data, feature extraction and classification. The third objective of this project was achieved by applying filtering techniques on the data and ICA algorithm to de-noise and clean the raw data and prepare it for feature extraction. The fifth and sixth objectives were achieved by extracting the specific features from the EEG data according to the purpose of this study and classified to find the accuracy of the methods and the success rate of them.

In the next chapter, all the achieved results will be presented and compared to other research studies and experiments to see the advantages and weaknesses of the proposed methods.

Chapter 5

Results and Evaluation

5.1 Introduction

This chapter is the achievement of the last objective of the project which is to evaluate the results for the permanency of the brain pattern, usability and security level of the proposed methods. It includes two parts according to the two presented methods in the previous chapter which shows the results achieved from each method separately. Each part includes the results from the classification, testing and evaluation of the method.

In the first method, the results from each user are compared separately and the average accuracy rates achieved from each user for both 2D and real object pictures were saved. The results achieved from each picture were compared to each other and the average result was saved for each picture that was used as a picturing pattern. The 2D and real object pictures are compared in detail. At the end the average accuracy rate of the first method is compared to other research in detail.

In the second method, the result from each user doing deep breathing was recorded and compared in detail. The deep breathing pattern was compared in its three different parts including inhalation, breath holding and exhalation in detail according to the accuracy rates achieved from each part. At the end, the average accuracy rate of this method is compared to other research in detail.

This chapter covers the last objective of this thesis which is evaluate the achieved results for permanency of the brain pattern and both usability and security of the method.

5.2 SaS-BCI Method

This method proposed to improve the usability and security in the BCI process for authentication purposes. This was done by predicting image memorability in the human brain. Visualised things, we remember for a long time. It is the second memory pathway to the brain. Our brain processes visual information 60,000 times faster than text. The brain can recall images more easily than abstract thoughts. This means picturing not only would be a better pattern for the brain to remember in the long term, but also it would be more secure than muscle movement patterns and other stimuli that need an external object to be used as a security pattern.

In this experiment, the total recorded EEG data divided into three categories for each user position. Three PSD feature vectors were created and classified by SVM and LDA classifiers.

Table 5.1 shows the average acquired accuracy rate for the pictures recalled from 20 participants. These percentages are by image category per user.

The results showed that the picturing of an image could be considered as a security brain-based pattern or Brain-ID for authentication.

Table 5.1. Image recall success percentage for both 2D and real object pictures

User ID	2D Object	Real Object	User ID	2D Object	Real Object
1	100%	65%	11	98%	65%
2	100%	63%	12	100%	54%
3	98%	54%	13	94%	18%
4	98%	30%	14	100%	21%
5	98%	65%	15	98%	45%
6	98%	23%	16	98%	33%
7	92%	58%	17	100%	61%
8	98%	30%	18	94%	15%
9	96%	11%	19	100%	18%
10	98%	45%	20	100%	38%

According to the results, there might be many reasons that are producing the EEG signals to be higher for the image that was successfully recalled later. For instance, as identified by the BCI, the increase in mental activities could be credited to the user trying to mentally pronounce the image name.

2D object images with higher EEG amplitudes had a higher chance of being recalled in comparison to the real object images with lower amplitudes.

It is significant here that there may be various reasons why the EEG signals are higher for the images that were successfully recalled later. For instance, as identified by the BCI the ascent in mental activities could be connected to the user naming the image mentally. Another explanation behind this ascent could be that the image is causing mental imagery.

It shows that real object pictures are harder to remember and recall. The 2D object pictures have a much higher successful recall (98%) than the real object pictures (41%). The recall differences between individuals can be noticed when it comes to real object pictures. About 60% success rate was achieved for a quarter of the users for recalling the real object images. SVM classifiers have been used to predict image recall. The data used in this experiment is for both successfully and unsuccessfully recalled images averaged over the 14 channels per

user. After doing the experiment, the participants were asked to fill in a questionnaire to see each real object’s memorability and which picture was easier to remember by asking them about 3 main details in each image. Figure 5.1 shows the percentage of remembrance of participants for each real object picture separately.

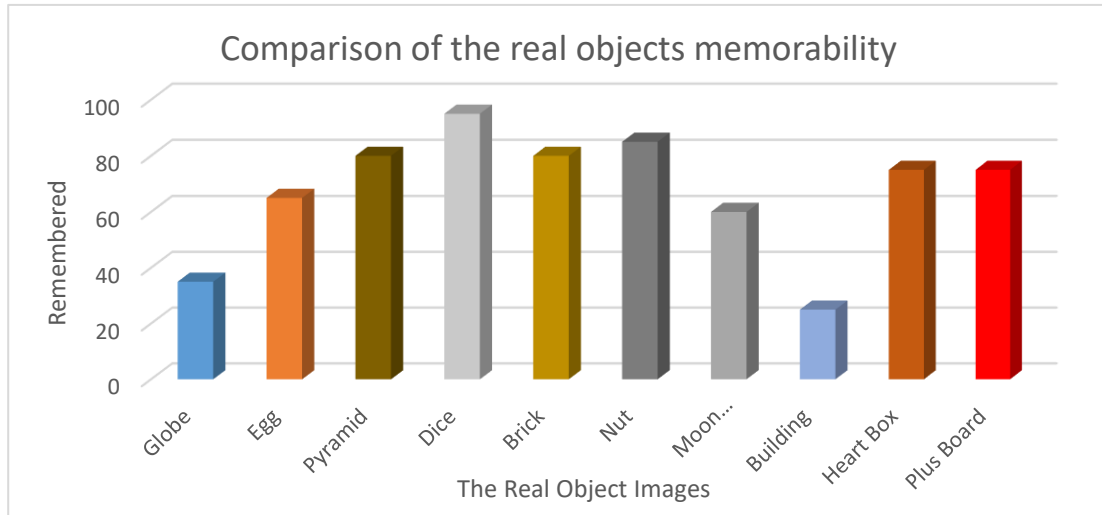


Figure 5.1. A comparison between the real object pictures in terms of difficulty to remember the details

This data was used for feature extraction and selection in the domains deliberated earlier. As discussed in Chapter 3, there are two fundamental aspects that must be tested in biometric systems: system effectiveness and user acceptance. Biometric systems should measure FAR, FRR, and EER as key effectiveness metrics. The first two establish whether the system accurately identifies the user while the last specifies the error rate where FAR and FRR are equal. These values are determined as follows:

$$FRR = \frac{\text{False Rejections}}{\text{Unauthorized Attempts}} \times 100\% \quad (5.1)$$

$$FAR = \frac{\text{False Acceptances}}{\text{Unauthorized Attempts}} \times 100\% \quad (5.2)$$

EER is defined as the point where FAR equals FRR. A lower EER indicates a more accurate system. Tables 5.2 describes the best results of the analysis in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), and Error Rate (ERR) for Log-Bandpower paradigm, across the chosen learning algorithms: LDA, SVM.

Table 5.2. The results of the classifiers for picturing pattern

Participant	Classifier	TPR	TNR	FAR	FRR	ERR	Participant	Classifier	TPR	TNR	FAR	FRR	ERR
1	LDA	0.79	0.97	0.21	0.05	0.088	1	SVM	0.75	0.97	0.23	0.02	0.067
2	LDA	0.95	1	0.17	0.03	0.037	2	SVM	1	0.96	0.31	0.08	0.055
3	LDA	1	0.95	0.25	0.05	0.05	3	SVM	0.88	1	0.16	0.06	0.039
4	LDA	0.93	1	0.21	0.02	0.037	4	SVM	0.83	0.97	0.18	0.12	0.088
5	LDA	0.86	1	0.21	0.05	0.05	5	SVM	0.76	0.89	0.2	0.08	0.083
6	LDA	1	0.88	0.13	0.03	0.03	6	SVM	0.88	0.97	0.25	0.02	0.027
7	LDA	0.7	0.95	0.21	0.02	0.091	7	SVM	0.88	1	0.16	0.12	0.039
8	LDA	0.95	1	0.18	0.1	0.035	8	SVM	0.76	0.88	0.29	0.1	0.091
9	LDA	0.91	0.95	0.21	0.02	0.021	9	SVM	0.85	0.95	0.25	0.06	0.035
10	LDA	0.6	0.88	0.19	0.05	0.05	10	SVM	0.72	0.97	0.21	0.08	0.021
11	LDA	0.79	1	0.23	0.03	0.035	11	SVM	0.8	0.92	0.19	0.13	0.057
12	LDA	0.6	0.95	0.19	0.03	0.037	12	SVM	0.6	0.83	0.13	0.06	0.035
13	LDA	0.97	1	0.17	0.05	0.055	13	SVM	0.97	0.97	0.17	0.05	0.037
14	LDA	0.8	1	0.17	0.02	0.088	14	SVM	0.86	0.93	0.23	0.08	0.055
15	LDA	1	0.88	0.21	0.06	0.067	15	SVM	0.79	0.96	0.19	0.1	0.088
16	LDA	0.92	1	0.3	0.05	0.055	16	SVM	0.86	0.92	0.21	0.12	0.088
17	LDA	0.79	0.95	0.19	0.1	0.039	17	SVM	0.93	1	0.23	0.06	0.037
18	LDA	0.76	1	0.18	0.05	0.033	18	SVM	0.82	0.97	0.25	0.05	0.053
19	LDA	0.92	0.97	0.21	0.03	0.083	19	SVM	1	0.88	0.2	0.03	0.037
20	LDA	0.88	1	0.25	0.02	0.027	20	SVM	0.75	0.96	0.21	0.12	0.057
Ave	...	0.856	0.96	0.203	0.043	0.050	Ave	...	0.834	0.945	0.212	0.077	0.054

The relative accuracy of the system can also be determined using the following formula:

$$Accuracy = \frac{TPR + TNR}{TPR + TNR + FPR + FNR} \quad (5.3)$$

Where TPR = True Positive Rate, TNR = True Negative Rate, FPR = False Positive Rate, and FNR = False Negative Rate. Also, FAR = FPR and FRR= FNR. From the collected data, it is clear that Log-Bandpower provides higher accuracy. The performance of the classifiers based on the extracted feature sets is shown in Table 5.3.

Table 5.3. The average results for the performance SVM & LDA classifiers

Classifier	Feature Set	Precision	Recall	F-Score	Accuracy
LDA	PSD	0.89	0.83	0.85	0.86
SVM	PSD	0.89	0.86	0.86	0.88

The PSD resulted in an average rate of 88% accuracy by the SVM classifier and an average rate of 86% accuracy by the LDA classifier. It is important to mention that the image recall’s prediction achieved in this experiment is only from the short-term memory, and the results could be different for long-term memory. This method specifically concentrated on the pictures that users were asked to memorize in their minds. It provides an understanding into how the brain observes images with different characteristics and helps provide a significant improvement for mental imagery security while recognising the human unique feature in the system.

Most of the researchers reported that higher accuracy rates can be achieved with more complex tasks [22] [19] [126], but complex tasks make the system less practical, because both processes of system training and authentication would be very time-consuming. In regard to this matter, the presented authentication method with the SaS brain-based paradigm is simpler and faster in comparison with the other methods in different studies.

Table 5.4 shows a comparison between this research and two other studies for brain-based authentication. The accuracy of the presented method is 88% which is lower than Gui et al. [153] with 90% accuracy. Although it is less than the results from Gui et al., the authentication method used in the proposed study is simpler and less complex than that of Gui et al. Higher accuracy can be achieved by combining several extracted features, but the classification takes a long time to process and it makes the experiment more complex. Task

complexity makes the computational cost higher and it is more time consuming which makes the authentication process slow and less practical.

Using more subjects raises the accuracy rate of classification methods. It was confirmed by Chen et al. [19] with execution multi and single-trial classification. Using fewer subjects delivers a better accuracy rate than more subjects, therefore the similar ones can be found in a bigger set [152]. The approaches which, demonstrate high accuracy with small numbers of subjects, might not represent a strong result for a large population in terms of security, because the risk of hacking the system would be higher. The average accuracy rate for the “SaS” strategy is in second place by using 20 subjects in comparison to Yeom et al. [107] with fewer subjects. This means that the presented authentication system achieved a higher accuracy with more subjects using the SaS strategy. On the other hand, brain patterns for a specific mental task can change over time. Specifically, accuracy of frameworks trained by preference-based tasks [22] can corrupt as user tastes change. It is important to note that the experiment performed in this study can be used for the both short-term and long-term memories. It means that for the long-term memory issues, the brain can produce the same signal amplitude by re-seeing the same picture that has been seen (memorized) as a Brain-ID.

Table 5.4. Comparison of three different experiments with different strategies and classifiers

Experiments	Signal Acquisition Strategy	The Number of Subjects	Channels	Features	Classifier	Ave Accuracy
Gui et al. [153]	Read the words silently	32	6	Wavelet packet decomposition	Neural Network	90%
Yeom et al. [107]	Visual evoked potentials	10	18	Dynamic feature	SVM	86%
Proposed method	SaS	20	14	PSD	SVM	88%

EEG brain signals are distinctive in general; however, the processes of feature extraction to normalize differences in time is a reason for some loss of uniqueness, which is why the results obtained in some parts are not without errors. There are many different ways and methods for signal processing such as different types of signal filtering and noise removing, feature extraction algorithms and many other classification methods and classifiers that could achieve different results but not significantly.

According to the literature, for this type of authentication method the alpha and beta frequencies are the most appropriate bands because the main stimulus is thinking and imagining a picture (visualising) which is active. However, in some cases, the combination of Beta and Alpha bands (8–40 Hz) could acquire better accuracy than the separate frequency bands. The differences between the accuracy rates for each user with the same user-strategy shows that capturing the raw signal can affect the results. It means, for some users the signal strength of the electrodes was not steady in the time of recording because some of the participants had long hair and the hair had an influence on the quality of the signals and on the other hand, the situation of electrodes in Emotiv device was not suitable for the shape of some users' heads. What this experiment adds is specific to images that users are required to memorise, then, participants have been asked to remember the introduced images. This study gives some knowledge into how the brain sees pictures with various attributes, and what that can educate us concerning this image recall, which may help improving the security process for brain-based authentication methods.

5.3 Deep Breathing Method

The rhythm of breathing creates electrical activity in the human brain that enhances emotional judgments and memory recall. These effects on behaviour depend on whether it is inhale, exhale or breath holding. It means that deep breathing can bring back brain signal to its own normal state and help remembering, picturing memorised patterns. The human brain is not stable during life and, depending on different situations, it could lose its normal state to create any patterns. Deep breathing can improve any brain-based security patterns in the long term. This experiment is done to prove the effects of deep breathing on the brain and see if the deep breathing itself can be a security pattern for authentication purposes.

The brain EEG data were acquired from 50 individuals doing two tasks: normal breathing and deep breathing. The deep breathing task was done in three parts of inhalation, breath-holding, and exhalation. The recorded data sets were pre-processed and the necessary features regarding the aim of this research were extracted and selected for classification. The three labels, inhalation, breath-holding, and exhalation were performed for both SVM and NN classifiers. All 3 steps of the deep breathing task had a successful recall percentage. However, the results showed that the inhale and exhale part of the deep breathing task are harder to recall but the general trend of breath-holding had a much higher successful recall

than the other two. According to the results the breath-holding part of the deep breathing task is considered as the brain pattern for the authentication process. Table 5.5 shows the results of the classifiers for all 50 participants.

Table 5.5. The average results of both SVM and NN classifiers for breath-holding pattern

<i>Classifier</i>	<i>TPR</i>	<i>TNR</i>	<i>FAR</i>	<i>FRR</i>
<i>SVM</i>	0.82	0.97	0.17	0.02
<i>NN</i>	0.86	0.97	0.15	0.03

The selected features according to the three domains discussed earlier were fed into each classifier as separated feature sets. The performance of the classifiers was based on the three selected features. The results of the classifiers for recalling the breath-holding part of the task were with an average accuracy of 0.89, 0.88 with the accuracy rate of 90% and 91% for NN and SVM classifiers respectively with a precision of 0.95 [Table 5.6].

Table 5.6. The average performance of the classifiers for *recalling* Breath-Holding vs *not recalled*

<i>Classifier</i>	<i>Precision</i>	<i>Recall</i>	<i>F-Score</i>	<i>Accuracy</i>
<i>NN</i>	0.95	0.88	0.86	0.90
<i>SVM</i>	0.95	0.89	0.85	0.91

Table 5.7 is a comparison between some high-results performance experiments that were achieved in previous works in the EEG-based authentication area. As you can see, high enough accuracy rates have been achieved in all experiments. Patel et al., got the highest accuracy rates 92.5% among all of them, following that Armstrong et al., with 89% and Zhendong et al. with 87.3%. Both Armstrong et al. and this thesis passed the permanency test, but the result achieved from this thesis using the deep breathing method is higher by 3% with a 91% accuracy rate. In comparison to other mental tasks and brain patterns used in the studies, the deep breathing pattern can be performed with no equipment, no cost and most importantly deep breathing can be done anywhere by anyone in any situation of human life at any time.

Table 5.7. A comparison between this paper and previous works

<i>Author</i>	<i>Brain State Tasks</i>	<i>Accuracy</i>	<i>Permanency Test</i>
Armstrong et al. [33]	Text reading	89%	Yes
Patel et al. [34]	Visual stimulus	92.5%	No
Zhendong et al. [36]	Visual stimulus	87.3%	No
Proposed technique	Deep Breathing	91%	Yes

The results showed that deep breathing could bring back brainwaves to a normal state. It also promotes alpha waves, which is the band related to mind relaxation and would be very helpful to create a pattern no matter what situation the person is experiencing including stress, fear, anxiety, sickness, and many other conditions that can distract the brain from its normal state. Deep breathing can also promote other brainwaves including Delta, which occurs in the deepest state of complete relaxation, and Theta, during extreme mind relaxation. Therefore, deep breathing not only could help other brain states in terms of permanency but also could be an appropriate option to be used as a brain pattern for authentication purposes.

5.4 Summary

This chapter includes all the results achieved from both picturing patterns and deep breathing patterns brain-based authentication methods. The first proposed method achieved a high accuracy rate of 88% which shows this could be a more practical method to heighten the level of security and the usability of the system. The second proposed method achieved a high accuracy rate of 92% which shows a great improvement in permanency of the brain pattern in time. The last objective of this thesis was achieved in this chapter. The results from both proposed methods were presented and compared to other research and experiments which shows improvements in the BCI authenticating process in terms of usability, security and permanency of a brain-based authentication pattern that can be used as a biometric user identification technique.

Chapter 6

Conclusion

6.1 Overall Conclusion

In the near future, biometric authentication methods will be the most useful methods for devices and applications because of the usability, security level, ease of use, and fast execution. Many brain computer interface experiments were performed using brain signals as an alternative biometric authentication method, where some of them achieved high accuracy for their experiences. However, there are several limitations such as usability, security level and permanency of the system through time associated to such methods which need to be resolved for any brain-based authentication in the future.

Brainwaves are another human biometric that could be the most secure biometric technique. In comparison with other biometric techniques in terms of security, the human brain signal has a number of advantages. Firstly, it is the only biometric that is changeable, not visible to duplicate and does not have a shoulder-surfing problem. Secondly, it is more useful for disabled individuals of which a good example would be the famous scientist Stephen Hawking who was using a kind of brain-computer interface technology.

The proposed research was initiated by investigating the use of EEG brain signals for biometric authentication. Two strategies were presented as brain-based authentication methods: SaS-BCI picturising pattern and deep breathing method.

Earlier in Chapter 1, the research aim and objectives were set out and only a brief summary is presented here. The main target for this research was to propose techniques and strategies to improve security, usability and stability of a brain pattern in a BCI authentication process.

Our goal was to create a user strategy using different techniques of feature extraction and classifications of brain signal to achieve higher accuracy rates in results, and improve the BCI authentication process in terms of speed, usability, security and permanency of the method in time.

Seven primary objectives were specified in order to achieve the principal goal. First, investigating different biometric authentications, brain-computer interfaces and brain-based authentication techniques in previous studies, to have a better view of the whole spectrum of biometric authentication methods and their advantages and disadvantages. Second, proposing new user strategies to record the EEG signal using a BCI device which was done by Emotiv EPOC+ non-invasive brain device. Third, capturing a primary data set following

the appropriate ethical procedures from the LJMU. Fourth, applying filtering techniques and algorithms to de-noise the data from artifacts and unnecessary signals and clear the required components in the recorded data. Fifth and Sixth, using methods and machine learning algorithms to extract the useful features and classify them to test and achieve the desired result. Finally evaluating the archived results for usability, security and permanency of the method in time. All the objectives were met in order to achieve the research goal.

The first three objectives which were an accurate investigation into previous experiments and research in this area and recording the EEG data from participants using Emotiv Epoc+ device, were completed, and the primary data archived according to research ethical regulation approved by LJM University. All the EEG raw data were saved in the university computer system and prepared for analysis.

In order to achieve the fourth objective which is applying filtering techniques and the Independent Component Analysis (ICA) algorithm on the data for noise removal; the fifth objective, which is extracting the needed features according to proposed strategies to use as the authentication signature; and the sixth objective, which is applying the new signal processing and classification method on the data to achieve better results for a brain-based biometric authentication system, two different strategies and methods were proposed as the SaS-BCI method using picturising pattern and deep breathing pattern in three parts of inhalation, breath-holding and exhalation. The security and usability of the BCI authentication process improved by proposing the SaS-BCI user strategy using picturising pattern as a brain ID, applying the band-pass filtering technique and ICA algorithm to de-noise the data, applying FFT, PSD methods and log-bandpower paradigm to extract the biometric features and finally classifying the data using SVM and LDA classifiers to achieve the desired results.

The stability and permanency of the BCI authentication process was improved by proposing the deep breathing user strategy using breath-holding as a brain ID, and the same process as the first proposed method for signal pre-processing and noise removal and DWT method for feature extraction and finally classifying the data using SVM and NN classifiers.

The last objective of this thesis was archived after evaluating and comparing the archived results from each method and classifier to other experiments and previous researches which

showed big improvements in terms of usability, security and stability of the method in comparison to other researcher works.

Selecting each of the general protocols for recording EEG including physical tasks and imaginary tasks can affect the process and the accuracy of brain-based authentication process.

Different mental tasks or brain-based paradigms will have different outcomes. According to the literature, it is shown that better results have been achieved from imaginary tasks and protocols in comparison to the physical ones. Many different mental tasks have been tested and good results achieved. However, most of them are very complex and time-consuming for the authentication process.

For a secure and fast brain-based authentication process, we need an imaginary brain paradigm that can be used as a brain-ID. Regarding the literature, pictures and shapes can be easier to memorize and choosing a good authorization paradigm could be very important for authentication purposes. Therefore, in this study a brain picturing pattern has been tested by the proposed method to predict image memorability and see which types of images are easier to remember and are more appropriate to use as brain-IDs

The results showed that SaS-BCI could be a very useful way of authorization from each human's brain ID. For this process, the user can look at a specific picture, memorise it and register the brain-ID by imagining the picture in the mind. Therefore, in terms of security, the combination of these two could be a new hybrid strategy to get better results for using the brain signals as an authentication technique. Mental imagery and using the picturing pattern in the mind could be a more secure brain pattern to use as a brain-based authentication method. Memorising a picture in the mind as a user ID would be a useful way in terms of security according to the fact that no one can see it in the user's mind and the user can change the pattern whenever is necessary.

The first method of this study has investigated the use of an EEG brain signal to predict image memorability and the possibility of using the mental imagery pattern as a biometric authentication method. A new strategy (SaS) was used which in comparison to other studies in terms of security could be one of the most useful brain-based authentication patterns. This method by using all the techniques and algorithms, which were for the pre-processing and

feature extraction and classification resulted in an average of 88% accuracy rate. It should be noted that the results could be slightly different by using different techniques and algorithms of signal processing and classification.

The big challenge for all brain-based authentication studies is that the brain patterns can change depending on the brain situation. For instance, EEG data of a person can change in situations like being sick, being drunk, being addicted to drugs, and getting mental issues like anxiety, high stress, deep sadness and many other situations that any human can experience. Therefore, it needs a new method to improve the results, which can be useful in all different mental situations of the human brain, not just for specific tasks in a specific situation. The second method in this study is presented to cover this issue.

The second method presented an EEG-based authentication method using deep breathing as a brain pattern by recording the EEG data from 50 individuals, taking deep breaths in three steps for each session. The result shows that deep breathing tasks could improve brainwaves, specifically the alpha wave in different situations no matter what the individual's brain is experiencing. A deep breathing task could be the best choice to have a stable EEG pattern with a high accuracy rate for brain-based authentication purposes. This technique achieved an average of 92% accuracy rate successfully. It showed that the proposed method using a deep breathing pattern could improve the process of authentication in terms of permanency and stability of the brain pattern. This work may provide the basis for future investigations on EEG data to do accurate predictions for long-term memory tasks.

6.2 Limitations and problems

- There were some problems and limitations in the process of this project, which had an influence on the quality of the results and, the number of users. These limitations are as follows:
- The electrode position of the Emotiv device was not suitable for some participants' heads
- The signal strength of the Emotiv device is weak and was unstable for a number of the participants that had long hair.
- Emotiv EPOC+ device problems: The electrodes of this device were getting dirty and rusty through the experiments which meant taking out the electrodes and cleaning them to get better quality signals.

- Emotiv Pro software: As mentioned before, the Emotiv device needed special software (Pro Software) to capture the signals and record them to a computer. It made the process harder because that software was not open source and free and the device would not record the data without its specific licence, which had to be paid for.
- The pandemic situation caused by COVID-19 made it harder to find individuals to participate in this study.

Resolving the mentioned limitations will be the main part of our future work which is explained in the next section.

6.3 Future works

This research focused on brain signal as a new biometric authentication method. Considering the aforementioned limitations, a number of possible future directions can be recommended. According to the weakness of the brain signals recorded non-invasively, we need stronger BCI devices that could record brain signals with much less noise, and auto detect the unnecessary signals and separate them with the desired signals according to the created pattern. There are many different types of BCI devices to capture and record the brain signals. Using different devices will be another decision to acquire the brain signals and investigate them.

In terms of the technology according to our fast progress world, there are new types of BCI devices which are more practical, stronger and faster than the device that was used in this research. To create a practical and suitable authentication method using brain signals, it is very important to use a high-tech brain device which works faster with more accuracy in recording the specific components of the human brain. We will use the best recent brain devices for our future experiments and try to see the strengths and weaknesses of different types of devices and design a new piece of technology that could record human brain signals in as efficient, easy-to-use and cost-effective way as possible.

In terms of participants and users, in the future a larger number of users will be tested to achieve results with higher accuracy that would be more trustworthy to be used in real time life experiments. The larger the number of users, the more reliable result would be acquired.

In terms of user strategy or signal acquisition, the human brain is not stable depending on different situations that any human would experience in life. Therefore, more user strategies

would be used to find the best one which can be more stable through time and would be easier for authentication process. Different types of users will be investigated and tested, especially disabled individuals who are not able to use their hands and move their bodies. Therefore, better methods can be developed specifically for users with disability to make it easier for them to use the brain-based technologies.

In terms of the signal processing feature extraction and classification of EEG data there are many different methods and algorithms that we would consider to use and investigate to select the best techniques and improve them in a way that could have a direct effect on the accuracy of the results. Recent machine learning methods need strong computers with a high specification to process the larger amount of data which makes the process of the authorisation and authentication slower. The other machine learning methods would be investigated and be updated to improve the speed and the accuracy of the process which has a direct influence on the authentication process.

In terms of security level, more security-based methods will be investigated like two-factor authentication methods using EEG signals. It enables users to improve their pattern with the mental state and it can improve the level of security using brain signals.

Our major concerns for the future work will be investigating the recent BCI devices and find their advantages and weaknesses to create a piece of technology which can record brain signals non-invasively with a stronger signal recording electrodes that can record the EEG data with fewer noises and artifacts. A device that could allow us to integrate different machine learning algorithms including the methods presented in this research, in its recording process that can do the steps of pre-processing, feature extraction and classification in real-time.

In summary, the major goal of the proposed study was to achieve faster, easy to use, and secure BCI authentication system that can be integrated on security-based technologies and devices. It is hoped that the present thesis might pave the way for future researchers in this realm and to indicate the directions in which future BCI biometric authentication research should proceed.

References

- [1] Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, 38, pp.97-102.
- [2] Burrows, M., Abadi, M. and Needham, R.M., 1989. A logic of authentication. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 426(1871), pp.233-271.
- [3] Bissada, A. and Olmsted, A., 2017, December. Mobile multi-factor authentication. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 210-211). IEEE.
- [4] Simmons, G.J., 1988. A survey of information authentication. *Proceedings of the IEEE*, 76(5), pp.603-620.
- [5] Khan, H.Z.U. and Zahid, H., 2010. Comparative study of authentication techniques. *International Journal of Video & Image Processing and Network Security IJVIPNS*, 10(04), pp.09-13.
- [6] DeBow, B. and Syed, K., 2006, October. 802.11 wireless network end-user authentication using common access cards. In *Military Communications Conference, 2006. MILCOM 2006*. IEEE (pp. 1-5). IEEE.
- [7] Kittler, J., Ballette, M., Czyz, J., Roli, F. and Vandendorpe, L., 2002. Enhancing the performance of personal identity authentication systems by fusion of face verification experts. In *Multimedia and Expo, 2002. ICME'02. Proceedings. 2002 IEEE International Conference on* (Vol. 2, pp. 581-584). IEEE.
- [8] Taher, K.A., Nahar, T. and Hossain, S.A., 2019, January. Enhanced cryptocurrency security by time-based token multi-factor authentication algorithm. In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)* (pp. 308-312). IEEE.
- [9] Jain, A., Bolle, R. and Pankanti, S. eds., 1999. *Biometrics: personal identification in networked society* (Vol. 479). Springer Science & Business Media.
- [10] Otti, C., 2016, May. Comparison of biometric identification methods. In *Applied Computational Intelligence and Informatics (SACI), 2016 IEEE 11th International Symposium on* (pp. 339-344). IEEE.
- [11] Lal, N.A., Prasad, S. and Farik, M., 2016. A review of authentication methods. *vol. 5*, pp.246-249.
- [12] Nishiuchi, N., Komatsu, S. and Yamanaka, K., 2010. Biometric verification using the motion of fingers: a combination of physical and behavioural biometrics. *International Journal of Biometrics*, 2(3), pp.222-235.
- [13] Alsaadi, I.M., 2015. Physiological biometric authentication systems, advantages, disadvantages and future development: A review. *International Journal of Scientific & Technology Research*, 4(12), pp.285-289.
- [14] Garnett, S., 2005. *Using brainpower in the classroom*. Taylor & Francis.
- [15] Konstantyan, V.N., Sabanchiev, A.M., Sannikov, A.S., Aliev, M.I. and Glashev, R.M., 2021, September. Contactless Compact Through-joint Supply Voltage and Control Signals Transferring Method. In *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 380-383). IEEE.
- [16] Allison, B.Z., Wolpaw, E.W. and Wolpaw, J.R., 2007. Brain-computer interface systems: progress and prospects. *Expert review of medical devices*, 4(4), pp.463-474.
- [17] Hartson, H.R. and Hix, D., 1989. Human-computer interface development: concepts and systems for its management. *ACM Computing Surveys (CSUR)*, 21(1), pp.5-92.
- [18] Ramadan, R.A., Refat, S., Elshahed, M.A. and Ali, R.A., 2015. Basics of brain computer interface. In *Brain-Computer Interfaces* (pp. 31-50). Springer, Cham.
- [19] Chen, Y., Atnafu, A.D., Schlattner, I., Weldtsadik, W.T., Roh, M.C., Kim, H.J., Lee, S.W., Blankertz, B. and Fazli, S., 2016. A high-security EEG-based login system with RSVP stimuli and dry electrodes. *IEEE Transactions on Information Forensics and Security*, 11(12), pp.2635-2647.

- [20] Chuang, J., Nguyen, H., Wang, C. and Johnson, B., 2013, April. I think, therefore I am: Usability and security of authentication using brainwaves. In International conference on financial cryptography and data security (pp. 1-16). Springer, Berlin, Heidelberg.
- [21] La Rocca, D., Campisi, P., Vegso, B., Cserti, P., Kozmann, G., Babiloni, F. and Fallani, F.D.V., 2014. Human brain distinctiveness based on EEG spectral coherence connectivity. *IEEE transactions on Biomedical Engineering*, 61(9), pp.2406-2412.
- [22] Ruiz-Blondet, M.V., Jin, Z. and Laszlo, S., 2016. CEREBRE: A novel method for very high accuracy event-related potential biometric identification. *IEEE Transactions on Information Forensics and Security*, 11(7), pp.1618-1629.
- [23] Thorpe, J., van Oorschot, P.C. and Somayaji, A., 2005, September. Pass-thoughts: authenticating with our minds. In Proceedings of the 2005 workshop on New security paradigms (pp. 45-56). ACM.
- [24] Di, Y., An, X., He, F., Liu, S., Ke, Y. and Ming, D., 2019. Robustness analysis of identification using resting-state EEG signals. *IEEE Access*, 7, pp.42113-42122.
- [25] Barry, R.J., Clarke, A.R., Johnstone, S.J., Magee, C.A., Rushby, J.A., 2007. Eeg differences between eyes-closed and eyes-open resting conditions. *Clin. Neurophysiol.* 118 (12), 2765–2773 .
- [26] Ruiz-blondet, M., Khalifian, N., Armstrong, B.C., Jin, Z., Kurtz, K.J., Laszlo, S., 2014. Brainprint: identifying unique features of neural activity with machine learning. In: Proc. 36th Annual Conf. of the Cognitive Science Society, pp. 827–832 .
- [27] Zuquete, A., Quintela, B., Silva Cunha, J.P., 2010. Biometric authentication using brain responses to visual stimuli. In: International Conference on Bio-inspired Systems and Signal Processing, pp. 103–112 .
- [28] Das, R., Piciuccio, E., Maiorana, E., Campisi, P., 2016. Visually evoked potentials for EEG biometric recognition. In: 2016 1st International Workshop on Sensing, Processing and Learning for Intelligent Machines, SPLINE 2016 – Proceedings .
- [29] Zhang, F., Mao, Z., Huang, Y., Lin, X., Ding, G., 2018. Deep learning models for eeg-based rapid serial visual presentation event classification. *J. Inf. Hiding Mul-timed. Signal Process.* 9 (1), 177–187 .
- [30] Alyasseri, Z.A.A., Khader, A.T., Al-Betar, M.A., Papa, J.P., Ahmad Alomari, O., 2018. Eeg-based person authentication using multi-objective flower pollination algorithm. In: 2018 IEEE Congress on Evolutionary Computation (CEC). IEEE, pp. 1–8 .
- [31] Kumari, P., Vaish, A., 2016. Feature-level fusion of mental task's brain signal for an efficient identification system. *Neural Comput. Appl.* 27 (3), 659–669 .
- [32] Yousefi, F., Kolivand, H. and Baker, T., 2020. SaS-BCI: a new strategy to predict image memorability and use mental imagery as a brain-based biometric authentication. *Neural Computing and Applications*, pp.1-15.
- [33] Armstrong, B.C., Ruiz-Blondet, M.V., Khalifian, N., Kurtz, K.J., Jin, Z. and Laszlo, S., 2015. Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics. *Neurocomputing*, 166, pp.59-67.
- [34] Patel, V.; Burns, M.; Chandramouli, R.; Vinjamuri, R. Biometrics based on hand synergies and their neural representations. *IEEE Access* 2017, 5, 13422–13429.
- [35] Mu, Z., Hu, J. and Min, J., 2016. EEG-based person authentication using a fuzzy entropy-related approach with two electrodes. *Entropy*, 18(12), p.432.
- [36] Abo-Zahhad, M.; Ahmed, S.M.; Abbas, S.N. A new multi-level approach to eeg based human authentication using eye blinking. *Pattern Recognit. Lett.* 2016, 82, 216–225.
- [37] Neupane, A., Satvat, K., Hosseini, M. and Saxena, N., 2019, August. Brain hemorrhage: When brainwaves leak sensitive medical conditions and personal information. In 2019 17th International Conference on Privacy, Security and Trust (PST) (pp. 1-10). IEEE.

- [38] Fingelkurts, A.A., Fingelkurts, A.A., Ermolaev, V.A. and Kaplan, A.Y., 2006. Stability, reliability and consistency of the compositions of brain oscillations. *International Journal of Psychophysiology*, 59(2), pp.116-126.
- [39] Baldassarre, L., Pontil, M. and Mourão-Miranda, J., 2017. Sparsity is better with stability: Combining accuracy and stability for model selection in brain decoding. *Frontiers in neuroscience*, 11, p.62.
- [40] Akilli, M. and Yilmaz, N., 2018. Study of weak periodic signals in the EEG signals and their relationship with postsynaptic potentials. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 26(10), pp.1918-1925.
- [41] Vink, J.J., Klooster, D.C., Ozdemir, R.A., Westover, M.B., Pascual-Leone, A. and Shafi, M.M., 2020. EEG functional connectivity is a weak predictor of causal brain interactions. *Brain topography*, 33(2), pp.221-237.
- [42] Kevric, J. and Subasi, A., 2017. Comparison of signal decomposition methods in classification of EEG signals for motor-imagery BCI system. *Biomedical Signal Processing and Control*, 31, pp.398-406.
- [43] Wang, X., Gong, G., Li, N. and Ma, Y., 2016. A survey of the BCI and its application prospect. In *Theory, Methodology, Tools and Applications for Modeling and Simulation of Complex Systems* (pp. 102-111). Springer, Singapore.
- [44] Faundez-Zanuy, M., 2006. Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, 21(6), pp.15-26.
- [45] Rabuzin, K., Baca, M. and Sajko, M., 2006, August. E-learning: Biometrics as a Security Factor. In *Computing in the Global Information Technology, 2006. ICCGI'06. International Multi-Conference on* (pp. 64-64). IEEE.
- [46] Miller, B., 1994. Vital signs of identity [biometrics]. *IEEE spectrum*, 31(2), pp.22-30.
- [47] Agrafioti, F., Bui, F.M. and Hatzinakos, D., 2009, September. Medical biometrics: The perils of ignoring time dependency. In *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems* (pp. 1-6). IEEE.
- [48] Jaiswal, S., Bhadauria, S.S. and Jadon, R.S., 2011. Biometric: case study. *International Journal of Global Research in Computer Science (UGC Approved Journal)*, 2(10), pp.19-48.
- [49] S. R. M. Prasanna, S. K. Sahoo, and T. Choubisa, "Multimodal biometric person authentication: A review," *IETE Tech. Rev.*, vol. 29, no. 1, pp. 54–75, 2012.
- [50] Bubeck, D.S.U. and Sanchez, D., 2003. *Biometric Authentication*. Universidade Estadual de San Diego.
- [51] Jorgensen, Z. and Yu, T., 2011, March. On mouse dynamics as a behavioral biometric for authentication. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 476-482).
- [52] El-Abed, M., Giot, R., Hemery, B. and Rosenberger, C., 2010, October. A study of users' acceptance and satisfaction of biometric systems. In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology* (pp. 170-178). IEEE.
- [53] Li, R., Tang, D., Huang, B. and Li, W., 2012, March. How Many Samples Does Convincible Performance Evaluation of a Biometric System Need?. In *2012 International Symposium on Biometrics and Security Technologies* (pp. 23-26). IEEE.
- [54] Sulong, A. and Siddiqi, M.U., 2009, March. Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network. In *2009 5th International Colloquium on Signal Processing & Its Applications* (pp. 151-155). IEEE.
- [55] Revett, K., Deravi, F. and Sirlantzis, K., 2010, September. Biosignals for user authentication-towards cognitive biometrics?. In *2010 International Conference on Emerging Security Technologies* (pp. 71-76). IEEE.
- [56] Matyas, V. and Riha, Z., 2003. Toward reliable user authentication through biometrics. *IEEE Security & Privacy*, 1(3), pp.45-49.

- [57] Sauro, J. and Lewis, J.R., 2016. Quantifying the user experience: Practical statistics for user research. Morgan Kaufmann.
- [58] Neustadter, E., Mathiak, K. and Turetsky, B.I., 2016. EEG and MEG Probes of Schizophrenia Pathophysiology. In *The Neurobiology of Schizophrenia* (pp. 213-236).
- [59] Roux, F. and Uhlhaas, P.J., 2014. Working memory and neural oscillations: alpha–gamma versus theta–gamma codes for distinct WM information? *Trends in cognitive sciences*, 18(1), pp.16-25.
- [60] Millet, D., 2002, June. The origins of EEG. In *7th Annual Meeting of the International Society for the History of the Neurosciences (ISHN)*.
- [61] Haas, L.F., 2003. Hans berger (1873–1941), richard caton (1842–1926), and electroencephalography. *Journal of Neurology, Neurosurgery & Psychiatry*, 74(1), pp.9-9.
- [62] Balasubramanian, G., Kanagasabai, A., Mohan, J. and Seshadri, N.G., 2018. Music induced emotion using wavelet packet decomposition—An EEG study. *Biomedical Signal Processing and Control*, 42, pp.115-128.
- [63] Niedermeyer, E. and da Silva, F.L. eds., 2005. *Electroencephalography: basic principles, clinical applications, and related fields*. Lippincott Williams & Wilkins.
- [64] Catarino, A., Churches, O., Baron-Cohen, S., Andrade, A. and Ring, H., 2011. Atypical EEG complexity in autism spectrum conditions: a multiscale entropy analysis. *Clinical neurophysiology*, 122(12), pp.2375-2383.
- [65] Blinowska, K. and Durka, P., 2006. *Electroencephalography (eeg)*. Wiley encyclopedia of biomedical engineering.
- [66] Harris, A., 2006. Brainwaves. *Acta Neuropsychiatrica*, 18(6), pp.234-235.
- [67] Korde, K.S. and Paikrao, P.L., 2018. Analysis of EEG signals and biomedical changes due to meditation on brain: a review. *International Research Journal of Engineering and Technology*, 5(1), pp.603-606.
- [68] Vallabhaneni, A., Wang, T. and He, B., 2005. Brain—computer interface. In *Neural engineering* (pp. 85-121). Springer, Boston, MA.
- [69] Rao, R.P. and Scherer, R., 2010. Brain-computer interfacing [in the spotlight]. *IEEE Signal Processing Magazine*, 27(4), pp.152-150.
- [70] Bi, L., Fan, X.A. and Liu, Y., 2013. EEG-based brain-controlled mobile robots: a survey. *IEEE transactions on human-machine systems*, 43(2), pp.161-176.
- [71] Van Erp, J., Lotte, F. and Tangermann, M., 2012. Brain-computer interfaces: beyond medical applications. *Computer*, 45(4), pp.26-34.
- [72] Hsu, W.Y., 2011. Continuous EEG signal analysis for asynchronous BCI application. *International journal of neural systems*, 21(04), pp.335-350.
- [73] Corralejo, R., Hornero, R. and Álvarez, D., 2011, June. A domotic control system using Brain-Computer Interface (BCI). In *International Work-Conference on Artificial Neural Networks* (pp. 345-352). Springer, Berlin, Heidelberg.
- [74] Abhang, P.A., Gawali, B. and Mehrotra, S.C., 2016. *Introduction to EEG-and speech-based emotion recognition*. Academic Press.
- [75] Palmiini, A., 2006. The concept of the epileptogenic zone: a modern look at Penfield and Jasper's views on the role of interictal spikes. *Epileptic disorders*, 8(2), pp.10-15.
- [76] Mills, K.R., 2005. The basics of electromyography. *Journal of Neurology, Neurosurgery & Psychiatry*, 76(suppl 2), pp.ii32-ii35.
- [77] Bryn Farnsworth, 2020 Top 14 EEG Hardware Companies [Ranked], Available at: <https://imotions.com/blog/top-14-eeg-hardware-companies-ranked/> (Accessed: 28/07/2020).

- [78] Petrov, B.B., Stamenova, E.D. and Petrov, N.B., 2016, September. Brain-computer interface as internet of things device. In Scientific Conference Electronics (ET), International (pp. 1-4). IEEE.
- [79] EMOTIV, 2020 Emotiv EPOC +, Available at: <https://www.emotiv.com/epoc/> (Accessed: 09/07/2020).
- [80] Khalid, M.B., Rao, N.I., Rizwan-i-Haque, I., Munir, S. and Tahir, F., 2009, February. Towards a brain computer interface using wavelet transform with averaged and time segmented adapted wavelets. In 2009 2nd international conference on computer, control and communication (pp. 1-4). IEEE.
- [81] Major, T.C. and Conrad, J.M., 2014, March. A survey of brain computer interfaces and their applications. In SOUTHEASTCON 2014, IEEE (pp. 1-8). IEEE.
- [82] Tan, D. and Nijholt, A., 2010. Brain-computer interfaces and human-computer interaction. In Brain-Computer Interfaces (pp. 3-19). Springer, London.
- [83] Norani, N.M., Mansor, W. and Khuan, L.Y., 2010, November. A review of signal processing in brain computer interface system. In Biomedical Engineering and Sciences (IECBES), 2010 IEEE EMBS Conference on (pp. 443-449). IEEE.
- [84] Bin, G., Gao, X., Yan, Z., Hong, B. and Gao, S., 2009. An online multi-channel SSVEP-based brain-computer interface using a canonical correlation analysis method. *Journal of neural engineering*, 6(4), p.046002.
- [85] Lee, P.L., Sie, J.J., Liu, Y.J., Wu, C.H., Lee, M.H., Shu, C.H., Li, P.H., Sun, C.W. and Shyu, K.K., 2010. An SSVEP-actuated brain computer interface using phase-tagged flickering sequences: a cursor system. *Annals of biomedical engineering*, 38(7), pp.2383-2397.
- [86] Mallick, A. and Kapgate, D., 2015. A review on signal pre-processing techniques in brain computer interface. *Int J Comput Technol*, 2(4), pp.130-134.
- [87] Peterson, D.A., Knight, J.N., Kirby, M.J., Anderson, C.W. and Thaut, M.H., 2005. Feature selection and blind source separation in an EEG-based brain-computer interface. *EURASIP Journal on Advances in Signal Processing*, 2005(19), p.218613.
- [88] Yamaguchi, T., Nagata, K. and Truong, P.Q., 2007, September. Pattern recognition of EEG signal during motor imagery by using SOM. In *icicic* (p. 121). IEEE.
- [89] Y. Bian, L. Zhao, H. Li, G. Yang, H. Shen, Q. Meng, "Research on Brain Computer Interface Technology Based on Steady State Visual Evoked Potentials, Proceedings of the IEEE on Bioinformatics and Biomed. Eng., pp I - 4, 2010
- [90] Kousarrizi, M.R.N., Ghanbari, A.A., Teshnehlab, M., Shorehdeli, M.A. and Gharaviri, A., 2009, August. Feature extraction and classification of EEG signals using Wavelet transform, SVM and artificial neural networks for brain computer interfaces. In 2009 international joint conference on bioinformatics, systems biology and intelligent computing (pp. 352-355). IEEE.
- [91] McFarland, D.J., Anderson, C.W., Muller, K.R., Schlogl, A. and Krusienski, D.J., 2006. BCI meeting 2005-workshop on BCI signal processing: feature extraction and translation. *IEEE transactions on neural systems and rehabilitation engineering*, 14(2), pp.135-138.
- [92] Abuhashish, F.A., Sunar, M.S., Kolivand, H., Mohamed, F. and Mohamad, D.B., 2014. Feature extracted classifiers based on eeg signals: a survey. *Life Science Journal*, 11(4).
- [93] Duin, R.P. and Tax, D.M.J., 2005. Statistical pattern recognition. In *Handbook of Pattern Recognition and Computer Vision* (pp. 3-24).
- [94] Pal, S.K. ed., 1992. Fuzzy models for pattern recognition: methods that search for structures in data. Institute of Electrical & Electronics Engineers (IEEE).
- [95] Breiman, L., 1998. Arcing classifier (with discussion and a rejoinder by the author). *The annals of statistics*, 26(3), pp.801-849.

- [96] Lotte, F., 2006, September. The use of fuzzy inference systems for classification in EEG-based brain-computer interfaces. In 3rd International Brain-Computer Interfaces Workshop and Training Course.
- [97] Abdulkader, S.N., Atia, A. and Mostafa, M.S.M., 2015. Brain computer interfacing: Applications and challenges. *Egyptian Informatics Journal*, 16(2), pp.213-230.
- [98] Jain, A.K., Ross, A. and Prabhakar, S., 2004. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), pp.4-20.
- [99] Marasco, E. and Ross, A., 2014. A survey on antispooofing schemes for fingerprint recognition systems. *ACM Computing Surveys (CSUR)*, 47(2), pp.1-36.
- [100] Cao, K. and Jain, A.K., 2016. Hacking mobile phones using 2D printed fingerprints. Michigan State University, Tech. Rep. MSU-CSE-16-2.
- [101] Kubitschko, S., 2015. Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence*, 21(3), pp.388-402.
- [102] Wijdicks, E.F., 1995. Determining brain death in adults. *Neurology*, 45(5), pp.1003-1011.
- [103] Trokielewicz, M., Czajka, A. and Maciejewicz, P., 2016, June. Post-mortem human iris recognition. In 2016 International Conference on Biometrics (ICB) (pp. 1-6). IEEE.
- [104] Jain, A., Bolle, R. and Pankanti, S. eds., 1999. *Biometrics: personal identification in networked society (Vol. 479)*. Springer Science & Business Media.
- [105] Riera, A., Dunne, S., Cester, I. and Ruffini, G., 2008, May. STARFAST: A wireless wearable EEG/ECG biometric system based on the ENOBIO sensor. In Proceedings of the international workshop on wearable micro and nanosystems for personalised health.
- [106] Jayarathne, I., Cohen, M. and Amarakeerthi, S., 2016, October. BrainID: Development of an EEG-based biometric authentication system. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual (pp. 1-6). IEEE.
- [107] Yeom, S.K., Suk, H.I. and Lee, S.W., 2013. Person authentication from neural activity of face-specific visual self-representation. *Pattern Recognition*, 46(4), pp.1159-1169.
- [108] Luck, S.J., 2014. *An introduction to the event-related potential technique*. MIT press..
- [109] Marcel, S. and Millán, J.D.R., 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE transactions on pattern analysis and machine intelligence*, 29(4), pp.743-752.
- [110] Chuang, J., Nguyen, H., Wang, C. and Johnson, B., 2013, April. I think, therefore I am: Usability and security of authentication using brainwaves. In International conference on financial cryptography and data security (pp. 1-16). Springer, Berlin, Heidelberg.
- [111] Kumari, P. and Vaish, A., 2016. Feature-level fusion of mental task's brain signal for an efficient identification system. *Neural Computing and Applications*, 27(3), pp.659-669.
- [112] Clark, J.M. and Paivio, A., 1987. A dual coding perspective on encoding processes. In *Imagery and related mnemonic processes* (pp. 5-33). Springer, New York, NY.
- [113] Nelson, D.L., Cermak, L. and Craik, F., 1979. Remembering pictures and words: Appearance, significance and name. *Levels of processing in human memory*, pp.45-76.
- [114] Pearson, J., 2019. The human imagination: the cognitive neuroscience of visual mental imagery. *Nature Reviews Neuroscience*, 20(10), pp.624-634.
- [115] Slotnick, S.D., Thompson, W.L. and Kosslyn, S.M., 2012. Visual memory and visual mental imagery recruit common control and sensory regions of the brain. *Cognitive neuroscience*, 3(1), pp.14-20.

- [116] Sooriyaarachchi, J., Seneviratne, S., Thilakarathna, K. and Zomaya, A.Y., 2020. MusicID: A brainwave-based user authentication system for internet of things. *IEEE Internet of Things Journal*, 8(10), pp.8304-8313.
- [117] Komori, T., 2018. Extreme prolongation of expiration breathing: Effects on electroencephalogram and autonomic nervous function. *Mental illness*.
- [118] Stassen, H. H., G. Bomben, and P. Propping. "Genetic aspects of the EEG: an investigation into the within-pair similarity of monozygotic and dizygotic twins with a new method of analysis." *Electroencephalography and clinical neurophysiology* 66, no. 6 (1987): 489-501.
- [119] Poulos, M., Rangoussi, M. and Alexandris, N., 1999, March. Neural network based person identification using EEG features. In *Acoustics, Speech, and Signal Processing, IEEE International Conference on* (Vol. 2, pp. 1117-1120). IEEE Computer Society.
- [120] Poulos, M., Rangoussi, M., Alexandris, N. and Evangelou, A., 2002. Person identification from the EEG using nonlinear signal classification. *Methods of information in Medicine*, 41(01), pp.64-75.
- [121] Van Beijsterveldt, C.E.M. and Van Baal, G.C.M., 2002. Twin and family studies of the human electroencephalogram: a review and a meta-analysis. *Biological psychology*, 61(1-2), pp.111-138.
- [122] Thorpe, J., Van Oorschot, P.C. and Somayaji, A., 2005, September. Pass-thoughts: authenticating with our minds. In *Proceedings of the 2005 workshop on New security paradigms* (pp. 45-56).
- [123] Wang, M., Hu, J. and Abbass, H.A., 2020. BrainPrint: EEG biometric identification based on analyzing brain connectivity graphs. *Pattern Recognition*, 105, p.107381.
- [124] Piplani, T., Merrill, N. and Chuang, J., 2018, October. Faking it, making it: fooling and improving brain-based authentication with generative adversarial networks. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)* (pp. 1-7). IEEE.
- [125] Abo-Zahhad, M., Ahmed, S.M. and Abbas, S.N., 2015. State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. *IET Biometrics*, 4(3), pp.179-190.
- [126] Ashby, C., Bhatia, A., Tenore, F. and Vogelstein, J., 2011, April. Low-cost electroencephalogram (EEG) based authentication. In *2011 5th International IEEE/EMBS Conference on Neural Engineering* (pp. 442-445). IEEE.
- [127] Campisi, P. and La Rocca, D., 2014. Brain waves for automatic biometric-based user recognition. *IEEE transactions on information forensics and security*, 9(5), pp.782-800.
- [128] EMOTIV. (n.d.). EMOTIV EPOC+ 14 Channel Mobile Brainwear®. [online] Available at: <https://www.emotiv.com/product/emotiv-epoc-14-channel-mobile-eeeg/#tab-description> (Accessed 20 Jun. 2022).
- [129] Arnaud Delorme, 2018 EEG Pre-processing: Visualizing Data, Available at: <https://www.youtube.com/watch?v=SgQxdVgryVY> (Accessed: 18/07/2020).
- [130] Hyvärinen, A. and Oja, E., 2000. Independent component analysis: algorithms and applications. *Neural networks*, 13(4-5), pp.411-430.
- [131] Al-Fahoum, A.S. and Al-Fraihat, A.A., 2014. Methods of EEG signal features extraction using linear analysis in frequency and time-frequency domains. *International Scholarly Research Notices*, 2014.
- [132] Pfurtscheller, G., & Neuper, C. (2002). Motor imagery and direct brain-computer communication. *Proceedings of the IEEE*, 89 (7), 1123-1134. doi: 10.1109/5.939829
- [133] Pfurtscheller, G., and da Silva, L. "Event-related EEG/MEG synchronizaion and desynchronization: basic principles." *Clin Neurophysiol* 110 (1999), 1842-1857.
- [134] McFarland, D., McCane, L., David, S., & Wolpaw, J. (1997). Spatial filter selection for EEG-based communication. *Electroencephalogram Clinical Neurophysiology*, 103 (3), 386-394.

- [135] Übeyli, E.D., 2008. Wavelet/mixture of experts network structure for EEG signals classification. *Expert systems with applications*, 34(3), pp.1954-1962.
- [136] Kumar, Y., Dewal, M.L. and Anand, R.S., 2014. Epileptic seizure detection using DWT based fuzzy approximate entropy and support vector machine. *Neurocomputing*, 133, pp.271-279.
- [137] Li, M., Chen, W. and Zhang, T., 2017. Classification of epilepsy EEG signals using DWT-based envelope analysis and neural network ensemble. *Biomedical Signal Processing and Control*, 31, pp.357-365.
- [138] Faust, O., Acharya, U.R., Adeli, H. and Adeli, A., 2015. Wavelet-based EEG processing for computer-aided seizure detection and epilepsy diagnosis. *Seizure*, 26, pp.56-64.
- [139] Wayman, J.L., 1996. Technical testing and evaluation of biometric identification devices. In *Biometrics* (pp. 345-368). Springer, Boston, MA.
- [140] Neto, E., Biessmann, F., Aurlien, H., Nordby, H. and Eichele, T., 2016. Regularized linear discriminant analysis of EEG features in dementia patients. *Frontiers in aging neuroscience*, 8, p.273.
- [141] Savan Patel (2017) SVM (Support Vector Machine)—Theory, Available at: <https://medium.com/machine-learning-101/chapter-2-svm-support-vector-machine-theory-f0812effc72> (Accessed: 29/08/2020).
- [142] Hasenauer, J., Heinrich, J., Doszczak, M., Scheurich, P., Weiskopf, D. and Allgöwer, F., 2012. A visual analytics approach for models of heterogeneous cell populations. *EURASIP Journal on Bioinformatics and Systems Biology*, 2012(1), pp.1-13.
- [143] Sejdic, E. and Falk, T.H. eds., 2018. *Signal Processing and Machine Learning for Biomedical Big Data*. CRC press.
- [144] Miyamoto, C., Baba, S. and Nakanishi, I., 2009, February. Biometric person authentication using new spectral features of electroencephalogram (EEG). In *2008 international symposium on intelligent signal processing and communications systems* (pp. 1-4). IEEE.
- [145] Nakanishi, I., Baba, S. and Miyamoto, C., 2009, January. EEG based biometric authentication using new spectral features. In *2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)* (pp. 651-654). IEEE.
- [146] Rathinavel, S. and Arumugam, S., 2011. Full shoe print recognition based on pass band DCT and partial shoe print identification using overlapped block method for degraded images. *International Journal of Computer Applications*, 26(8), pp.16-21.
- [147] Gunn, S.R., 1998. Support vector machines for classification and regression. *ISIS technical report*, 14(1), pp.5-16.
- [148] Guo, L., Rivero, D., Dorado, J., Munteanu, C.R. and Pazos, A., 2011. Automatic feature extraction using genetic programming: An application to epileptic EEG classification. *Expert Systems with Applications*, 38(8), pp.10425-10436.
- [149] Panda, R., Khobragade, P.S., Jambhule, P.D., Jengthe, S.N., Pal, P.R. and Gandhi, T.K., 2010, December. Classification of EEG signal using wavelet transform and support vector machine for epileptic seizure detection. In *2010 International conference on systems in medicine and biology* (pp. 405-408). IEEE.
- [150] Benzy, V. K., and E. A. Jasmin. "A Combined Wavelet and Neural Network Based Model for Classifying Depth of Anaesthesia." *Procedia Computer Science* 46 (2015): 1610-1617.
- [151] De Jesús Rubio, J., 2009. SOFMLS: online self-organizing fuzzy modified least-squares network. *IEEE Transactions on Fuzzy Systems*, 17(6), pp.1296-1309.
- [152] De Jesús Rubio, J., 2017. USNFIS: uniform stable neuro fuzzy inference system. *Neurocomputing*, 262, pp.57-66.
- [153] Gui, Q., Jin, Z. and Xu, W., 2014, December. Exploring EEG-based biometrics for user identification and authentication. In *2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)* (pp. 1-6). IEEE.