BIUST

BOTSWANA INTERNATIONAL UNIVERSITY
OF SCIENCE & TECHNOLOGY

EEG Human Biometric Authentication Using Eye Blink Artefacts

by

THAMANG TEDDY MADILE

Reg. No: 16100741

BSc (Computer Systems Engineering)

University of Sunderland

Department of Computer Science and Information Systems,

Faculty of Science,

Botswana International University of Science and Technology

thamang.madile@studentmail.biust.ac.bw

(+267) 71897004

A Dissertation/Thesis Submitted to the College of ICT in Partial Fulfilment of the Requirements for the Award of the Degree of Master of Science in Computer Science of BIUST

Supervisor(s): Dr. Hlomani Hlomani

Department of Computer Science and Information Systems,

Faculty of Science, BIUST

E-mail Address, Phone Number including the code (+267 4931107)

Signature: H.B. Hlomani Date: 01/03/2021

Declaration and Copyright

I, **Thamang Teddy Madile** declare that this dissertation/thesis is my own original work and that it has not been presented and will not be presented to any other university for a similar or any other degree award.

Signature T. MADILE………………………………

Certification by Supervisor(s)

The undersigned certifies that he/she has read and hereby recommends for acceptance by the College of … a dissertation/thesis titled**: EEG Human Biometric Authentication Using Eye Blink Artefacts,** in fulfilment of the requirements for the degree of Master of Science (*Programme of Study*) of the BIUST.

H. B. Hlomani
………………………………

Dr. Hlomani Hlomani

(Supervisor)

Date: 01/03/2021

Acknowledgements

I would like to extend my heartfelt gratitude to my supportive family for their valuable contribution in advising and encouraging me to stay focused on my research work. I thank my wife, Kitso A. Madile, for her love, for it was through her love that I found a great source of motivation and enthusiasm to finish this research work.

I would also like to exhibit my deepest gratitude to Dr Hlomani Hlomani, my supervisor, who had tremendous input in the progression of my research through his guidance. Also, through his suggestions and directions in designing experiments. I thank all participants who availed themselves and took part in the experiments that were conducted. Also, I thank my friends and colleagues who shared the same goal. They offered opinions that had a significant impact on overcoming obstacles in completing this work.

Above all, I would like to humble myself and acknowledge the power and greatness of the all mighty God, for granting me the grace to finish this work, may he continue to reign over my life and bless the work of my hands.

Table of Contents

Cover Page i

Declaration and Copyright ii

Certification by Supervisor(s) iii

Acknowledgements iv

Table of Contents v

List of Abbreviations ix

List of Figures x

List of Tables xii

List of Equations xiii

Abstract xiv

Chapter 1. Introduction 1

1.0 Overview 1

1.1 Introduction 1

1.2 Background to the problem 2

1.3 Problem Statement 4

1.4 Objectives 4

1.4.0 General Objective 4

1.4.1 Specific Objectives 4

1.5 Research Questions 4

1.6 Thesis Structure 5

Chapter 2. Literature Review 6

2.0 Overview 6

2.1 Electroencephalogram 6

2.1.0 Introduction to EEG 6

2.1.1 Practical uses of EEG 7

2.1.2 EEG Measurement 8

2.2 Eye Blink 10

2.3 EEG devices 11

2.3.0 Emotiv Epoc+ 11

2.3.1 NeuroSky Mindwave Mobile 2 11

2.3.2 Emotiv Insight 12

2.3.3 Muse Headband 2016 12

2.3.4 Summary of EEG Devices 13

2.4 EEG Authentication 14

Chapter 3. Proposed Approach 23

3.0 Introduction 23

3.1 Overview 23

3.2 EEG Data Collection 24

3.2.0 Minimising Electrode Impedance 24

3.2.1 Signal Extraction 25

3.2.2 Signal Recording 26

3.3 EEG Signal Pre-processing 27

3.3.0 Low-Pass Filter 27

3.3.1 High-Pass Filter 27

3.3.2 Notch Filter 27

3.4 Feature Extraction 28

3.5 Proposed Authentication Algorithm 30

3.5.0 Overview 30

3.5.1 Algorithm Description 30

3.5.2 Pattern Matching Algorithm 32

3.6 Summary 38

Chapter 4. Experimental Setup 40

4.0 Introduction 40

4.1 Performance Metrics 40

4.2 Performance Evaluation: FRR 41

4.2.0 Briefing of Subjects 42

4.2.1 Giving Instructions 42

4.2.2 EEG Headset Installation On The Subject 43

4.2.3 Enrolling Subjects 44

4.2.4 Demonstration of Pattern Formation 45

4.2.5 Training Subjects 46

4.2.6 Authentication 48

4.3 Performance Evaluation: FAR 48

4.3.0 True Subject Authentication 49

4.3.1 Impostor Observation 49

4.3.2 Impostor Authentication 50

4.4 Effect of Emotions on Our Proposed Approach Experiment 50

4.4.0 Experimental Setup 51

4.5 Effect of Exercise on Our Proposed Approach Experiment 53

4.5.0 Experimental Setup 54

Chapter 5. Results & Discussion 57

5.0 Introduction 57

5.1 Performance Results 57

5.2 Effect of Emotions Results 62

5.3 Effect of Exercise Results 64

5.4 Summary 65

6.0 Conclusion & Further Work 66

6.1 Conclusion 66

6.2 Further Work 68

References 69

Appendix A 76

Appendix B 78

Appendix C 80

List of Abbreviations

AR	Auto-regressive coefficients
BCI	Brain-Computer Interface
COH	Cross-spectral Coherence
CSP	Common Spatial Patterns
DDL	Data Definition Language
EEG	Electroencephalography
ENN	Elman Neural Network
EOG	Electro-oculography
ERP	Event-Related Potentials
FAR	False Acceptance Rate
FRNN	Fuzzy-Rough Nearest Neighbour
FRR	False Rejection Rate
IHLC	Inter-Hemispheric Linear Complexity
IHPD	Inter-Hemispheric Power Difference
KNN	K-nearest Neighbour
LDA	Linear Discriminant Analysis
LVQ	Learning Vector Quantisation
MOFPA - WT	Multi-Objective Flower Pollination Algorithm Based on Wavelet Transform
PSD	Power Spectral Density
RAM	Random Access Memory
RSVP	Rapid Serial Visual Representation
SP	Spectral Power
SVM	Support Vector Machine

List of Figures

Figure 1. EEG controlled drone [29]..8

Figure 2. 10/20 International Position System for measuring EEG [32]..9

Figure 3. Brainwave signal showing an eye blink. 10

Figure 4. Emotive Epoc+ [34]...11

Figure 5. NeuroSky Mindwave Mobile 2 [35] 12

Figure 6. Emotiv Insight 5 Channel Mobile EEG [36] 12

Figure 7. Left(Muse Headband), right(electrode positioning according to 10/20 system) [15] 13

Figure 8. An overview of the proposed approach (EEG Authentication Algorithm) 24

Figure 9. Electrode site position (Fp1 and left ear lobe) to be cleaned [59]...25

Figure 10. Extracting the blink strength value from the tgPaser dictionary object 29

Figure 11. A custom function used to extract soft, normal & hard blink features..30

Figure 12. Capturing and recording data at the enrolment phase...31

Figure 13. Capturing, recording, and matching data at the authentication phase. 31

Figure 14. Pseudocode for the proposed pattern matching algorithm..32

Figure 15. Code snippet for matching blink number...33

Figure 16. Code snippet for the function that validates a given range of values...34

Figure 17. Pseudocode for blink time matching algorithm. 35

Figure 18. Code snippet for blink time matching algorithm...36

Figure 19. Pseudocode for blink strength matching algorithm...37

Figure 20. Code snippet for blink strength matching algorithm. 38

Figure 21. Experimental setup flowchart for evaluating FRR. 42

Figure 22. Headset installation position [62]...43

Figure 23. NeuroSky Mind Wave mobile Bluetooth connection results. 44

Figure 24. Registration Form for Capturing Basic Details...44

Figure 25. Demonstration of Pattern Formation..45

Figure 26. Important Sections of the System. 46

Figure 27. Experiment 2 flowchart for evaluating FAR...49

Figure 28. Emotion analysis 2D model [52]. 50

Figure 29. A flowchart for the effect of emotions experiment. 52
Figure 30. Flow chart for the effect of exercising experiment. 54
Figure 31. M3 Smart Bracelet Fitness Tracker (left) and FitPro App (right) 56
Figure 32. Authentication algorithm results (summary) 59
Figure 33. Subjects authentication results after exercise 64
Figure 34. DEAP dataset application form. 76
Figure 35. DEAP dataset request approval. 77
Figure 36. Experiment session timeline..87

List of Tables

Table 1. Summary of widely used EEG devices. 13

Table 2. Summary of related EEG authentication studies 20

Table 3. Description of EEG data received from NeuroSky Mindwave Mobile 2. 28

Table 4. A summary of the fundamental components of performance metrics. 40

Table 5. Heartrate results after the robe skipping exercise 55

Table 6. Authentication algorithm results 58

Table 7. Performance metric results (TP, FN, FP, TN) 60

Table 8. Performance metric results (FAR, FRR & ACC) 61

Table 9. Mean performance metric results (FAR, FRR & ACC) 61

Table 10. Authentication results for excited, sadness, and calm emotions 62

List of Equations

(1) 34
(2) 35
(3) 36
(4) 37
(5) 41
(6) 41
(7) 41
(8) 41
(9) 41
(10) 55

Abstract

This study proposes a new electroencephalography (EEG) biometric authentication for humans based on eye blinking signals extracted from brainwaves. The brainwave signal has been investigated for person authentication over the years because of its difficulties in spoofing. Due to advancing low-cost EEG hardware equipment, it has recently been significantly explored. Most studies in brainwave authentication focus on the use of imagination and mental task to authenticate a subject. Such conventional approaches are prone to the effect of human emotions and exercising, since this effect alters the brainwave signal significantly, making such approaches to be less practical in the real world. This study overcomes this limitation by introducing a new approach, where the effect of eye blinks on the brainwave is used for authentication. The eye blink effect on the brainwave signal is considered an artefact in EEG authentication and is usually removed at the pre-processing stage. However, it holds properties that are ideal for use in authentication, and it is not prone to human emotions and exercising, thus improving the practicality of brainwave authentication. Brainwaves were recorded using Neurosky Mindwave Mobile 2 headset. The NeuroSky blink detection algorithm was used to extract eye blinks and their properties from the brainwaves. A new authentication algorithm is developed based on three (3) properties: blink strength, blink time, and the number of blinks at a given time. The proposed authentication algorithm matches the eye blinking properties stored in a database at the enrolment stage against the one recorded at the authentication stage. The overall algorithm results were calculated on a range of 0 – 100. A threshold value of 70 was used to authenticate a subject. Three (3) experiments were conducted. In the first experiment, we evaluated the performance of the proposed algorithm. The second experiment evaluated the effect of emotions (Excitement, Calmness and Stress) on the proposed algorithm. The third experiment evaluated the effect of exercising on the proposed algorithm. The performance of the algorithm is measured using False Rejection Rate (FRR), False Acceptance Rate (FAR), and Accuracy (ACC). Results showed a FAR value of 5% and an FRR value of 1%. The proposed algorithm achieved an accuracy of 97%. These results show good performance. Results also indicate that more complex patterns have low FAR and high FRR, while less complicated patterns have high FAR and low FRR. Results also show that human emotions and exercising have no significant impact on the proposed approach.

Chapter 1. Introduction

1.0 Overview

This chapter outlines a brief overview of this research. The chapter entails the introduction, background to the problem, problem statement, objectives, and hypothesis/research questions. The last section of this chapter presents a short description of how the rest of the document is organised.

1.1 Introduction

Electroencephalography (EEG) is the electrical recording and the measuring of brain activity from the surface of the head of an individual using electrodes. The measurement depicts a summation of the small electrical impulses produced by the brain's neurons [1]. EEG devices are used to measure these electrical impulses through sensors (electrodes) attached to an individual's head. The acquired EEG signal will then be forwarded to a computer system for processing. EEG forms the core of Brain-Computer Interface (BCI) technologies, and it is applied in various fields, including gaming [2], medical applications [3], and assisting disabled people [4]. EEG has also been used in biometric human authentication [5].

Biometrics is the statistical analysis and measurement of a person's distinct behavioural, physiological, biological, and structural characteristics [6]. It has been used over a long period for identification and authentication purposes. EEG has been used in person authentication and recognition field [1], [5], [7], [8], [9] as a form of human biometric, and it has attracted much interest because of its low likelihood of being replicated or fabricated. It has some security advantages over the conventional biometric modalities. For example, handwriting may be mimicked, and voice can be recorded, face and iris information can be photographed [10].

Authentication involves a process by which the identity claimed by a particular individual is accepted or rejected. It is a one-to-one matching. In contrast, identification intends to give the identity of a particular individual out of a group of people, therefore making it a one-to-N matching. Blinking is a semi autonomic process of opening and closing of eyelids in a given short period. It is generally regarded as an artefact when extracting specific data from the

EEG signal. Interior brain activities are known to be linked to eye blinks [11]. When an eye blink occurs, the eyeball rotates in its axes, generating an electric signal of high amplitude.

Eye blinks are visible in the brainwave signal as an EEG artefact and get recorded together via EEG devices like NeuroSky Mindwave. The advancement of technology has made such EEG devices cheap, small, portable, and wearable, making them more practical for use in various fields, including EEG authentication. EEG human biometric authentication using eye blink artefacts, involves a process where eye blinks extracted from the EEG signal are used to identify a particular individual using EEG devices. Such a process includes an enrolment stage where the EEG signal is recorded and stored, then later during authentication, the signal is recorded and matched using pattern matching algorithms, against the one previously stored.

Using biometrics for authentication or person recognition requires measurable behavioural or physical attributes that meet the following aspects: distinctiveness, circumvention, universality, collectability, acceptability, permanence, and performance [12]. EEG signals, as a promising biometric trait, go beyond satisfying the first four aspects and is superior as compared to other biometric traits [13]. The privacy, acceptability, and non-invasiveness of this form of data acquisition make EEG based biometrics have a robust advantage of public tolerance. However, the performance and permeance of EEG based biometrics is a research area that is still being explored further [13].

1.2 Background to the problem

As discussed in Section 1.1, EEG based biometric authentication provides a high level of security as opposed to other conventional methods like fingerprint, face, iris and passwords [14]. It is also a feasible alternative to other person authentication and recognition methods. The implicit features of EEG, which are nearly impossible to forge gives it an immanent advantage[13]. Many studies [7], [15], [16], [17], [18], [19] have reported high permeance and accuracy for EEG based authentication systems. However, many of them were conducted and evaluated under a controlled environment like labs and subjects in specific mental states. These conditions are unrealistic because, in a real-life scenario, such systems would operate in an uncontrolled environment like workplaces. Also, users of these systems are generally not in the same mental state throughout the day. For this reason, these systems face significant challenges in performance when it comes to realistic conditions. In this section, we discuss the major problem surrounding EEG based authentication systems.

One of the most significant challenges in implementing an EEG based biometric system is in its operation [13]. EEG experiments are conducted in such a way that subjects participate only a few times, if not once. In reality, a biometric system is often used multiple times in a day over several years in a way that is different from the experiments conducted in laboratories. Furthermore, for a biometric system to be practical and useable, it must allow users to operate it by themselves, without requiring an operator.

A practical person identification or authentication system must be able to recognise enrolled users even after a prolonged time. [20] conducted a study on EEG based authentication system where half total error rate increased to 36.2% from 7.1% in just three days. The same trend was observed from a study by [21], where the true positive rate dropped to 83.64% from 94.60% after a single week and further dropped to 78.20% after six months. These studies indicate a template ageing challenge [22], whereby, over time, EEG based biometric system performance degrades.

Other several studies used EEG signals in authentication, but using different stimuli ranging from imaginary motor movement to baseline relaxation, solving math problems, and visualisation [15]. These studies [7], [15], [23] have something in common; they depend on a thought or an imagination that a subject creates based on a given stimulus. [24] piloted a study on the effects of familiarity on the EEG signal. In this study, music was used as stimuli, and it was discovered that music familiarity influences both the brain functional connectivity and the power spectra of brainwaves to a certain level.

[25] conducted a study to evaluate the EEG spectral asymmetry index (SASI) for discrimination of the effect of positive, neutral, and negative emotions on human EEG. Results indicated that both positive and negative evoked emotions change the EEG signal. Another study was conducted by [26] on examining the effect of moderate physical exercise on EEG. Results indicated that the amplitude of EEG power spectra, including beta, alpha, and theta frequency bands, significantly increased after exercise, and concluded that the EEG signal is altered by exercise.

As discussed, the effect of exercising and emotions on the EEG signal has a considerable negative effect on the performance of EEG based biometric systems. The performance of such systems tends to degrade under the mentioned conditions, therefore challenging their practicality and robustness. Although EEG based biometric studies report accuracies of up to 100%, they were conducted in a laboratory setup, and subjects kept at a steady position and resting conditions [27]. Furthermore, they do not provide information on the performance under practical conditions. For such systems to be practical, they need to overcome these challenges.

1.3 Problem Statement

The problem that EEG based biometric methods have lies in the effect of physiological artefacts (emotions and exercising) that alter the EEG waveform, thus increasing false rejection rate in EEG authentication systems.

1.4 Objectives

1.4.0 General Objective

The main objective of this study is to develop an EEG based human biometric authentication algorithm that is based on eye blink artefact.

1.4.1 Specific Objectives

1. To collect the EEG signal.
2. To pre-process the acquired EEG signal.
3. To extract relevant features from the EEG data.
4. To develop an authentication algorithm based on eye blink artefact.
5. To evaluate the performance of the authentication algorithm.

1.5 Research Questions

The core of this study focuses on implementing an EEG authentication algorithm based on eye blinks. Therefore, this research seeks to offer a comprehensive solution to the following research questions:

1. How can the EEG signal be collected?
2. How is the acquired EEG data pre-processed?
3. What relevant features can be extracted from the EEG signal to be used in the authentication algorithm?
4. How can eye blink artefact be used to develop an authentication algorithm?
5. How is the performance of the authentication algorithm evaluated?

1.6 Thesis Structure

There are relatively six (6) chapters in this document. The first chapter introduces our work, the background to the main problem, and the problem statement that this study is addressing. Followed by the general objective, research questions, and specific objectives. The second chapter introduces EEG, its practical use, and measurement, followed by a review of literature on EEG devices and EEG authentication methods. Chapter 3 explains in detail how the objectives discussed in chapter 1 are archived. It starts with an introduction and an overview of our proposed approach. Followed by EEG signal pre-processing methods, selection of relevant data features, and the development of the algorithm. Chapter 4 consists of the experimental setup. Chapter 5 entails results and discussion, while chapter 6 is the conclusion and further work.

Chapter 2. Literature Review

2.0 Overview

This chapter is an outline of the literature review. It entails an introduction to EEG, practical uses, and measurement of EEG, followed by a detailed description of the eye blinking process. A review of various EEG devices and EEG authentication methods follows. At the end of this chapter is a summary of the authentication methods.

2.1 Electroencephalogram

2.1.0 Introduction to EEG

Electroencephalography is the measurement of electrical activity that occurs in the brain of a human being. The nervous system of a human being, including the brain, consists of nerve cells called neurons. These so-called neurons send electrical signals amongst each other, causing some voltage fluctuations. These voltage fluctuations are then measured using some electrodes placed on the scalp. It is mostly used in the medical field though it has much potential in other fields like computer security.

The waves of EEG patterns are in sinusoidal form. They are categorised into several classes based on their frequency bandwidth. When a subject performs different activities, each category of these waves become visible. There are five commonly known categories of these waves. They are:

a) Alpha Waves

The frequency of these waves is on a range of 8Hz to 15Hz. They usually appear while the subject is in a relaxed state. More can also be observed when the subject's eyes are closed.

b) Beta Waves

The frequency of these waves is on a range of 16Hz to 31Hz. They are usually visible when a subject is awake and have a low amplitude. They are also visible during concentration, active thinking, and arousal states.

c) Gamma Waves

The frequency of these waves is above 32Hz, and they are involved during cognitive functioning like higher processing tasks, sight, and sound perception. The occurrence of lower gamma waves is found in people with disabilities.

d) Theta Waves

The theta waves range on a frequency of 4Hz to 8Hz. They appear as consciousness slips towards drowsiness.

e) Delta Waves

The delta waves range on a frequency of 1Hz to 4Hz. They are primarily associated with deep sleep.

2.1.1 Practical uses of EEG

EEG is mainly used in the medical field for inspecting the patient's brain conditions. A patient's brain death status, coma, and alertness are examples of its use in the medical field. It is also used to locate and investigate the patient's damaged areas in the brain since abnormal readings of EEG can indicate the problem from or near the affected area. Also, EEG can be used to monitor some procedures, during operations, it can measure the depth of anaesthesia. Calm brainwaves indicate that patients are in a relaxed state. The other uses involve investigating epilepsies, seizures, and test the convulsive effects of drug use.

In the medical field, the use of EEG is influenced by the advantages it has over other methods for monitoring brain function. The cost and size of EEG measuring devices are generally low, therefore making it more practical to be deployed in many hospitals and clinics. Medical settings usually use a sampling rate between 250Hz and 2000Hz, but other devices have the capability of recording at a sampling rate that is above 2000Hz. EEG does not have side effects like claustrophobia in contrast to other Magnetic Resonance Imaging (MRI).

Another field that has attracted much interest in the implementation of EEG is Brain-Computer Interface (BCI). EEG in BCI acts as a gateway between the users and computer devices through the provision of an interface that gives users the ability to interact with external devices through their brainwaves. Beyond just facilitating input commands to computer games and software, it has been implemented in drones that are remotely controlled [28],[29],[30],[31]. Figure 1 shows a quad-copter parrot 2.0 drone remotely controlled via Emotiv EEG headsets using brainwaves.

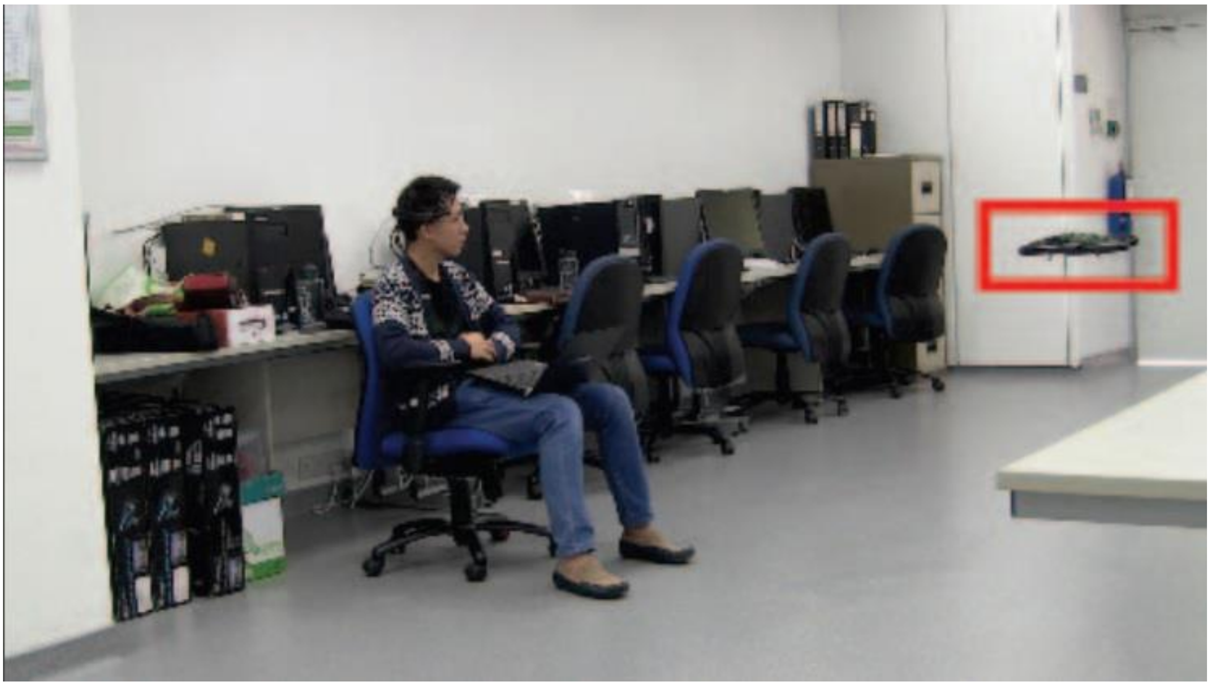


Figure 1. EEG controlled drone [29]

2.1.2 EEG Measurement

EEG is measured using EEG recording devices. These devices have electrodes that are attached to the skull to measure the electrical activity on the scalp. The electrodes are positioned in the desired points on the head. The number of these electrodes can range from 1 up to 65 or even more. Each electrode measures the electrical activity at the points they are attached to on the scalp. In the medical field, the device is generally in a cap form, with electrodes attached to it. In BCI, these devices are usually in form of electronic gadgets. EEG measurement has two main categories of recording methods. These methods are invasive and non-invasive.

a) Invasive EEG

In this method of recording, electrodes are directly embedded inside the skull but on the surface of the brain. Surgery is a required procedure in this method since the electrodes have to touch the surface of the brain. Modern EEG devices usually do not require that, unless in extreme cases where there is a need for the electrode to touch the brain like in some epilepsy surgeries.

b) Non-Invasive EEG

Unlike invasive EEG, where electrodes need to come in contact with the brain directly, non-invasive EEG only requires electrodes to touch the surface of the head. However, this makes it prone to noise from other factors, creating a need for signal filtering and signal processing. Modern EEG applications mostly use EEG devices that are non-invasive and wearable, therefore making such applications more practical. In non-invasive EEG, electrodes are placed anywhere on the surface of the head for EEG measuring. However, there are international standards that exist for placing electrodes on the surface of the head. A system named 10-20 for electrode placement is an accepted international standard. It consists of twenty-one points (21), and each point has a specific name given to it. These names are based on the brain lobes near the electrode position. For example, the electrodes paced near the frontal lobe, occipital lobe, and temporal lobe are named F, O, and T, respectively. Figure 2 indicates an international standard 10-20 system for EEG measurement. The percentages in the figure indicate the distance relative to the total distance from nasion to inion (nose to back of the skull) and preauricular to preauricular (ear to ear).

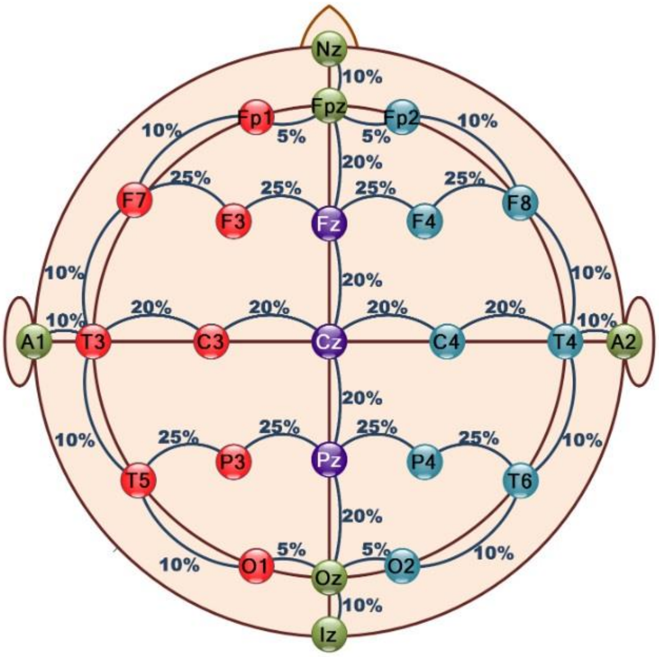


Figure 2. 10/20 International Position System for measuring EEG [32]

2.2 Eye Blink

Blinking is a process of rapid closure and opening of eyelids. It is an act that occurs involuntarily and voluntarily. According to [33], when an eye blink occurs, there is a rotation of the eyeball within its axis. This rotation causes a large amplitude of an electric signal. An eyeblink occurs in two (2) stages. In the first stage, the eyelids close while the eyeball rotates upwards, causing the cornea (positive pole) to get closer to the frontal lobe at the Fp1 electrode in the left eye. The same process happens in the right eye, where the cornea gets close to the Fp2 electrode. A positive deflection in the signal is produced by this process. In the last stage, while the eyelids open, the eyeball rotates in the opposite direction (downwards). The positive pole gets far from the frontal lobe but adjacent to the ground (reference) electrode, thus creating a negative deflection. The signal generated can be detected by the electrodes of the EEG device. These positive and negative deflections can be seen in the EEG waveform, as depicted in Figure 3.

Figure 3 depicts an EEG waveform altered by an eye blink. The vertical axis represents the voltage, while the horizontal axis represents time. Section (b) and (c) denotes eye closing and opening, respectively, while section (a) denotes the center position of the eyeball.

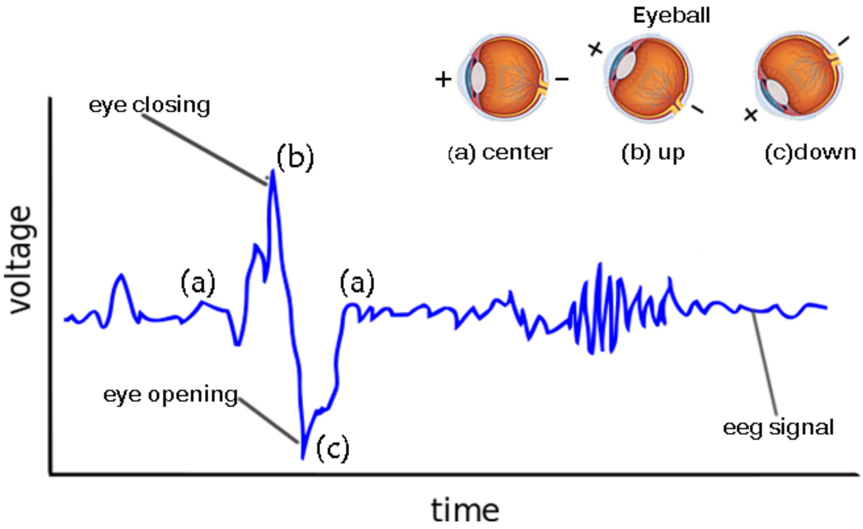


Figure 3. Brainwave signal showing an eye blink.

2.3 EEG devices

2.3.0 Emotiv Epoc+

The Emotive Epoc+ headset by [34] shown in Figure 4, is a wireless 14 channel EEG recording device. It has 14 electrodes (AF3, AF4, P7, P8, O1, O2, T7, T8, FC5, FC6, F3, F4, F7, F8) and two others which are reference electrodes (P3, P4). It uses Bluetooth connectivity, has up to twelve (12) hours of battery life using a USB receiver and up to six (6) hours via Bluetooth. The internal sampling rate is 2048. Through user configuration, it can be down sampled to either 256SPS or 128 SPS. The range of its bandwidth is 0.16Hz to 43Hz. It has digital notch filters at 60Hz and 50Hz. It also has an embedded digital fifth-order Sinc filter.

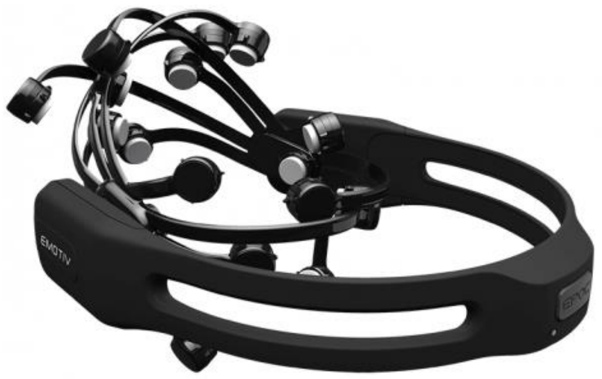


Figure 4. Emotive Epoc+ [34].

2.3.1 NeuroSky Mindwave Mobile 2

The NeuroSky MindwaveMobile 2 headset by [35] shown in Figure 5, is a single-channel EEG recording device. It has a single electrode that rests above the eye at the (Fp1) position according to the 10/20 International Position System. The device's EEG electrode is situated at the tip of the front of the sensor arm. The ground and reference electrodes are located in the ear-clip. It uses the TGAM1 module and has a battery life of eight (8) hours. It is a wireless device that uses Bluetooth. It outputs 12-bit raw brainwaves on a frequency band range of 3Hz – 100Hz, with a sampling frequency of 512Hz. It has a built-in notch filter.

Figure 5. NeuroSky Mindwave Mobile 2 [35]

2.3.2 Emotiv Insight

The Emotiv Insight headset by [36], as shown in Figure 6, is a five-channel EEG recording device. It has five electrodes (Pz, T7, T8, AF3, AF4) and two others, which are reference electrodes. It is a wireless Bluetooth device with a battery life of up to eight (8) hours using a USB connection and up to four (4) hours using a Bluetooth connection. The sampling frequency of this device is 128 per channel. Its bandwidth is on a range of 0.5Hz to 43Hz with digital notch filters at 60Hz and 50Hz. It has a built-in digital fifth-order Sinc filter.

Figure 6. Emotiv Insight 5 Channel Mobile EEG [36]

2.3.3 Muse Headband 2016

The Muse Headband by [37] shown in Figure 7, is a non-invasive four-channel EEG recording device. It has five electrodes (AF7, AF8, TP9, TP10, FPz) of which one (FPz) is a reference electrode. It uses two electrodes on the right and the other two on the left, so it is appropriate for exploring hemispheric asymmetries. It is a wireless Bluetooth device with up to 10 hours of battery life. It has a sampling rate of 256Hz. It has no built-in notch filter.

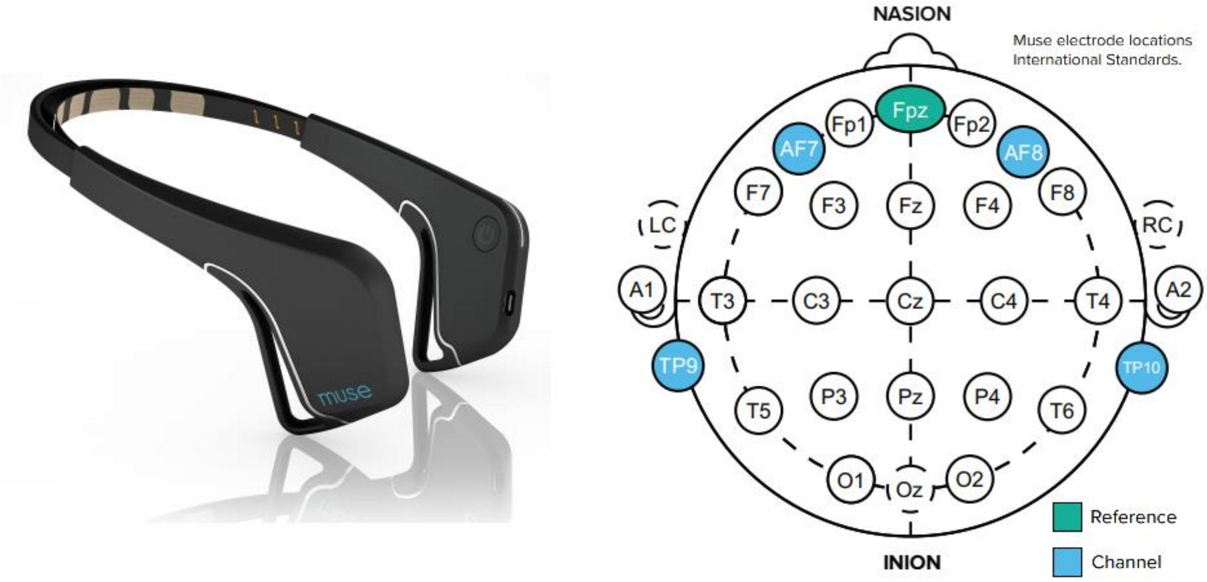


Figure 7. Left(Muse Headband), right(electrode positioning according to 10/20 system) [15]

2.3.4 Other EEG Devices

Other EEG devices include Neural Impulse Actuator, MindFlex, HiBrain, Melon Headband, OpenBCI, IFocusBand and Aurora Dream Headband. These devices are also used, but not as widely as the ones discussed section 2.3 above. A summary of these devices is depicted by Table 1.

Table 1*. Summary of other widely used EEG devices.*

EEG Device	No of Electrodes	Type of Sensor	Year Released
Neural Impulse Actuator	3	dry	2008
MindFlex	1	dry	2009
HiBrain	1	dry	2014
Melon Headband	4	dry	2014
OpenBCI	8/16	dry/wet	2014
IFocusBand	1	dry	2014
Aurora Dream Headband	1	dry	2015

2.3.5 Summary of EEG Devices

The EEG devices stated in section 2.3 are the most commonly used, simply because of their portability, low cost, and their effectiveness in terms of usability. At the time of writing, Muse headband, Emotiv Insight, Emotiv Epoc+, and Neurosky Mindwave Mobile 2 cost \$219.99, \$299.00, \$699.00, and \$99.99, respectively; with Neurosky Mindwave Mobile 2 being the most affordable. All of the mentioned devices use dry electrodes. According to [38], the use of wet electrodes is linked with high signal quality due to abrasive or conductive gels that reduce skin-electrode impedance. However, such devices may not be feasible for long term purposes due to allergic reactions and skin irritation.

The Emotiv Epoc+ has the largest number of electrodes (14) compared to the other three (3) devices. The advantage of multiple electrodes lies in the reduced or minimal loss of crucial data and the detection of critical clinical signals. However, crucial data is dependent on a given use case. It is because various brain sections perform different functions. The most substantial area to obtain the blinking signal is the frontal lobe (Fp1 and Fp2). Even though the Emotiv Epoc+ have the advantage of multiple electrodes, none of its electrodes utilises the Fp1 and Fp2 position. Amongst the four (4), Neurosky Mindwave Mobile 2 is the only device utilising at least one of these positions (Fp1).

When these devices operate using Bluetooth, their battery life ranges from four (4) to ten hours (10). The Neurosky Mindwave Mobile 2 and Muse headband show the most extended battery life of eight (8) and ten (10) hours, respectively. Shorter battery life prohibits prolonged usage of the device. In comparison, longer battery life increases efficiency and the usability aspect of the device [39], which means that longer battery life is desirable and convenient. Regarding usability, other factors like the design, number, and position of electrodes affect user comfort. The Emotiv Epoc+ has fourteen (14) electrodes that require more time to install on the subject's head since the electrodes have to penetrate the hair to touch the scalp. The Neurosky Mindwave Mobile 2 and the Muse headband can be quickly installed since all the electrodes rest on the forehead and the earlobe.

2.4 EEG Authentication

A protocol named CEREBRE, introduced by [40] authenticate users using EEG signals. Four hundred images were used as stimuli, including one hundred faces of celebrities, one hundred food images, one hundred words with low frequency, and one hundred sine gratings. In addition to the mentioned categories, another category of an oddball stimulus was also included in order to evolve the sought EEG pattern further. This study was performed with a total number of fifty participants. A device called Brain-vision BrainAmp DC that has three (EOG) electrodes and twenty-six (EEG) electrodes, was used to capture signals at a sampling rate of 500Hz. A band-pass filter (1-55Hz) was used to filter Event-Related Potentials (ERP), and normalised cross-correlation (discriminant function based) was deployed in classification. The results verified that middle occipital electrodes are activated by visual tasks. Both minimal (four categories and four channels) and maximal (all classifiers and channels) classifiers showed and accuracy of 100%, but maximum accuracy was showed when the minimal classifier used all trials. Results indicated that single-stimulus classifiers, relative to oddball and food stimuli, have the highest accuracy. Very poor performance was shown from the classification that was relative to resting-state EEG. Another poor performance was shown by an authentication method that was based on a memory recall task because of the time taken to recall. This study showed that ERP biometric identification within at least six months, does not degrade significantly.

In another study by [16], a method based on EEG spectral coherence connectivity was suggested for finding uniqueness. The overall idea was to establish distinctiveness using the information that is transferred between various brain regions. A dataset used in this proposed method consisted of one hundred and eight subjects, collected while eyes open and closed resting-state conditions. The EEG signal was captured using a gadget with 64 electrodes, at a sampling frequency of 160Hz. Anti-aliasing low-pass filter was used to down-sample data to 100Hz and extracted up to 50Hz. Power spectral density (PSD) and cross-spectral Coherence (COH) analysis methods were used for extracting spectral features. Algorithms like Match-Score Fusion and Mahalanobis Distance-based classifiers were used separately for calculation of distinctiveness. The analysis was conducted over three various brain regions (P: parieto-occipital, C: central, and F: frontal region). The PSD of eyes closed data displayed accuracy of 90.49% from a single element classifier for the P region. An accuracy of 100% was showed by match-score fusion algorithm for COH features of eyes-closed data from all regions, and eyes-open from the frontal region only. The method used is highly accurate and very robust in person identification. Better accuracy was shown by match-score fusion with COH features. However, COH needs stationary EEG signals and 20 minutes of analysis to process. This means that on conventional hardware, there may be poor classification performance with a large number of subjects (more than 100).

A study by [7] proposed Rapid Serial Visual Representation (RSVP) stimuli based authentication system. A BrainAmp amplifier was used to record EEG signals of 29 subjects. Wet and dry electrodes were separately used to collect data. Targets as a set of 3 symbols were used, and users asked to count the instances from a pool of trials that were created randomly. EEG data were collected from 600 trials comprising of 528 non-targets and 72 targets. The calculation of significant features was done by point-biserial correlation coefficients. Fisher's transformation was used to transform correlations into z-scores for each participant. ERP components were classified using regularised linear discriminant analysis. For single based trial classification, overall accuracy for 16 and 28 channel wet configurations was 85.9% and 87.5%, respectively, and 78.2% for 16 channel dry configuration. Both setups, dry and wet electrodes, showed an accuracy of 100% with 27.0s and 10.7s login times, respectively. The knowledge-based methods presented by this study could be tuned to any level of TAR depending on the needed security level. The login time can be reduced by setting the TAR to a low level. The authors indicate that in coercion situations, subjects can easily hide their passwords. However, the scope of applicability is limited by the need for data calibration.

[15], conducted a study where the number of recruited subjects was 15. A NeuroSky MindSet was used to capture data. The device used has only one electrode that is located at the Fp1 (frontal polar) region on the head. Seven (7) tasks were carried out, including pass-thought (authentication via thoughts), breathing, colour identification, finger movement (simulated), audio listing, sports activity, and passage or singing recitation. Data was simplified into a single dimension by flattening signals in the time domain. Only beta and alpha frequency bands got extracted. The similarity between pairs of signals was quantified by using the cosine similarity of the vector representation. The classification algorithm used was K-nearest Neighbour (KNN). Colour, audio, and sport tasks gave the highest classification accuracies. Nonetheless, the proposed method indicated an accuracy of 99% using tasks that are custom and also

custom acceptance thresholds for each subject. The friendliness of these tasks was checked through administering a questionnaire, and the results showed that the pass-thoughts task was the most challenging to carry out. The easiest tasks were colour, breathing, and audio. This study showed that it is feasible to get the best accuracy while maintaining user-friendliness.

Another study was conducted by [8], proposed a method based on Wavelet Transform and multi-objective Flower Pollination Algorithm to decompose the EEG signal and identify features that offer the best accuracy. A dataset "Motor Movement/Imaginary", which includes one hundred and nine subjects, was collected using a 64-channel EEG device, and it was based on different cognitive tasks. MOFPA-WT performance was evaluated using FAR, TAR, and accuracy. The proposed approach delivered the best accuracies from cognitive tasks; motor movement, in comparison with motor imagination results.

[41] proposed a user identification system using an Emotiv Epoc device that had 14 channels. The proposed approach was based on EEG data captured from six subjects. A lowpass filter called 5th order Butterworth (with a range of 6Hz – 35Hz) was used in the pre-processing phase to get a high signal-to-noise ratio. Features of the EEG signal were extracted using wavelet transform. Other features, including energy, mean, and standard deviation, were extracted from the EEG signal. User recognition was done using Learning Vector Quantization Neural Network in the classification phase. The calculation of recognition rate was done over distinct setups to observe the foremost fusion of EEG channels that can give accurate classification.

The same authors carried out research on cognitive tasks later in a different study to design a person identification system [42]. A dataset of motor/movement and imaginary tasks was used. This dataset was recorded from a single-channel EEG device (Cz). Wavelet Transform was deployed for EEG signal decomposition into five levels for feature extraction. The extracted features were: absolute energy, logarithm energy, energy, and REE energy. EEG signals were classified using Neural Network, from five users using two tasks from four various train-test scenarios. The authors found out that using motor imagination cognitive tasks can give high identification rates compared with motor movement results.

[43] Proposed an EEG based biometric identifier by extracting eye-blinking waveforms from the EEG signal. Neurosky Mindwave was used to record brain waves using MATLAB. In the pre-processing phase, two approaches were adopted. In the first approach eye-blinking signal was extracted by isolating the electrooculogram signal from the EEG signal using empirical mode decomposition. In the second approach, an eye-blinking signal was extracted directly from the EEG signal. Extracted features were based on time delineation of the eye blinking waveform, and classification was done using Linear Discriminant Analysis. A database of 25 subjects was used to obtain high recognition rates. In identification mode, the second approach achieved a correct identification rate of 98.51%, whereas, in verification mode, at a threshold of 1.2665, Equal Error Rate of 2.5% was obtained. This study indicates that eye-blinks are distinct and can distinguish subjects. However, the proposed method used a small database of only 25 subjects. Therefore, the correct identification rate may be affected in a negative way using a large database.

Another EEG authentication method, which specifically focused on the corresponding eye blink on the EEG signal, was introduced by [44]. This method was able to efficiently and accurately distinguish between several users. The proposed approach was convenient and burden-less to the subjects. A dataset of EEG eye blinks collected from twenty users was used in this study. Their implementation was in the form of multi-class classification where SVM with Radial Basis Function kernel was deployed to train multiclass data. A combined set of features, including mean, variance, peak, duration, area, Fourier Transform, and energy were extracted using PCA. Results showed a True Positive Rate of 92%. When using unsupervised classification, a TPR value of 80% was achieved. Results indicated that blink signals could be used to distinguish various users accurately.

[33] adopted a novel human authentication technique that is based on eye blinks extracted from electrooculogram signals. NeuroSky Mindwave headset was used to collect signals for a database of 25 subjects. The eye blinks were then extracted and applied for verification and identification tasks. They were extracted from EEG thorough empirical mode decomposition at the pre-processing stage. At the feature extraction stage, time delineation of the eye blink waveform was put to use. The classification was adopted using linear discriminant analysis. The accuracy and equal error rate achieved were 97.3% and 3.7%, respectively. Results

indicated that eye blinks carry discriminant data and can be used as a base for recognition tasks. However, this study assumes that maximum peaks in the EEG waveform are eye blinks. Therefore, their approach is prone to other EEG artefacts like seizure and epilepsy spikes, that can give similar peaks. Also, 25 blinks per user were averaged in order to produce a test sample. This frequent blinking can put more burden on the users hence lowering the level of practicality.

Another human biometric authentication approach was proposed by [45]. The approach used a multi-level technique where brainwaves during visual stimulation and relaxation were combined with eye blinks. This approach was carried out to enhance the performance using eye blink artefacts. In this multi-level approach, feature and score level fusion techniques were tested. At the feature extraction stage, time delineation of the eye blinking waveform and Autoregressive Modelling of EEG signals was adopted. A database of 31 subjects was used, where subjects performed three various tasks, including eye blinking, relaxation, and visual stimulation. A NeuroSky Mindwave headset was used as a recording device. An accuracy of 99.4% was achieved. Results indicated that the contribution of eye blinking features had significant improvements with regards to correct recognition and error equal rate on the proposed multi-level approach as compared to a single-level approach that uses only EEG.

Table 2 summarises the studies discussed above and other studies not discussed. It also summarises the characteristics used and the accuracy achieved. The precision of each authentication method generally relies heavily on these elements. Even if the complexity of tasks is very difficult to quantify, relaxation may be the simplest. Even if complicated tasks provide greater precision, subjects can relax more easily. In order to obtain greater precision, selected studies have distinct types of characteristics, such as various tasks, a variety of channels, and various algorithms. This table shows changes in precision-based on these parameters. [17] and [18] have determined that combining multiple tasks improves precision by examining various types of tasks. The proposed authentication method by [46] used both ECG and EEG signals. This study yielded high accuracy as compared to other studies that used the same task of relaxation. This high accuracy is because of an added extra ECG channel.

Table 2. *Summary of related EEG authentication studies*

Authors	**No. of Channels**	**No. of Participants**	**Task Done**	**Features Extracted**	**Classifier**	**Accuracy (%)**
[47]	18	10	Facial images as visual stimulation	Negative/positive peaks at defined latencies Distinction of average signals	SVM	86.1
[48]	8	10	Apprehension of images as visual stimulation	Mean amplitude, cross-correlation, coherence	FRNN	92
[49]	2	51	Relaxation with eyes closed	AR, standard deviation, skewness, entropy, Higuchi fractal dimension	LDA	97
[9]	14	12	A cognitive task of imagination of a four-digit number	Common Spatial Patterns	LDA	97
[46]	4	-	relaxation	Cross correlation (ECG & EEG data), FFT, AR, Coherence, mutual information	FDA	98
[50]	61	20	common objects drawings as visual stimulation	Multiple signal classification	ENN, k-NN	98

[15]	1	15	Audio listening, colour identification, breathing, pass thoughts, simulated finger movement, passage/singing recitation, sport activity	Cosine similarity of the vector representation	KNN	99
[17]	14	5	Visual counting, Relaxation, Geometric figure rotation, Limb movement	IHPD, IHLC, SP, AR, PSD	SVM	100
[18]	6	6	Match activity, visual counting, relaxation, mental letter composition, geometric figure rotation	AR, SP, IHPD, IHLC	LDA	100
[7]	16	29	RSVP	Fisher's transformation, point-biserial correlation coeffients	LDA	100
[16]	64	108	Relaxation with eyes open and eyes closed	PSD, COH	Match-score fusion and Mahalanobis distance-based classifier	100
[19]	3	50	Four hundred images as visual stimulation	ERP	Normalized cross correlation	100

EEG based authentication methods discussed in this section have proven that they provide a high level of security, permanence, and recognition accuracy. However, these studies were conducted and evaluated under unrealistic conditions, i.e., controlled emotions and labs. Therefore, there are a number of challenges associated with their level of practicability and usability. One of the challenges associated with EEG based authentication methods is their robustness to physiological and psychological changes [13]. Several EEG based authentication studies [7], [8], [15], [16], [41], [40], [47], [48], [49], are based on a signal generated by the cerebral neural activity. As stated by [13], this signal rapidly changes due to physiological and psychological factors, which cause a constant change in the brainwaves over time. This causes EEG based authentication methods to have a high false rejection rate.

Evidence indicates that physiological and psychological factors affecting EEG authentication-based systems include mental state [51], emotional state [52], [53], [25], [51], exercising [27], [26], [54] etc. The EEG signal is altered by these factors, which are referred to as EEG artefacts. However, the eye blink artefacts present in the EEG waveform are consistent despite changes in cerebral activity. For this reason, several studies [55], [56], [57] have emerged to investigate the use of a combination of EEG features and eye blinks to improve the overall accuracy and performance of EEG based authentication approaches. Such studies have also achieved high accuracies. However, their dependence on cerebral activity like thoughts and mental tasks, still make them prone to physiological and psychological factors. Their level of practicability and usability is still a concern [58]. This gap that the literature is outlining indicates that eye blink-based authentication needs to be explored further since this approach has the security advantage of EEG, yet showing the possibility of practicability and usability.

Chapter 3. Proposed Approach

3.0 Introduction

This chapter entails a detailed description of the steps carried out to formulate an approach that addresses the problem statement in Section 1.3 by implementing specific objectives in Section 1.4.1. The major problem of EEG authentication that this study addresses is its sensitivity to factors like human emotions and exercising. These factors significantly affect the performance of EEG authentication systems in a negative way. Therefore, making EEG authentication less practical in the real world. Researchers have come up with different approaches to tackle this issue, as discussed in Chapter 2, but these approaches have their limitations. We propose a new EEG authentication approach by implementing an algorithm that uses EEG artefacts (blinking).

The next sections of this chapter include an overview of the proposed approach, EEG signal collection, selection of relevant data features, authentication algorithm, and summary.

3.1 Overview

An overview of the proposed approach entails four (4) major sections being EEG signal collection, pre-processing, feature selection, and proposed algorithm. These four sections are carried out in both the enrolment and authentication phases, as depicted in Figure 8. The EEG signal was collected from subjects using a NeuroSky Mindwave Mobile 2 device. In this stage, necessary steps were carried out to minimise signal to noise ratio. These steps include cleaning the scalp and the electrode with alcohol. In the second stage, the pre-processing stage, the built-in noise filtering mechanism on the TGAT chip from the NeuroSky Mindwave Mobile device was used. Three (3) types of filters (Notch filter, Low-pass filter, and High-pass filter) were applied to the EEG signal. A High-pass filter was applied at a cut-off frequency of 3Hz to clean up low-frequency noise. A Low-pass filter was applied at a frequency cut-off of 100Hz on the EEG signal to remove high-frequency noise. A 50Hz notch filter was used to remove the 50Hz frequency noise caused by electric appliances and power lines. The TGAT chip performs some computations on the signal and outputs digital data. This data contains various features. Feature extraction was then performed, and relevant data features were selected. At the enrolment stage, the subject's EEG data were saved in the MySQL database.

The same process is repeated, except at the authentication stage, where the subject's data were compared with previously saved data using the pattern matching algorithm and a defined threshold to determine if the subject is accepted or rejected. This whole process is shown in Figure 8.

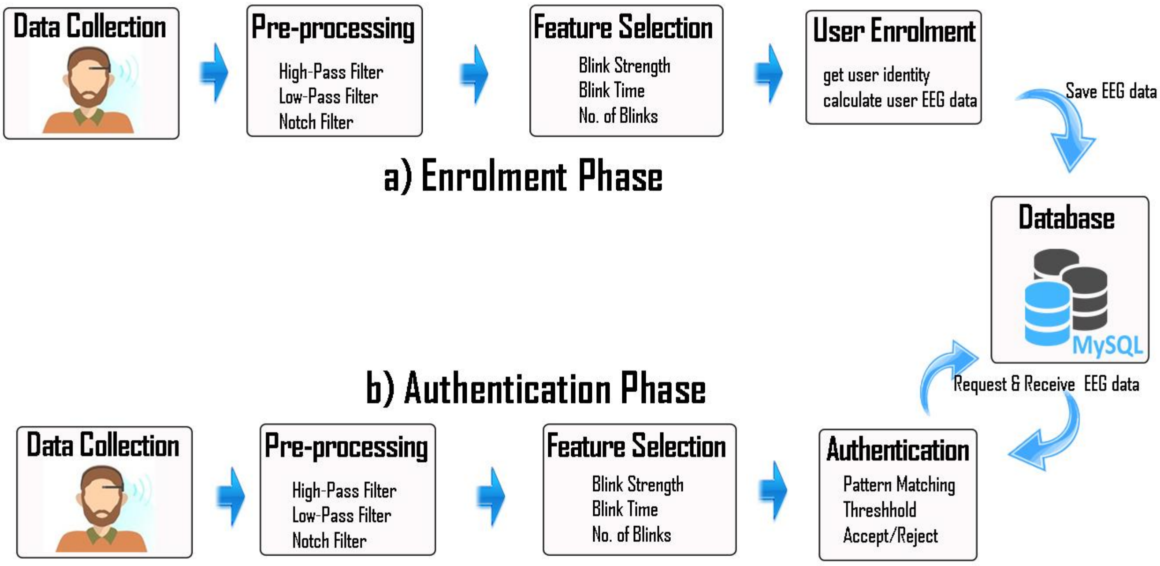


Figure 8. An overview of the proposed approach (EEG Authentication Algorithm)

3.2 EEG Data Collection

This section entails a detailed description of the process of collecting the EEG signal. It includes the steps, tools, and equipment used and a justification of how they were used and selected. The process of collecting the EEG signal is categorised into three sections. The first section deals with minimising electrode impedance, which includes the tools and steps carried out to enhance signal quality. The second section deals with the extraction of the EEG signal, which includes tools and methods used and their justifications. The last section, which is the third section, deals with the recording of the EEG data.

3.2.0 Minimising Electrode Impedance

The collection of clean EEG signal takes more than just having a good device. There has to be a very stable connection between the scalp and the electrode. However, sweat, oily skin, and dead skin cells accumulate on the surface of the scalp, therefore creating a layer of electrical resistance. This layer hinders electrical activity from propagating well. In EEG recording, this is known as impedance. It is of paramount importance to undertake necessary procedures to reduce electrode impedance to ensure that we acquire a cleaner signal. For that reason, alcohol was used to clean the region where the electrodes come in contact with the skin. This region is the Fp1 (just above the left eye) and the reference electrode area (left ear lobe), as shown in Figure 9. These areas were scrubbed gently using an abrasive gel and a cotton pad to remove any dirt that might have accumulated. Then the skin was cleaned with alcohol to de-grease the skin to allow the electrodes to stick better.

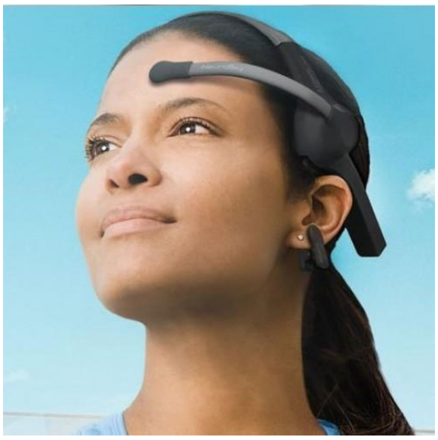


Figure 9. Electrode site position (Fp1 and left ear lobe) to be cleaned [59].

3.2.1 Signal Extraction

The second step in EEG signal collection deals with the extraction of the signal. We used the NeuroSky Mindwave Mobile 2 device for capturing EEG signals. Three main factors motivated the selection of this device. The first factor is the price. NeuroSky Mindwave Mobile 2 is a low-cost EEG device that is easily accessible yet according to the literature [15], [33], [43], [56], it is one of the popular devices used in EEG research, from simple projects to advanced complex projects like EEG authentication. The second factor is the electrode position. NeuroSky Mindwave Mobile 2 has two electrodes of which one that is located at the earlobe is a reference electrode. The other electrode is located at the forehead, above the eye at the (Fp1) position according to the 10/20 International Position System (See Figure 9). One of the key features in this research is the eye blink, therefore the (Fp1) position is the most ideal position since the electrode is placed close to the frontal lobe. The choice of this electrode position will tremendously contribute to the low signal-to-noise ratio hence improve the overall performance of our authentication algorithm. The third factor is portability. This device is very portable, easily adjustable and light in weight. Its adjustability makes it to perfectly fit well in any human head size. The lightweight factor reduces discomfort in users.

EEG signals were captured from the subject using NueroSky Mindwave Mobile 2 headset. These signals were then pre-processed. The details of the pre-processing stage are discussed in Section 3.3. The pre-processed data is transmitted over Bluetooth to the computer that has a ThinkGear Connector tool installed. The specifications of the computer used are as follows, a Dell Laptop with 8GB of RAM, 500GB of Hard disk, and Intel(R) Dual-Core (TM) i5-2540M CPU @ 2.60. These hardware specifications were motivated by the recommended specifications for running Microsoft Visual Studio by Microsoft.

The ThinkGear Connector tool manages communication between the computer and the connected NeuroSky Mindwave Mobile 2 device. This tool offers a daemon-like service to manage the two connected devices. It continuously runs in the background and maintains an open socket between the computer and NeuroSky Mindwave Mobile 2 headset, to allow applications to connect and read data. It is provided for the Windows platform as an executable file. Every NeuroSky product has a ThinkGear technology embedded in it. This technology allows the wearer's brain signals to be interfaced with the ThinkGear device. The ThinkGear chip calculates the eSense meters, like attention & meditation, and raw brainwaves. The calculated values are output to the PC through the headset by the ThinkGear chip. Table 3 indicates a list of all the output values.

3.2.2 Signal Recording

In the signal recording stage, Microsoft Visual Studio (MVS) is used to read and record data from the headset. Neurosky Mindwave device has great support for ".Net" libraries. For this reason, MVS becomes an ideal software for acquiring EEG data from the Neurosky Mindwave headset. MVS has many features, including "Nugget console" that is more efficient and time-saving. Nugget console is a feature that allows simple and easy addition of Frameworks and DDLs to one's project by just using a simple single command. The recorded data was then stored in the MySQL database.

3.3 EEG Signal Pre-processing

The NeuroSky Mindwave Mobile 2 EEG device has a ThinkGear AM (TGAM) PCB module that receives raw EEG signals from the sensors and filters out extraneous noise as well as electrical interference. The TGAM has an embedded TGAT chip, which comes programmed with filters that filter noise and separate EEG signals into different types of brainwaves. As the EEG signal enters the TGAM chip, it passes through a built-in Low-Pass Filter, High-Pass Filter, and Notch Filter. It is then divided by other filters according to the brainwave, for example, Gamma. Sampling is then performed at 512 Hz before 12-bit resolution data is sent to the analogue-to-digital converter (ADC). This process outputs final digital values for each type of brainwave. The processor then calculates Power FFT using the outputted digital values of each type of brainwave.

3.3.0 Low-Pass Filter

The EEG signal rarely reaches a frequency of 100Hz and anything above that is entirely noise. A low-pass filter was applied by default at a frequency cut-off of 100Hz on the EEG signal to remove high-frequency components or noise. This is a built-in process, of which further details are not availed by the manufacture.

3.3.1 High-Pass Filter

The EEG signal rarely goes below 3Hz, and anything below that is regarded as noise. A high-pass filter was applied by default at a cut-off frequency of 3Hz to clean up low-frequency noise and to remove DC components and drifts. This is also a built-in process, of which further details are not availed by the manufacture.

3.3.2 Notch Filter

A notch filter is a type of filter, which its function is to filter out noise at a predefined frequency instead of a range of frequency. The noise is caused by alternating current (AC) from standard electric sockets or outlets and appliances. The AC oscillates at 50Hz in our country Botswana. The 50Hz produced by the electrical appliances in our environment contaminates the EEG signal. The built-in notch filter was applied by configuring the TGAM chip’s M pin. The M pin was connected to the ground pin to set the filter at 50Hz.

3.4 Feature Extraction

This section entails a feature extraction process that implements a specific objective stated in section 1.4.1. The first part of this section describes the data retrieved from the TGAM module, followed by the feature selection process. The third part describes in detail all the steps and methods used in the feature extraction process.

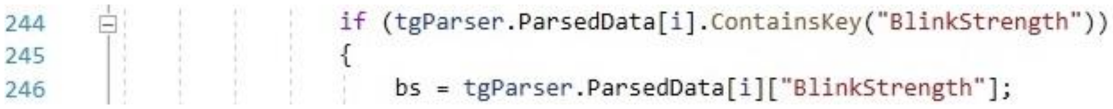
According to [35], data received from the TGAM module is converted into easily accessible data using the TGParser class from the NeuroSky SDK. This data is contained in a dictionary data structure. Table 3 below shows the EEG data as well as its description. The first column indicates a list of data features, while the second and last column indicates a description of these features and their data type, respectively.

Table 3*. Description of EEG data received from NeuroSky Mindwave Mobile 2.*

Data Features	Description	Data Types
Raw	Raw EEG data	short
Time	Timestamps of the packet received	double
EEGPowerTheta	Theta Power	int
EEGPowerGamma	Gamma Power	int
EEGPowerDelta	Delta Power	int
EEGPowerAlpha	Alpha Power	int
EEGPowerBeta	Beta Power	int
Attention	The level of the user’s mental focus	double
Meditation	The level of user’s mental calmness	double
PoorSignal	Signal quality status	double
BlinkStrength	The strength of a detected blink	int
MentalEffort	How hard the brain of the subject is working	double
Familiarity	How well a new task is learned by the subject	double

The authentication algorithm focuses on the use of eye blink properties, and for this reason, the blink data features become relevant. This includes blink strength. The blink strength value indicates the intensity of an eye blink. These values range from 1 to 255, where 1 indicates the weakest blink, and 255 indicates the strongest blink. According to [35], the blink strength value is directly dependent on the poor signal (signal quality status) value. This is the value that indicates how poor or good the signal received at the sensor is. The value ranges from 0 to 128. This range indicates that the headset is worn by the user, whereas a value greater than 128 indicates otherwise. The lower the value, the higher the signal quality. The blink strength value is only relevant and is calculated when the poor signal value is less than 51 [35]. The other important aspect is the time at which an eye blink occurs since it forms part of the authentication pattern. This qualifies the selection of the time feature to be useful and relevant in developing the authentication algorithm. This feature indicates the timestamp of the packet received and is represented in milliseconds.

After all relevant features were identified and selected, the next stage was the feature extraction process. As already discussed, the blink strength value ranges from 1 to 255. From this data, we extracted three (3) important features being “soft blink”, “normal blink” and “hard blink”. A soft blink is a blink which its value ranges from 1 to 50. A normal blink has a value that ranges from 51 to 90, whereas a hard blink value range from 91 to 255. In order to extract these features, we used the “SetBlinkDectection()” function from the NeuroSky API to enable blink strength data to be output. We then retrieved the blink strength value using the “BlinkStrength” key from the `tgParser` dictionary object as depicted by the code snippet in Figure 10.

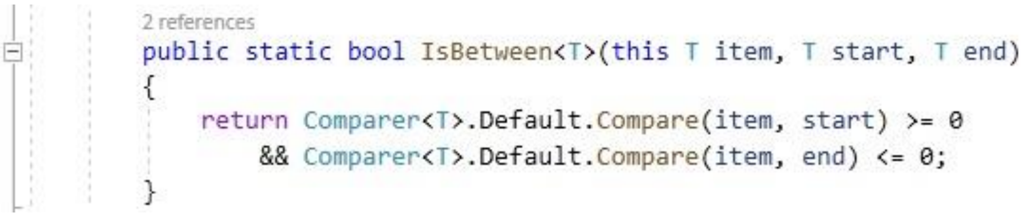


```
if (tgParser.ParsedData[i].ContainsKey("BlinkStrength"))
{
    bs = tgParser.ParsedData[i]["BlinkStrength"];
```

Figure 10. Extracting the blink strength value from the tgPaser dictionary object

Figure 10 above shows a code snippet where the blink strength value was retrieved from the `tgParser` dictionary object using `BlinkStrength` as the key, as shown in the first line of code. The second line of code indicates the value stored in variable `bs`.

The features soft blink, normal blink, and hard blink were derived using the `isBetween` custom function. This function uses the blink strength value as the first parameter in order to check if it falls between the range specified in the second and third parameters. Figure 11 below depicts the said function.



```
2 references
public static bool IsBetween<T>(this T item, T start, T end)
{
    return Comparer<T>.Default.Compare(item, start) >= 0
        && Comparer<T>.Default.Compare(item, end) <= 0;
}
```

Figure 11. A custom function used to extract soft, normal & hard blink features

The other feature being “blink time”, is the time represented in milliseconds, which indicates the time at which a blink occurred from the start of the session. It was derived by finding a time difference between the blink timestamp and the session timestamp. Another feature is the blinking number, which indicates the total number of blinks that occurred between the start and end of a session. It was derived by getting the size of the collection that stored blink timestamps.

3.5 Proposed Authentication Algorithm

3.5.0 Overview

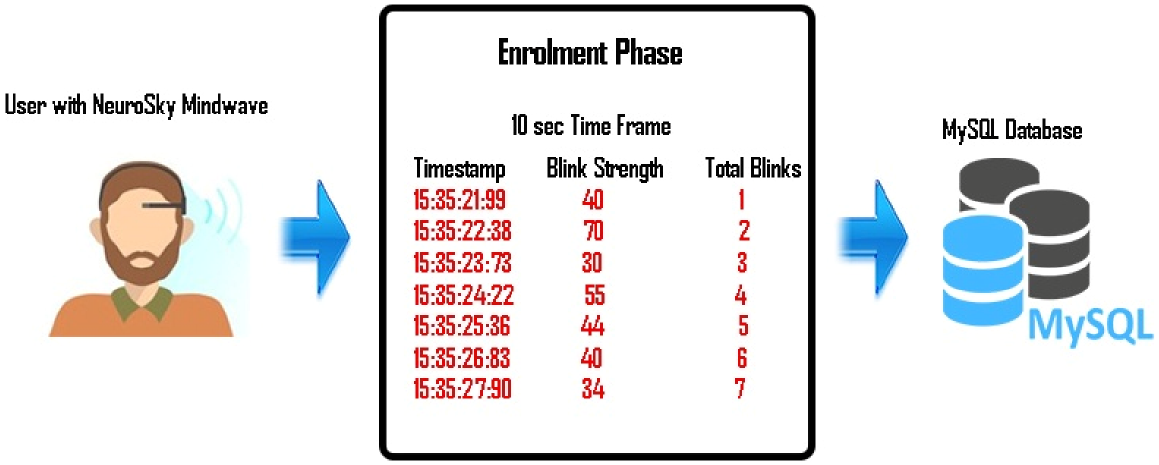
This section outlines how the specific objective mention in section 1.4.1, which reads “To develop an authentication algorithm based on eye blink artefact” is achieved. The first section (3.5.1) describes the architecture of the algorithm and the second section (3.5.2) outlines the implementation of the algorithm.

3.5.1 Algorithm Description

The proposed algorithm access data output by the TGAT chip through the NeuroSky SDK. On a defined timeframe, data was recorded from the user during the enrolment phase and then compared with the data recorded during the authentication phase. The experimental setup of the enrolment and authentication is further explained in section 4.2.

3.5.1.0 Enrolment Phase

At the enrolment phase, data was recorded from the user in a given 10 seconds timeframe. From the start of this timeframe, blink information being “blink timestamp” and “blink strength” is continuously saved in memory in a data structure until the 10 seconds period elapses. At the end of the 10 seconds, this data (total number of blinks, blink timestamp, and blink strength) was stored in a MySQL database. Figure 12 and 13 below depicts the said analogy.

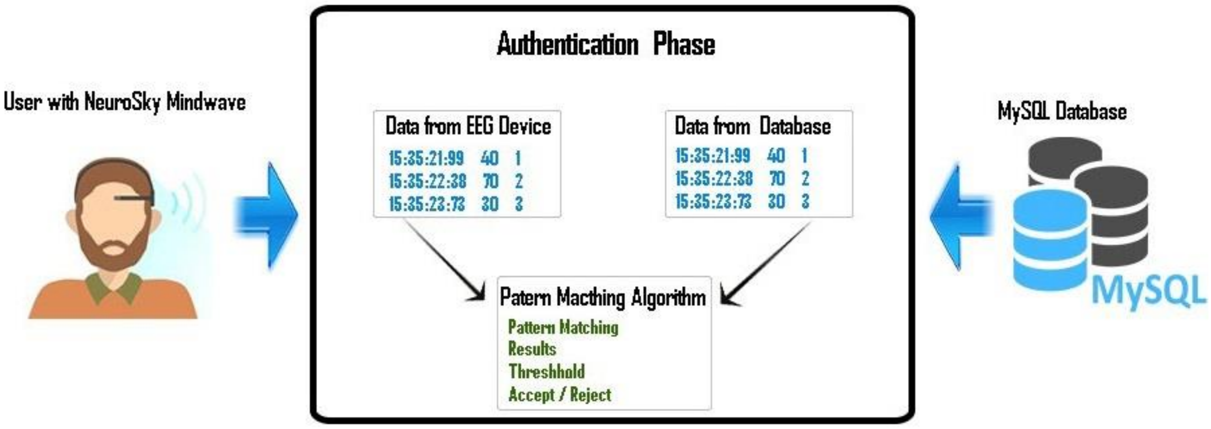


Timestamp	Blink Strength	Total Blinks
15:35:21:99	40	1
15:35:22:38	70	2
15:35:23:73	30	3
15:35:24:22	55	4
15:35:25:36	44	5
15:35:26:83	40	6
15:35:27:90	34	7

Figure 12. Capturing and recording data at the enrolment phase.

3.5.1.1 Authentication Phase

At the authentication phase, the same approach for data recording from the enrolment phase was carried out. At the end of the 10 seconds, the authenticating user's data was pulled from the database, that data was compared or matched with the data obtained from the user/EEG device. The matching algorithm calculated the difference and gave scores/results on a scale of 0 – 100, where 0 indicates no match, and 100 depicts a full match. The user was either accepted or rejected based on a defined threshold value. Figure 14 below depicts the said analogy.



Data from EEG Device
15:35:21:99 40 1
15:35:22:38 70 2
15:35:23:73 30 3

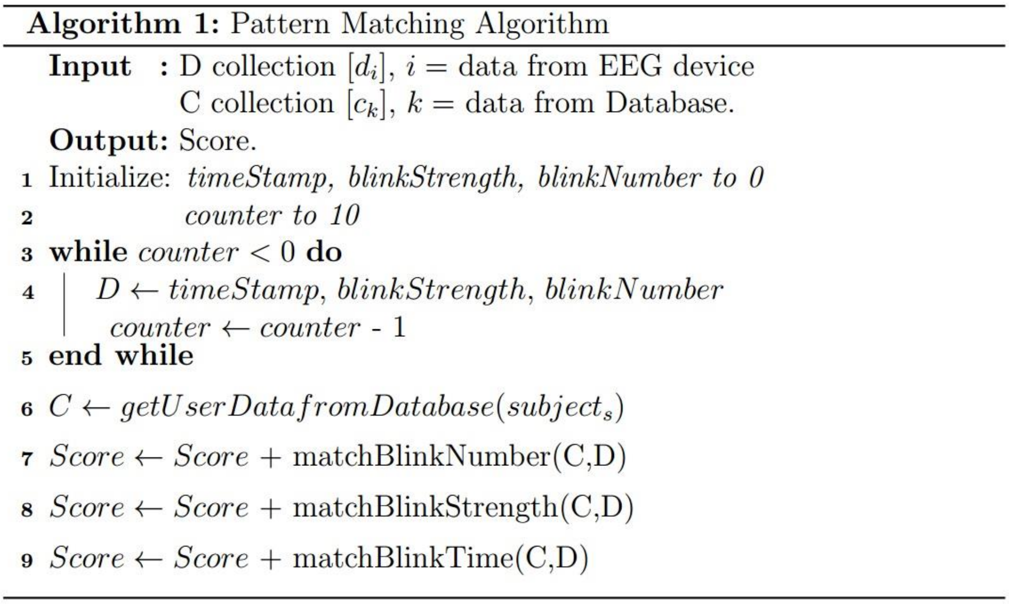
Data from Database
15:35:21:99 40 1
15:35:22:38 70 2
15:35:23:73 30 3

Patern Maching Algorithm
Pattern Matching
Results
Threshhold
Accept / Reject

Figure 13. Capturing, recording, and matching data at the authentication phase.

3.5.2 Pattern Matching Algorithm

Data from the NeuroSky Mindwave Mobile 2 device is compared with data previously stored in a database using the matching algorithm. This algorithm has three major sub algorithms. The first one compares the total number of blinks from the NeuroSky Mindwave Mobile 2 device during authentication with the total number of blinks previously stored in the database. The second sub-algorithm compares the timestamps, and the third sub-algorithm compares the blink strength. These sub algorithms are discussed below in detail.



```
Algorithm 1: Pattern Matching Algorithm
   Input  : D collection [$d_i$], $i$ = data from EEG device
            C collection [$c_k$], $k$ = data from Database.
   Output: Score.
1  Initialize: timeStamp, blinkStrength, blinkNumber to 0
2              counter to 10
3  while $counter < 0$ do
4      $D \leftarrow timeStamp, blinkStrength, blinkNumber$
       $counter \leftarrow counter$ - 1
5  end while
6  $C \leftarrow getUserDatafromDatabase(subject_s)$
7  $Score \leftarrow Score$ + matchBlinkNumber(C,D)
8  $Score \leftarrow Score$ + matchBlinkStrength(C,D)
9  $Score \leftarrow Score$ + matchBlinkTime(C,D)
```

Figure 14. Pseudocode for the proposed pattern matching algorithm.

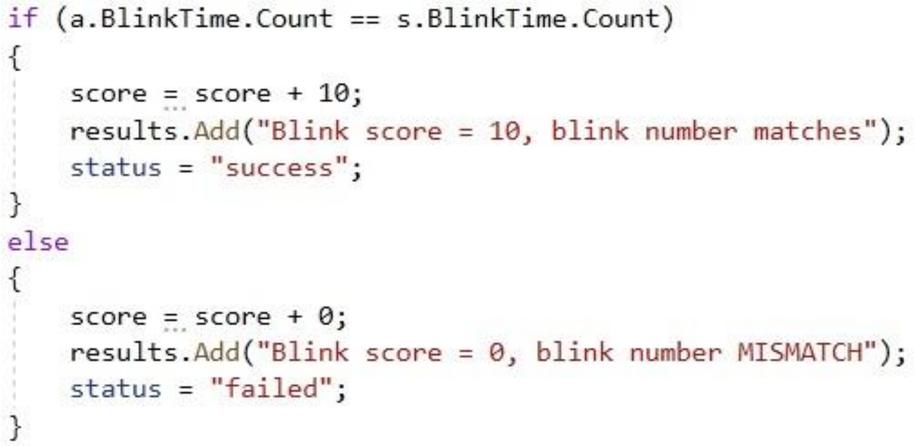
Figure 14 indicates that a collection `D` holds input data streamed by the EEG device in realtime. Another collection `C` holds input data from the database for the same subject. Both collections `C` and `D` hold the same type of data, which is: *`timeStamp`*, *`blinkStrength`*, and `blinkNumber`. A variable `score` holds the algorithm output results. The algorithm begins by initialising `timestamp`, `blinkStrength`, and `blinkNumber` to `0`. A variable `counter`, which keeps track of session time in seconds, is initialised to `10`. This indicates that the duration of the algorithm time is initially set to 10 seconds. In line `3`, a loop begins and data that is streamed by the EEG device is continuously saved in collection `D`. A `counter` variable is decremented by `1`, every second. This process repeats until the `counter` variable is less than `0`.

A function `getUserDatafromDatabase(subject_s)` is invoked to fetch the user data and store it in collection `C`. Another function, `matchBlinkNumber(C,D)`, a sub-algorithm that matches the blink number in collection `C` against collection `D`, is invoked, and the returned results are added to the variable `score`. The detailed operations of this sub-algorithm are further elaborated in section 3.5.2.0. In line `8`, function `matchBlinkStrength(C,D)`, a sub-algorithm that matches the blink strength in collection `C` against collection `D`, is invoked and the returned results are added to variable `score`. Also, its detailed operations are further elaborated in section 3.5.2.1. Lastly, function `matchBlinkTime(C,D)`, a sub-algorithm that matches the timestamps of blinks in collection `C` against collection `D`, is invoked and the returned results are added to variable `score`. The detailed operations of this sub-algorithm are further elaborated in section 3.5.2.2.

3.5.2.0 Blink Number Matching Algorithm

The total number of blinks obtained during the authentication phase was calculated, and the database was queried to fetch the value of the number of blinks previously stored in the database for the same user. Both values were compared, and if the match was one hundred percent, a ten (10) points score was awarded. Otherwise, 0 points were awarded. Upon a successful match, the algorithm invokes another algorithm and relinquishes the comparison task. The blink-number feature takes 10% of the overall score. Figure 15 shows the code snippet of the mentioned blink number matching algorithm.

Code Snippet



```
if (a.BlinkTime.Count == s.BlinkTime.Count)
{
    score = score + 10;
    results.Add("Blink score = 10, blink number matches");
    status = "success";
}
else
{
    score = score + 0;
    results.Add("Blink score = 0, blink number MISMATCH");
    status = "failed";
}
```

Figure 15. Code snippet for matching blink number.

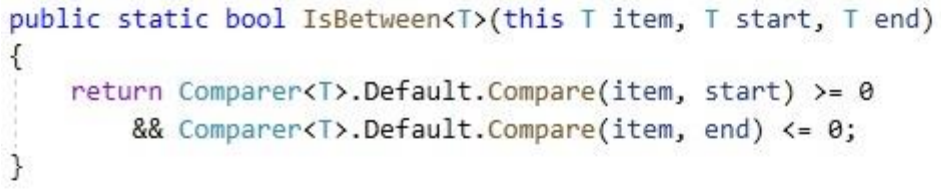
3.5.2.1 Blink Time Matching Algorithm

At the start of the authentication phase, a timestamp was recorded to indicate the beginning of an authentication phase. After that, the timestamp of every eye blink that occurred was recorded. The time difference between the start of the authentication phase and the occurrence of a blink was calculated, and the new value "blink time", was recorded (in milliseconds) for every blink stored in a collection. At the end of the authentication, a database was queried to fetch a collection that was previously stored for that particular user at the enrolment phase. Both collections were iterated, and each value was compared with the corresponding value in the other collection.

The comparison matches a value from the EEG device against a corresponding value from the database, in a range of 800 milliseconds (plus and minus). Meaning, a value "x" is matched against a corresponding value "y", where "y" is on a range of values as depicted by Equation (1).

$$(y - 800) < y < (y + 800) \qquad (1)$$

Equation (1) is translated into a function that takes three (3) parameters. The first parameter being the value of y, the second parameter depicting the minimum range value (y -800) while the third parameter indicates the maximum range value (y + 800). The function is shown in Figure 16.



```
public static bool IsBetween<T>(this T item, T start, T end)
{
    return Comparer<T>.Default.Compare(item, start) >= 0
        && Comparer<T>.Default.Compare(item, end) <= 0;
}
```

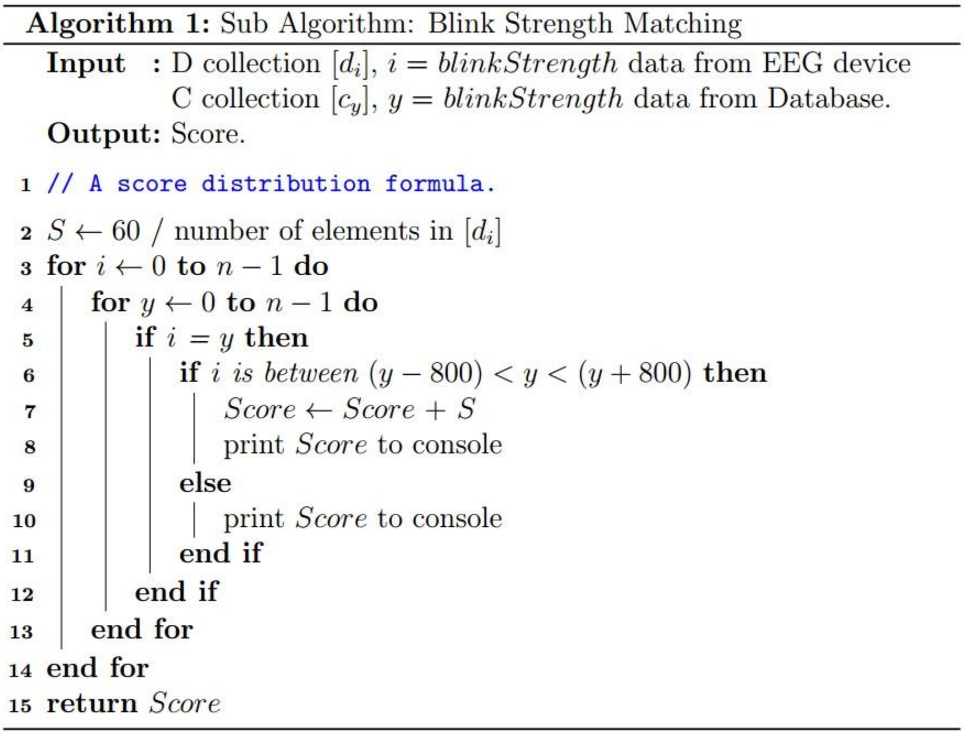
Figure 16. Code snippet for the function that validates a given range of values.

Upon a successful match, a score is awarded. Unlike the blinking number that gets 10% of the overall score, the blink time takes 60% of the overall score. This 60% score is divided evenly based on the total number of blinks a collection has, using Equation (2). Variable "s" depicts the maximum score each item in a collection can have, while variable "b" depicts the total number of items in a collection. This score distribution formula is depicted in Equation (2).

$$s = \frac{60}{b} \tag{2}$$

All the scores awarded by this sub-algorithm are summed up, and the resulting value is added to the main score.

a) Pseudo Code

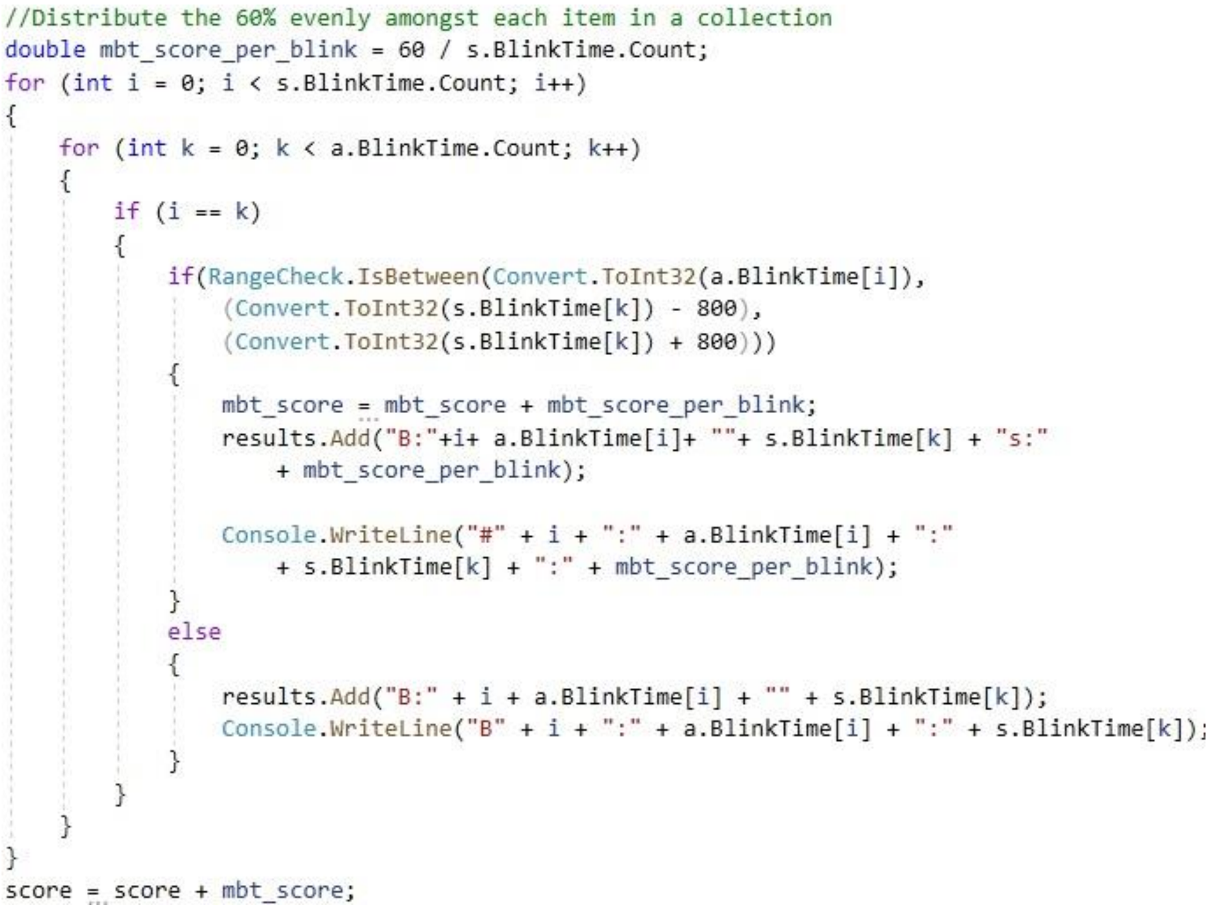


```
Algorithm 1: Sub Algorithm: Blink Strength Matching
  Input  : D collection $[d_i]$, $i = blinkStrength$ data from EEG device
           C collection $[c_y]$, $y = blinkStrength$ data from Database.
  Output: Score.
// A score distribution formula.
$S \leftarrow 60$ / number of elements in $[d_i]$
for $i \leftarrow 0$ to $n - 1$ do
    for $y \leftarrow 0$ to $n - 1$ do
        if $i = y$ then
            if $i$ is between $(y - 800) < y < (y + 800)$ then
                $Score \leftarrow Score + S$
                print $Score$ to console
            else
                print $Score$ to console
            end if
        end if
    end for
end for
return $Score$
```

Figure 17. Pseudocode for blink time matching algorithm.

Figure 17 indicates a sub-algorithm that matches blink strength data. A collection D holds blink strength input data streamed by the EEG device while collection C holds input data from the database for the same subject. A variable score holds the algorithm output results. The algorithm begins by executing a score distribution formula depicted by Equation (2). Results are stored in variable S. Both collection D and C are iterated, and each value in collection D is matched against a corresponding value in collection C. The corresponding values are found where index i in collection D is equal to index y in collection C. Then a value at index i in collection D is evaluated to check if it falls within a range depicted by Equation (1) on the corresponding index y in collection C. If the expression returns true, then the score S is added to the variable score. The variable score is then printed to the console. The same process repeats until all elements in both collections are compared. The algorithm then returns the variable `score` to the calling function.

b) Code Snippet.



```
//Distribute the 60% evenly amongst each item in a collection
double mbt_score_per_blink = 60 / s.BlinkTime.Count;
for (int i = 0; i < s.BlinkTime.Count; i++)
{
    for (int k = 0; k < a.BlinkTime.Count; k++)
    {
        if (i == k)
        {
            if(RangeCheck.IsBetween(Convert.ToInt32(a.BlinkTime[i]),
                (Convert.ToInt32(s.BlinkTime[k]) - 800),
                (Convert.ToInt32(s.BlinkTime[k]) + 800)))
            {
                mbt_score = mbt_score + mbt_score_per_blink;
                results.Add("B:"+i+ a.BlinkTime[i]+ ""+ s.BlinkTime[k] + "s:"
                    + mbt_score_per_blink);

                Console.WriteLine("#" + i + ":" + a.BlinkTime[i] + ":"
                    + s.BlinkTime[k] + ":" + mbt_score_per_blink);
            }
            else
            {
                results.Add("B:" + i + a.BlinkTime[i] + "" + s.BlinkTime[k]);
                Console.WriteLine("B" + i + ":" + a.BlinkTime[i] + ":" + s.BlinkTime[k]);
            }
        }
    }
}
score = score + mbt_score;
```

Figure 18. Code snippet for blink time matching algorithm.

3.5.2.2 Blink Strength Matching Algorithm

For every occurrence of a detected eye blink during authentication, the blink strength value is recorded and stored in a collection. A query is performed on the database to fetch the user's blink strength data previously recorded at the enrolment stage. Both collections are iterated, and each value is compared with the corresponding value from the other collection. The comparison matches a value from the EEG device against a corresponding value from the database, on a range of 15 units (plus and minus). Meaning, the value "x" is matched against a corresponding value "y", where "y" is on a range of values as depicted by Equation (3).

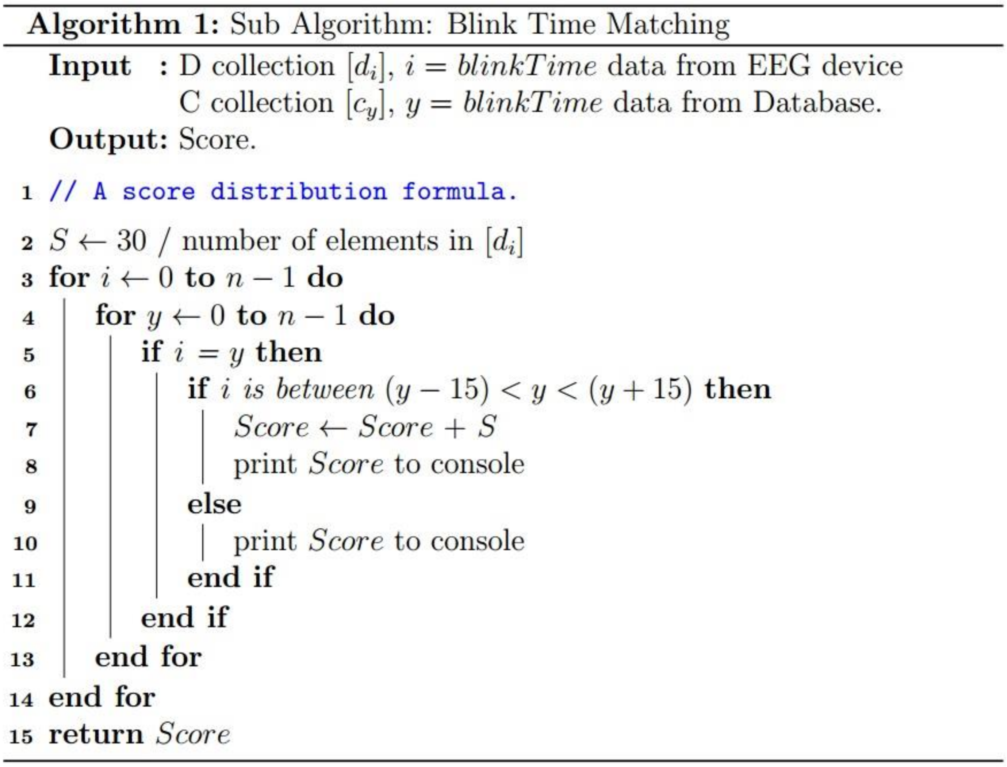
$$(y - 15) < y < (y + 15) \qquad (3)$$

Upon a successful match, a score is awarded. The blink strength takes 30% of the overall score. This 30% score is divided evenly across the total number of blinks a collection has, using a formula shown by Equation (4). Variable “s” depicts the maximum score each item in a collection can have, while variable “b” depicts the total number of items in a collection.

$$s = \frac{30}{b} \tag{4}$$

All the scores awarded by this sub-algorithm are summed up, and the resulting value is added to the main score.

a) Pseudo Code

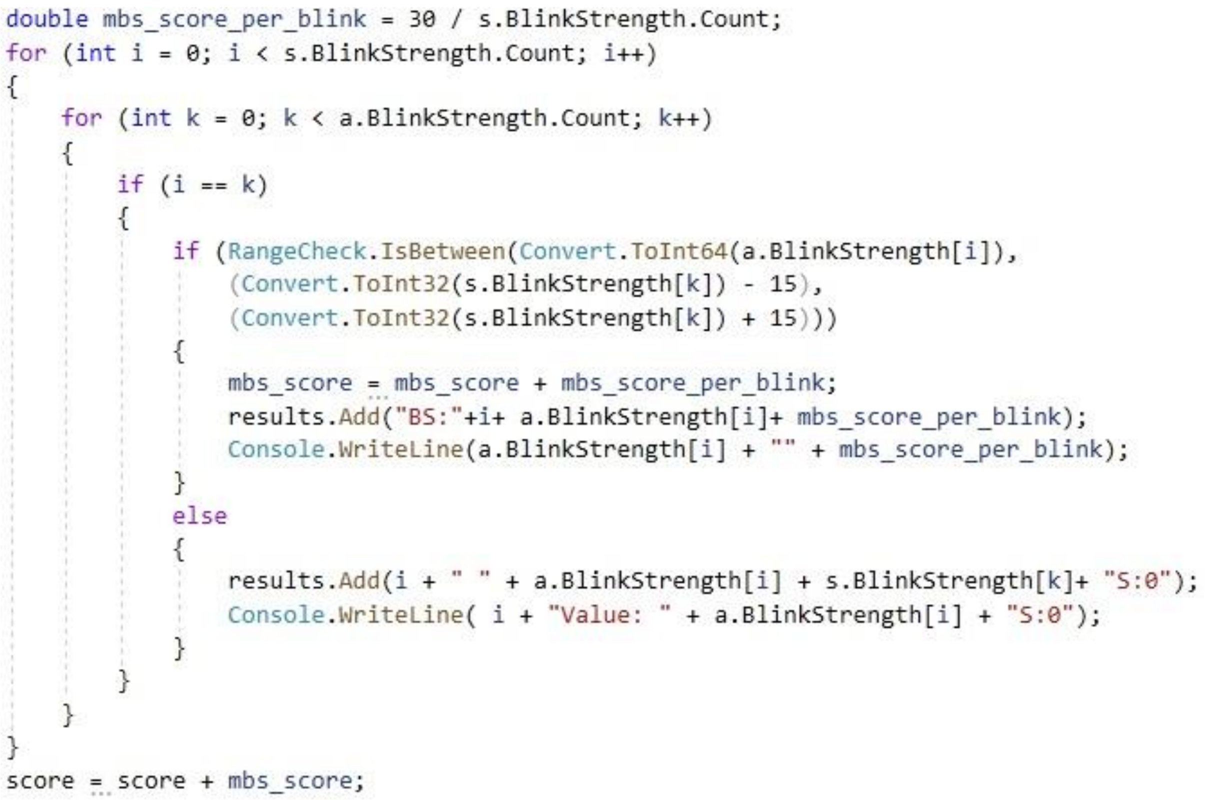


```
Algorithm 1: Sub Algorithm: Blink Time Matching
Input  : D collection $[d_i]$, $i = blinkTime$ data from EEG device
         C collection $[c_y]$, $y = blinkTime$ data from Database.
Output: Score.
// A score distribution formula.
$S \leftarrow 30$ / number of elements in $[d_i]$
for $i \leftarrow 0$ to $n - 1$ do
    for $y \leftarrow 0$ to $n - 1$ do
        if $i = y$ then
            if $i$ is between $(y - 15) < y < (y + 15)$ then
                $Score \leftarrow Score + S$
                print $Score$ to console
            else
                print $Score$ to console
            end if
        end if
    end for
end for
return $Score$
```

Figure 19. Pseudocode for blink strength matching algorithm.

Figure 19 indicates a sub-algorithm that matches blink time data. A collection `D` holds blink strength input data streamed by the EEG device while collection `C` holds input data from the database for the same subject. A variable `score` holds the algorithm output results. The algorithm begins by executing a score distribution formula depicted by Equation (4). Results are stored in variable `S`. Both collection `D` and `C` are iterated, and each value in collection `D` is matched against a corresponding value in collection `C`. The corresponding values are found where index `i` in collection `D` is equal to index `y` in collection `C`. Then a value at index `i` in collection `D` is evaluated to check if it falls within a range depicted by Equation (3) on the corresponding index `y` in collection `C`. If the expression returns `true`, then the score `S` is added to the variable `score`. The variable `score` is then printed to the console. The same process repeats until all elements in both collections are compared. The algorithm then returns the variable `score` to the calling function.

b) Code Snippet.



```
double mbs_score_per_blink = 30 / s.BlinkStrength.Count;
for (int i = 0; i < s.BlinkStrength.Count; i++)
{
    for (int k = 0; k < a.BlinkStrength.Count; k++)
    {
        if (i == k)
        {
            if (RangeCheck.IsBetween(Convert.ToInt64(a.BlinkStrength[i]),
                (Convert.ToInt32(s.BlinkStrength[k]) - 15),
                (Convert.ToInt32(s.BlinkStrength[k]) + 15)))
            {
                mbs_score = mbs_score + mbs_score_per_blink;
                results.Add("BS:"+i+ a.BlinkStrength[i]+ mbs_score_per_blink);
                Console.WriteLine(a.BlinkStrength[i] + "" + mbs_score_per_blink);
            }
            else
            {
                results.Add(i + " " + a.BlinkStrength[i] + s.BlinkStrength[k]+ "S:0");
                Console.WriteLine( i + "Value: " + a.BlinkStrength[i] + "S:0");
            }
        }
    }
}
score = score + mbs_score;
```

Figure 20. Code snippet for blink strength matching algorithm.

3.6 Summary

This chapter focused on the approach used to achieve specific objectives 1, 2, 3, and 4 specified in section 1.4.1.

To achieve objective 1, EEG signal collection was done using the NeuroSky Mindwave headset. The process involved three key steps. The first step involved minimising electrode impedance to improve signal quality. The second step involved extracting the EEG signal from the headset using the ThinkGear connector. The third step involved recording the signal using Microsoft Visual Studio (MVS) and MySQL database. The signal pre-processing process was carried out to achieve objective 2. This process was done through the application of three (3) filters. The first one, which is a low-pass filter, was applied to remove high-frequency noise. A high-pass filter was applied to remove low-frequency noise while a notch filter was applied to filter noise caused by electrical appliances. Feature selection and extraction were carried out to achieve objective 3. These features, poor signal, blink strength, blink timestamp, and blink number, were selected. Soft, normal, and hard blink features were extracted from the TgPaser object using “isBetween” function.

To achieve objective 4, an authentication algorithm was developed. The algorithm matched the authentication pattern recorded at the authentication phase against the pattern recorded at the enrolment stage. It comprises of three key parts. The first part matched the number of blinks by computing if the values are equal, and upon a successful match, a score was awarded. The second part matched the blink time. The blink timestamp recorded at the enrolment stage is matched against the corresponding blink timestamp at the authentication phase using Equation (2) discussed in section 3.5.2.1. The third part matched the blink strength using Equation (4) discussed in section 3.5.2.2. The algorithm awarded scores for every successful match, and these scores were summed up to give an overall score. This score was evaluated against a defined threshold of 70 to authenticate or reject a subject. The developed algorithm forms the main contribution of this study.

Chapter 4. Experimental Setup

4.0 Introduction

In order to meet the research objective of evaluating the performance of the developed authentication algorithm, there is a need to fulfil one important aspect of biometric authentication, which is performance. This study focuses on using the most common performance metrics being false acceptance rate and false rejection rate. The other important aspect of this study is validating the signal used for authentication against human emotions and exercise. We conducted three main experiments over a span of three (3) days with each experiment per day (see Appendix D, Figure 36); the first experiment focused on the performance of the algorithm and the second experiment focused on the validation of the signal against emotions. The third experiment focused on the effect of excessive exercise on the signal used in this study.

4.1 Performance Metrics

[60] indicated that biometric systems should measure False Rejection Rate (FRR) and False Acceptance Rate (FAR). Therefore, we adopt the same criteria to measure the performance of our proposed algorithm. FAR is the rate at which a system authorises illegitimate users, and FRR is the rate at which a system rejects a legitimate user [61]. For every authentication system, there are four possible outcomes, (1) a legitimate user is authorised, commonly denoted as True Positive (TP), (2) an illegitimate user is authorised, commonly denoted as False Positive (FP), (3) an illegitimate user is rejected, commonly denoted as True Negative (TN) and (4) a legitimate user is rejected, commonly denoted as False Negative (FN) as indicated in Table 4. According to [61], these four possible outcomes are the fundamental components for all performance metrics.

Table 4. *A summary of the fundamental components of performance metrics.*

	Legitimate User (True)	Illegitimate User (False)
System Accept (Positive)	TP	FP
System Reject	FN	TN

(Negative)		

False rejection rate, also known as false negative rate (FNR), defines the rate at which a system rejects a legitimate user as already discussed above. It is the total number of false rejections or false negative (FN) over the total number of attempts (False Negative + True Positive), as depicted by Equation (5).

$$FRR = \frac{No.of\ False\ Rejections}{No.of\ Authorized\ Attempts} * 100 \tag{5}$$

Equation (5) above is translated to Equation (6).

$$FNR = \frac{FN}{FN + TP} \tag{6}$$

False Acceptance Rate, also known as False Positive Rate (FPR), defines the rate at which a system authorises illegitimate users. It is the total number of false acceptances or False Positive (FP) over the total number of impostor attempts (False Positive +True Negative), as depicted by the Equation (7) below, which translates to Equation (8).

$$FAR = \frac{No.of\ False\ Acceptances}{No.of\ Impostor\ Attempts} * 100 \tag{7}$$

$$FPR = \frac{FP}{FP + TN} \tag{8}$$

The relative accuracy of a system is calculated using the Equation (9) below [60]. It defines the total number of denied illegitimate attempts (TN) and authorized legitimate attempts (TP) over the total number of all attempts made (FP, FP, TN & TP).

$$Accuraccy = \frac{TN + TP}{FN + FP + TN + TP} * 100 \tag{9}$$

4.2 Performance Evaluation: FRR

This section entails an experimental setup to evaluate the FFR of the proposed authentication algorithm. In this experiment, we recruited ten (10) subjects. Five (5) of them are adult females aged between 20 – 35 years. The other five (5) are adult males in the same age range. Figure 21 depicts the flowchart of the experiment.

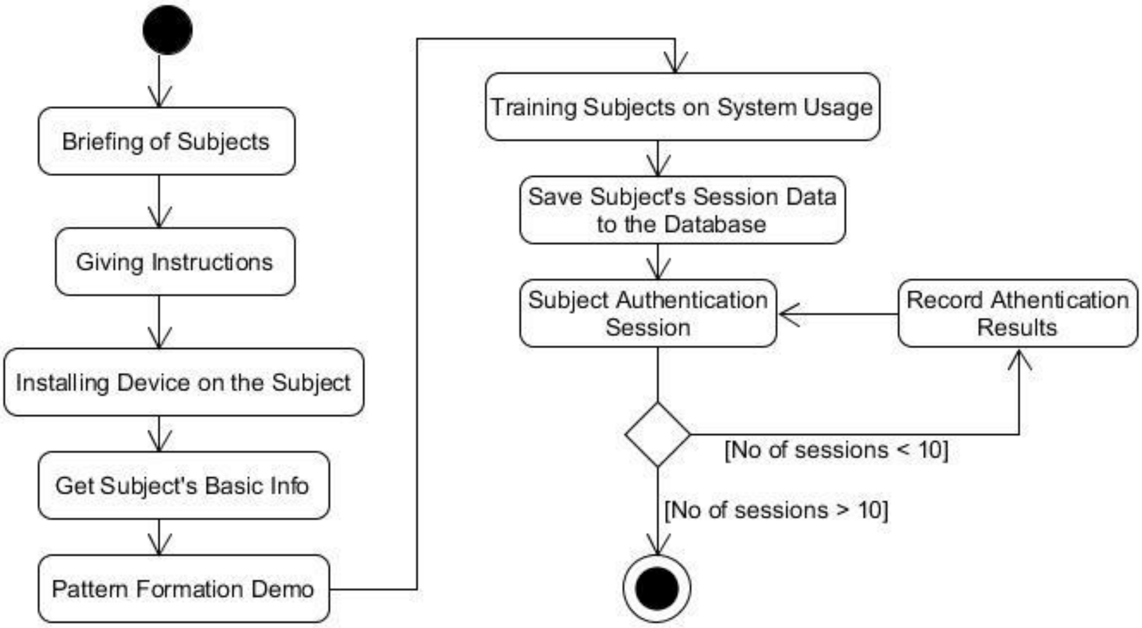

Briefing of Subjects
Giving Instructions
Installing Device on the Subject
Get Subject's Basic Info
Pattern Formation Demo
Training Subjects on System Usage
Save Subject's Session Data to the Database
Subject Authentication Session
Record Athentication Results
[No of sessions < 10]
[No of sessions > 10]

Figure 21. Experimental setup flowchart for evaluating FRR.

4.2.0 Briefing of Subjects

The first part of the experiment started with briefing the subject on the overall purpose of the experiment. The duration of the experiment was clearly stated. We explained to the subjects the tools that they were to use for the experiment and how those tools work. The tools included a NeuroSky Mindwave Mobile 2 headset and a Dell laptop. We acknowledged subjects for being part of the experiment. Consent forms were given to subjects to fill and sign, serving as a formal agreement of subjects to participate in the experiment. A sample of these forms is attached to this document (see Appendix B).

4.2.1 Giving Instructions

Before the experiment session, we distributed a guideline document that entailed detailed instructions for subjects (see Appendix C). Subjects were instructed to blink during the experiment. When subjects were in training, enrolment phase, or authentication phase, every eye blink detected (intentional or unintentional) from them was captured by the system.

Therefore, all the eye blinks from the subjects during the enrolment and authentication phase, are captured. We gave instructions on the kind of body movements and facial expressions permitted. Intensive head movement can alter the position of the EEG headset on the head. Therefore, only slight head movements were allowed where necessary. Some facial expressions, like extensively raising eyebrows during the experiment, negatively affect the EEG signal since it leads to a poor signal. Subjects were advised not to make such facial expressions.

4.2.2 EEG Headset Installation On The Subject

Before installing the EEG headset on the subject, the electrodes, together with the area where the electrodes come in contact with the subject’s skin, was cleaned with alcohol and cotton wool to remove dirt, oil, and dead skin cells that contribute to electrode impedance as discussed in Section 3.2. This procedure improves signal quality. The EEG headset was attached to the subject’s head, and it was adjusted to securely and adequately fit the subject. The reference electrode was attached to the ear lobe, and the other electrode was positioned just above the subject’s left eyebrow. This position is referred to as Fp1, according to the 10/20 International Position System, as shown in Figure 22. The device was turned on and connected to the computer wirelessly via Bluetooth. The results of the connection status were output by our custom application, as shown in Figure 23.

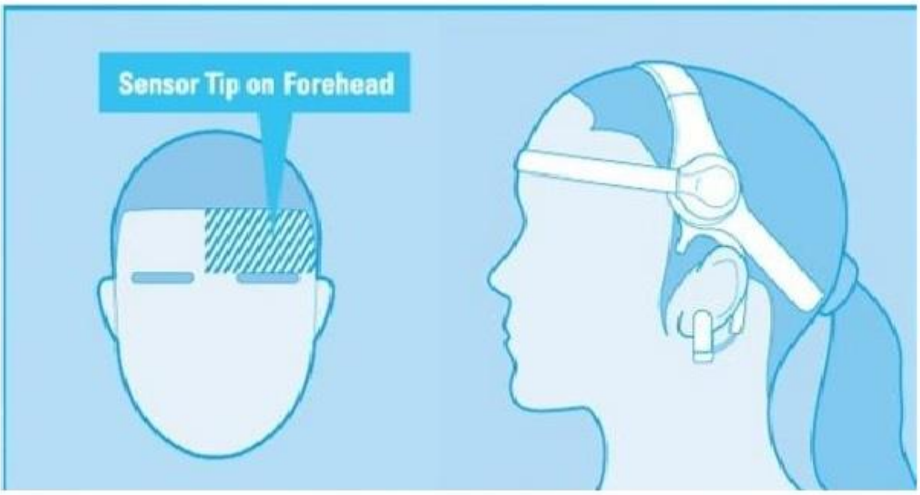
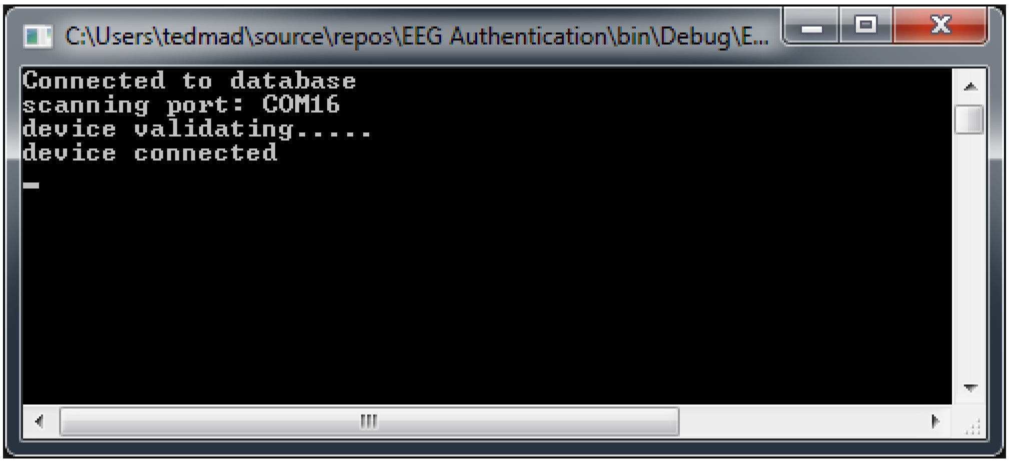


Figure 22. Headset installation position [62].


C:\Users\tedmad\source\repos\EEG Authentication\bin\Debug\E...

```
Connected to database
scanning port: COM16
device validating.....
device connected
_
```

Figure 23. NeuroSky Mind Wave mobile Bluetooth connection results.

4.2.3 Enrolling Subjects

At this stage, we registered subjects into the system. Basic information like name, surname, email, and profile image was input by the subject into the system. The information was saved in the database. The email field was used for uniquely identifying a subject in the system. This was the same field required during the authentication phase. Figure 24 below shows an interface used on the system to capture the subject's basic information.

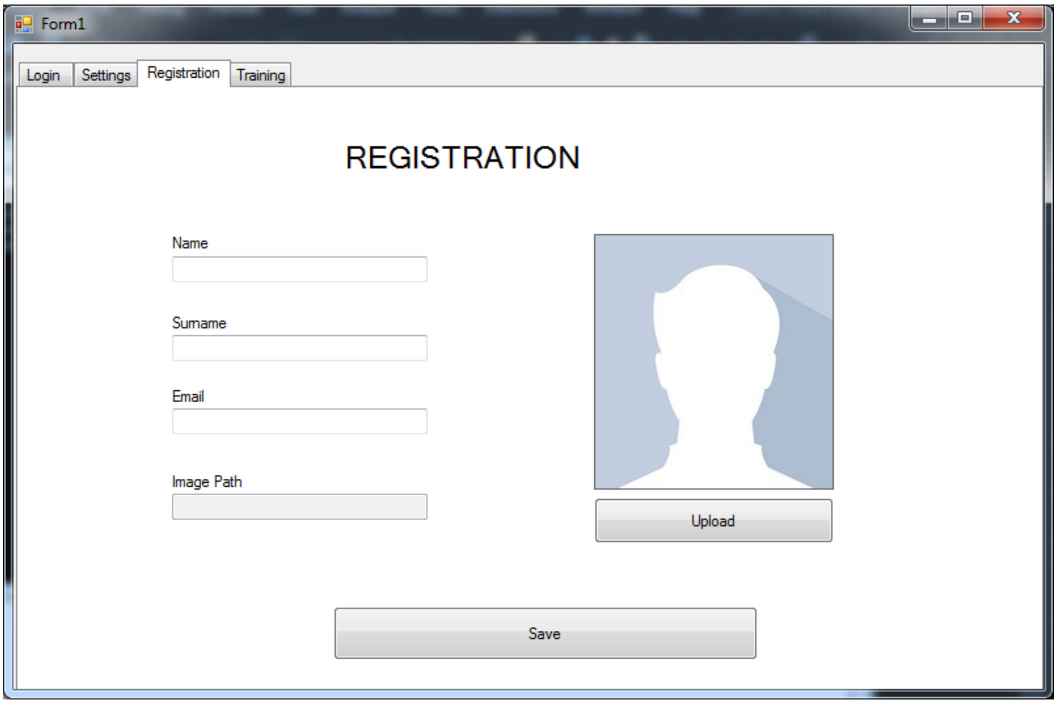


Figure 24. Registration Form for Capturing Basic Details.

4.2.4 Demonstration of Pattern Formation

We demonstrated to the subjects how a pattern (password) is made. There are three important aspects taken into account. The first aspect is the number of blinks in a given timeframe. Each subject was given ten (10) seconds to form a pattern from eye blinking. This pattern was the password for the subject. The number of blinks on a given timeframe of 10 seconds formed part of the password attributes. The other aspect was blink strength. Every eyeblink has a value that indicates its strength. Therefore, how soft or strong the blink is, is determined by this value. The third aspect is the blink time. As discussed in the previous chapter, this is the timestamp of a recorded eye blink within the given 10 seconds timeframe. Therefore, based on these three aspects, we demonstrated how an authentication pattern is formed. We made this demonstration in words and diagrams. Figure 25 below shows the diagram used in the demonstration.

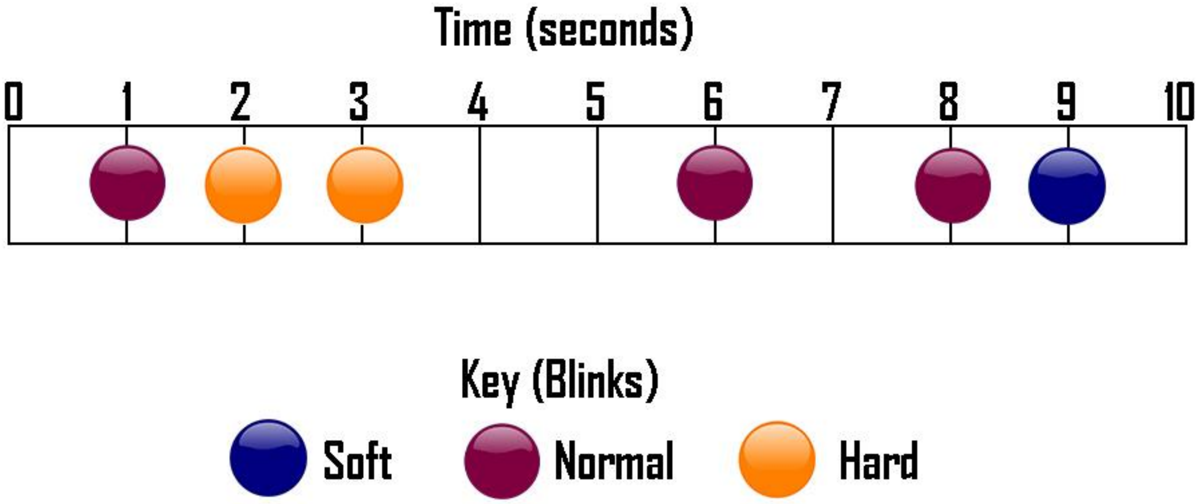
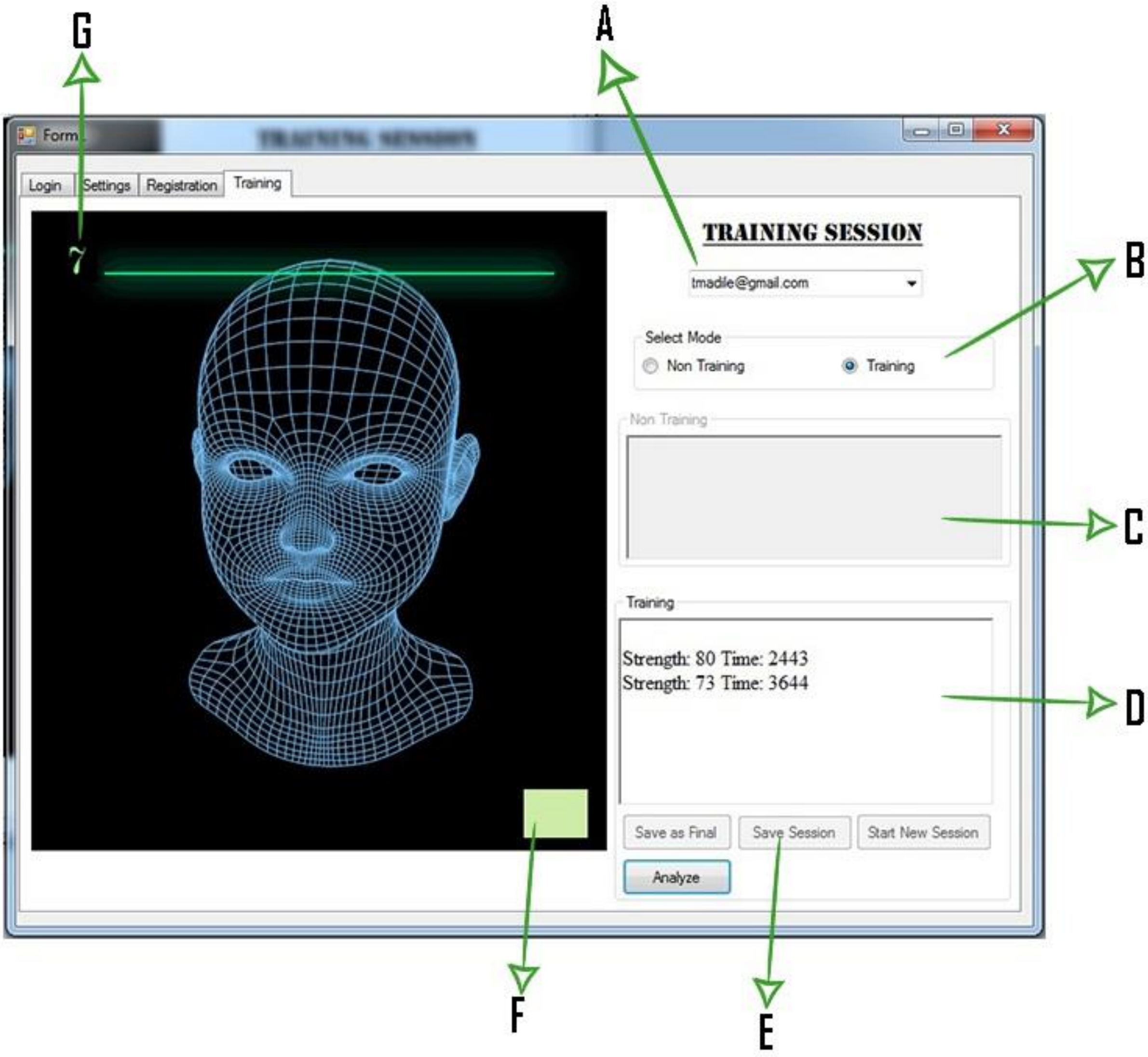


Figure 25. Demonstration of Pattern Formation

Figure 25 above shows a demonstration of pattern formation. The numbers 1 to 10 indicate the duration of the session in seconds. The coloured dots symbolise a blink that occurred at a given time. The colours of the dots depict the type of strength a blink has. A blue dot indicates a soft blink. A maroon dot indicates a normal blink. An orange dot indicates a hard blink. Figure 25 indicates that there was a normal blink a second from the start of the session, followed by two hard blinks in the second and third seconds. Another normal blink occurred at the 6th and 8th seconds, followed by a soft blink at the 9th second.

4.2.5 Training Subjects

When a thorough demonstration of the pattern formation process was completed, subjects were trained on how to form a pattern on a real-life system. They were given time to familiarize themselves with the system. They were walked through the system. Every part of the system was explained in detail how it works. Then they were given time to practise their pattern as many times as they felt confident and comfortable. Figure 26 shows important parts of the system that the subjects need to be familiar with.



tmadile@gmail.com

Select Mode: ○ Non Training ● Training

Strength: 80 Time: 2443
Strength: 73 Time: 3644

Figure 26. Important Sections of the System.

Part A: This is the area where the subject selects his email. This email field is crucial when saving the subject's data to the database since it forms a unique identifier for the subject.

Part B: This area consists of two (2) modes, “non-training” and “training”. The training mode, or the practice mode, is the mode where the subject familiarises himself with the system. None of the subject’s data is recorded when this mode is selected. The subject can perform as many trials as possible to get a feel of how the application and the device respond to his actions. The non-training mode is the mode where the subject makes the pattern that is to be saved in the database. This mode gives the subject the actual feel of what to expect when he/she is later authenticating into the system. It gives the subject a timeframe of 10 seconds to formulate a pattern.

Part C: This is the area where training data is displayed. Every data that is recorded from the subjects is displayed here, including blink time and blink strength.

Part D: This is where the non-training data were displayed. Every data recorded from the subject was displayed here, including blink time and blink strength. This part serves the same purpose as “part-c”, but they have been separated to reduce confusion on the subject. The difference between the two is that this “part d” only displays data within 10 seconds. After that, whatever data comes is disregarded unless another 10 seconds session is started.

Part E: This part consists of four sections. The first one being the “save as final” button which saves the 10-seconds data in the database. The second section being the “save session” button, does the same function as the “save as final” button, except that it saves data on a separate table in the database, and multiple session data can be saved. The “start new session” button clears data displayed in “part d” and resets the 10 seconds timer. This is useful in case the subject makes a mistake while trying to do his final trial. The last section being the “analyse” button, calls the authentication algorithm to match the previously saved data against the current session data.

Part F: This part indicates that a blink has been detected. It changes colour with every occurrence of a detected blink. It helps the subject to easily notice the blink has been detected while he is focused on the countdown timer.

Part G: This part indicates the duration of the session. It is a countdown timer. Subjects use it to time their blinking while forming a pattern.

Save Session Data

At this stage, the subject is confident enough about the pattern he formed. He uses the "save as final" button to save the session data.

4.2.6 Authentication

The login screen was presented to the subject. This screen has some of the features that are similar to the one at the enrolment phase. This includes the countdown timer and the field where the subject inputs the email. The subject was given a timeframe of 10 seconds to repeat the pattern previously saved in the system at the enrolment stage. At the end of the 10 seconds, the subject clicked the log in button. Then the authentication algorithm matched the data previously stored in the database with the data captured while the subject was logging in. The system then presents the subject with a "Login successful" message if the subject got the pattern correct. Otherwise, an "Unsuccessful Login" message was displayed.

4.3 Performance Evaluation: FAR

This section entails an experimental setup to evaluate FAR of the proposed authentication algorithm. The experiment involved an impostor who observed a true subject login into the system. The impostor attempted to mimic a true subject. Figure 27 shows a flowchart of this experiment.

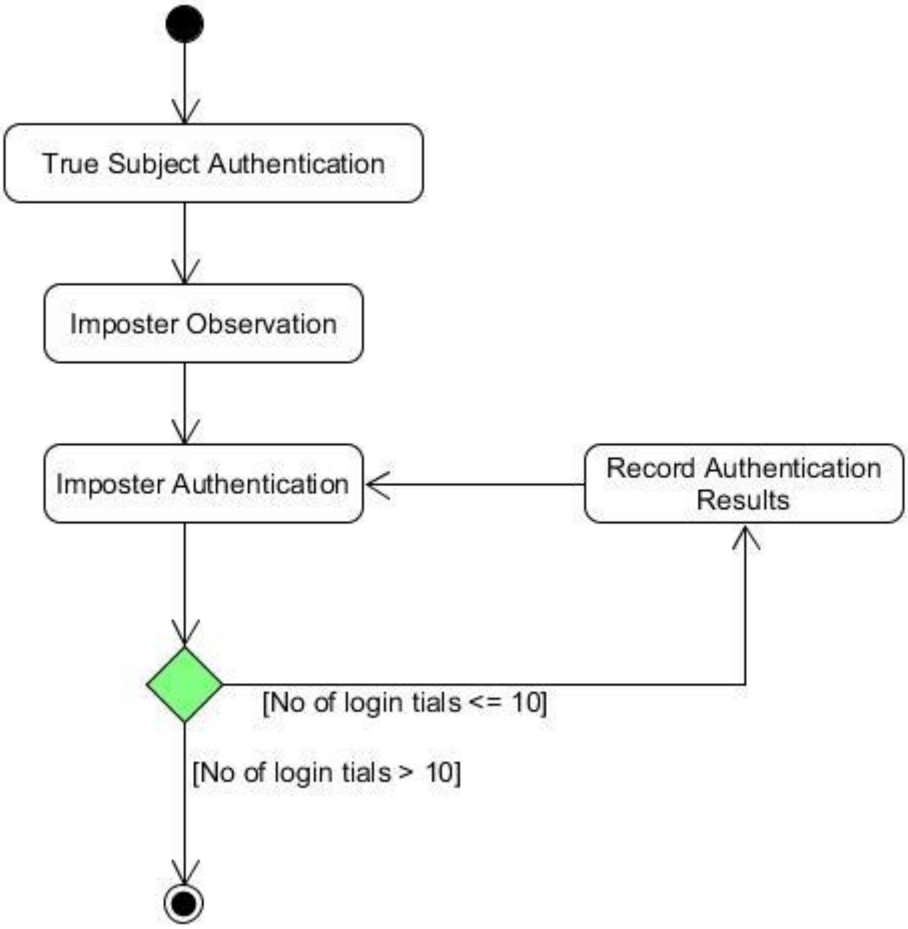

True Subject Authentication
Imposter Observation
Imposter Authentication
Record Authentication Results
[No of login tials <= 10]
[No of login tials > 10]

Figure 27. Experiment 2 flowchart for evaluating FAR.

4.3.0 True Subject Authentication

The experiment starts with a true subject login to the system. These are the subjects previously recruited and trained to use the system.

4.3.1 Impostor Observation

One of the ten recruited participants was selected to act as an impostor. For each session, a different subject was used as an impostor. The reason for selecting an already existing subject is that he is familiar with the system and has gone through training. In a real-life scenario, an impostor takes time to study and learn the system. Therefore it would not be ideal to use a subject who has no idea of how the system works. The subject who acts as an impostor is allowed to observe a subject who is authenticating.

4.3.2 Impostor Authentication

After an impostor has observed a true subject login to the system, he was allowed to log in to the system. The impostor was given ten (10) tries to log into the system. If the impostor failed to log into the system, it was recorded as a false negative (FN). Otherwise, a false positive (FP) was recorded. The same scenario was repeated for the other nine (9) subjects, each with a distinct impostor such that every subject also acted as an impostor.

4.4 Effect of Emotions on Our Proposed Approach Experiment

One of the significant challenges in EEG authentication is its sensitivity to emotions, which negatively affects the performance of EEG based authentication systems [52]. In this experiment, we analysed the effect of emotions on our proposed approach. We focused on three key emotions being sadness, excitement, and calmness [52]. We used a 2D model that is suitable for the analysis of emotions using psychological signals, according to [63] and [28]. This model presents emotions in a two-dimensional space, where arousal is in the vertical axis and valance in the horizontal axis [63], as depicted in Figure 28. Valence, in this case, refers to an individual's judgment on a given situation in terms of positivity and negativity, while arousal refers to the expression of one's degree of excitation [29].

This model is commonly used in EEG-based emotion recognition [64],[65],[66]. Therefore we use it in this research to refer to the meaning of distinct emotional states.

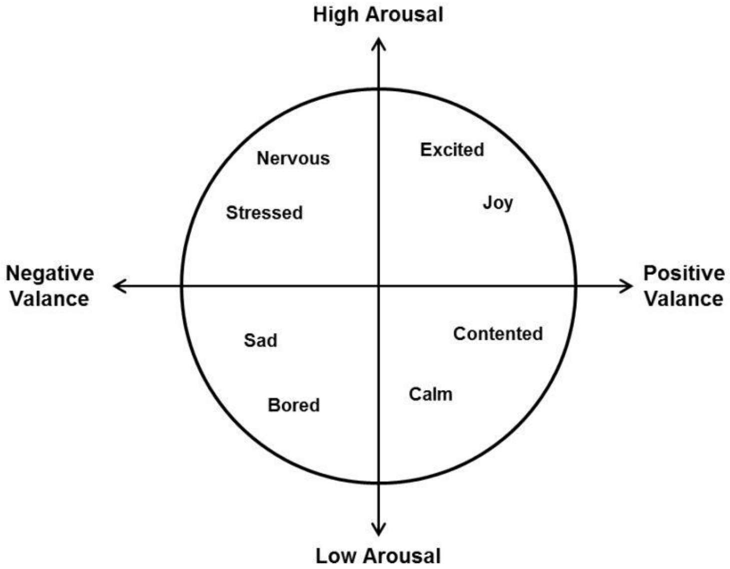


Figure 28. Emotion analysis 2D model [52].

4.4.0 Experimental Setup

In this experiment, subjects were shown short music video clips intended to change their emotional state. These videos were played on a Dell Laptop, and a subject was put on a comfortable office chair. The laptop was placed a meter away from the face in an office set-up. Three categories of videos were used, and each category consisted of two (2) music videos. The first category consisted of videos that stimulated emotions of excitement on the subject. The second and third category consisted of videos that stimulate the subject's emotional state to sadness and calmness, respectively. After every category, we asked subjects to authenticate, and their authentication results were recorded.

The videos used in this experiment were from the DEAP dataset [67]. A formal request was sent to seek consent to use the videos in our study. This request is attached (see Appendix A, Figure 34), and proof of authorisation mail is also attached (see Appendix A, Figure 35). The dataset consisted of 120 YouTube music videos collected using online self-assessment and were rated from an experiment. The experiment consisted of 14 – 16 volunteers, and it was based on arousal, valance, and dominance. From a pool of one hundred and twenty (120) videos, we selected six (6) videos under the category of "exciting", "calm" and "sad". Each category had two videos that were selected based on the highest ratings.

We used subjects already enrolled in the system because they were trained on how to use the system. Figure 29 depicts the flow chart of the experiment process mentioned above.

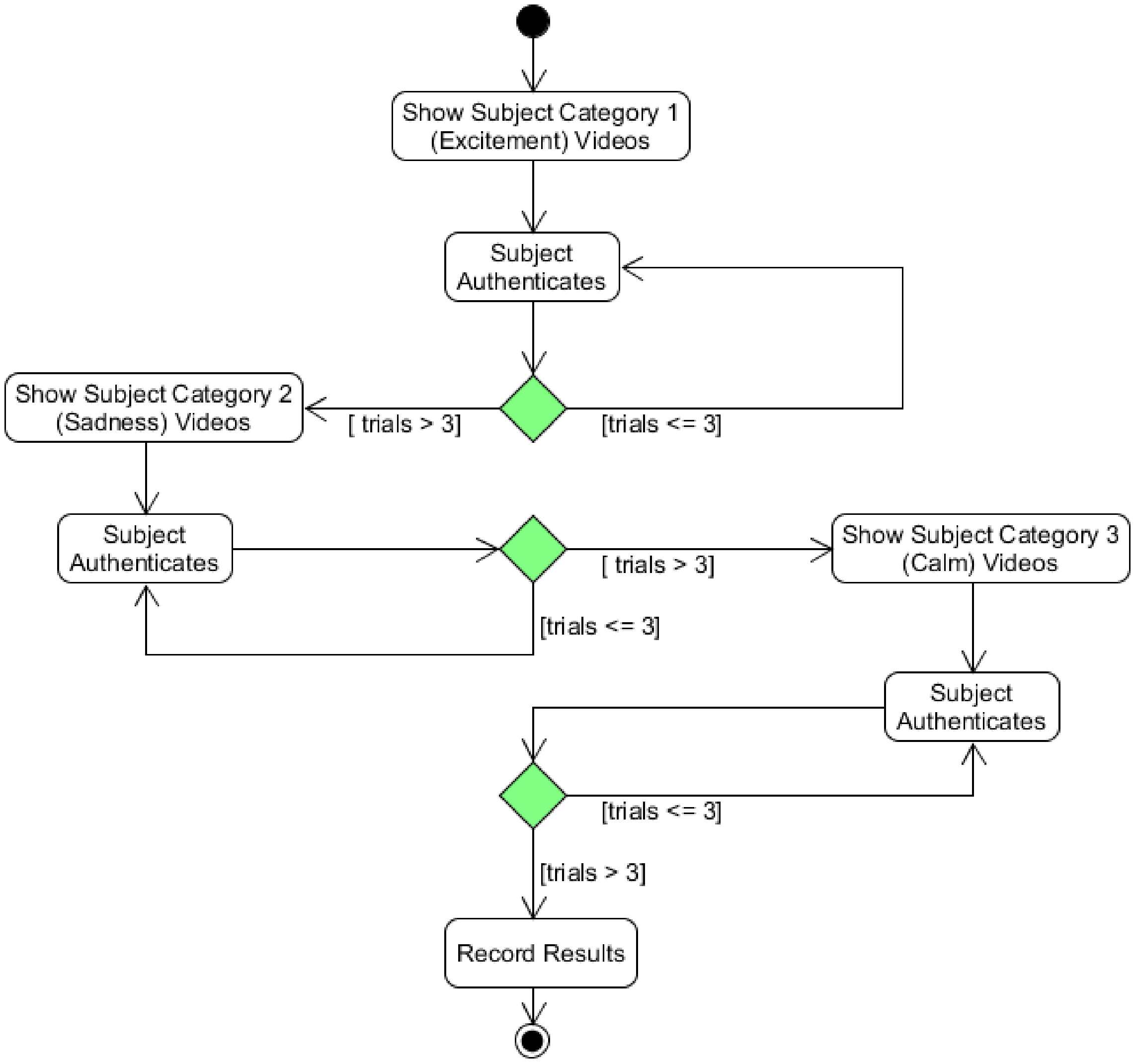


Figure 29. A flowchart for the effect of emotions experiment.

At the beginning of the experiment, we presented three different videos to the subject. The videos are played on a Dell Laptop with an external keyboard and mouse attached to it while the subject is seated on a comfortable office chair. The specifications of the laptop used for playing videos are mention in Section 3.2.1. The laptop was placed on a computer desk such that the face of the subject was approximately one meter from the display. A set of two (2) videos that fall in the same category were played, and the subject watched them. The first category contained two (2) videos that, according to a study by [32], trigger excitement emotions in an individual.

At the end of each video watching session, a subject was requested to rate the effect of the videos on his emotions. This task was necessary as it acted as a confirmation of a triggered emotion. If the subject confirmed that the videos excited him, the authentication session followed. Otherwise, another group of two (2) videos were selected from the "DEAP dataset [32]" and the watching session repeated. At the authentication phase, a subject was given three trials, and another group of videos that trigger sadness was presented. The same process is repeated for the sad and calm video categories. In the end, results were recorded.

4.5 Effect of Exercise on Our Proposed Approach Experiment

The effect of exercising has an impact on the brainwave signal [26], [54], [27]. Therefore, the performance of authentication algorithms that use this signal can be affected by this effect. We conducted an experiment on the effect of exercising on our proposed authentication algorithm. We used the same ten (10) subjects used for the other two experiments. Subjects were engaged in a rope skipping exercise, with a smart bracelet attached to their wrist for heart rate capturing. We used the heart rate to determine how intensive the exercise was. After the rope skipping exercise, subjects immediately authenticated into the system and their authentication results were recorded.

4.5.0 Experimental Setup

Flow Chart

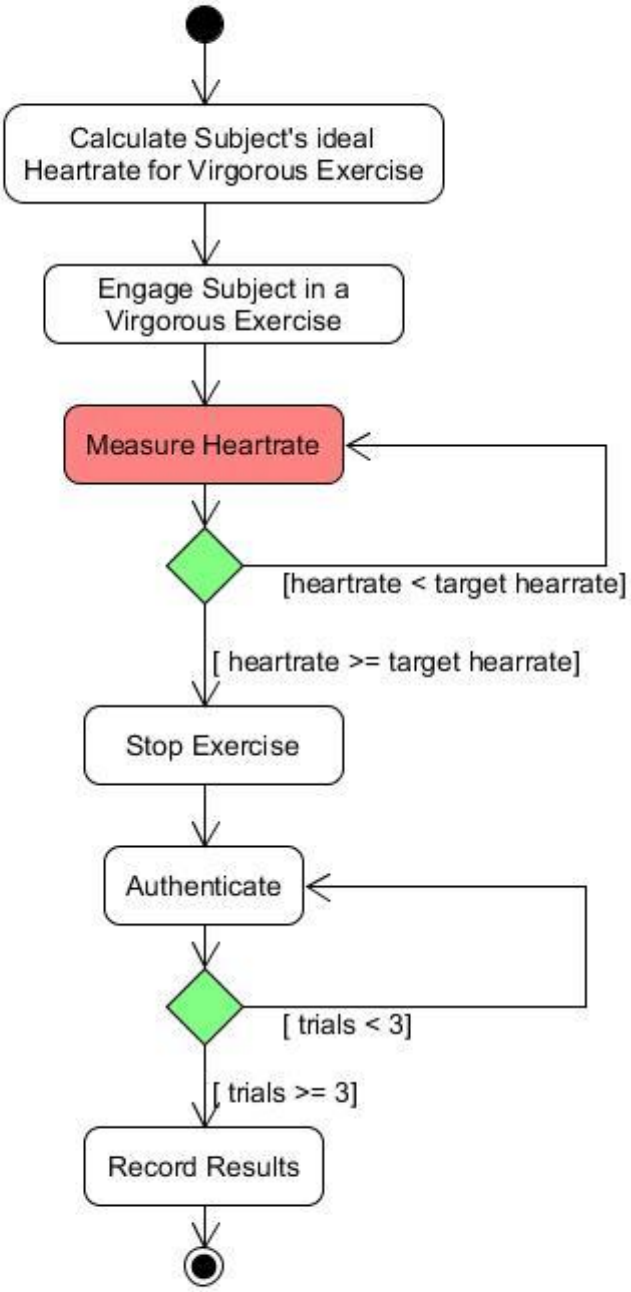

Calculate Subject's ideal Heartrate for Virgorous Exercise
Engage Subject in a Virgorous Exercise
Measure Heartrate
[heartrate < target hearrate]
[heartrate >= target hearrate]
Stop Exercise
Authenticate
[trials < 3]
[trials >= 3]
Record Results

Figure 30. Flow chart for the effect of exercising experiment.

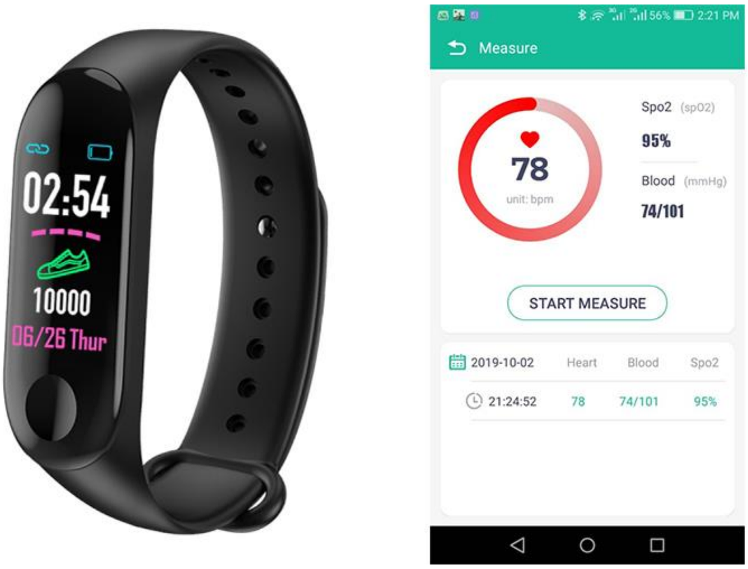
The first part of the experiment started with determining the ideal heart rate of the subject for an exercise. We used Equation (10) by [68], to calculate the maximum heart rate of the subject.

$$HRmax = 208 - 0.7 * age \tag{10}$$

To determine the subject's ideal heart rate for a vigorous exercise, we used 70% of the subject's maximum heart rate as the target heart rate and recorded it as depicted by Table 5. At the beginning of the exercise, we attached a smart bracelet to the subject's hand and paired it with a mobile phone via Bluetooth. The bracelet used was an M3 Smart Bracelet Fitness Tracker with a built-in Heart Rate sensor and monitor. The FitPro android application, downloaded from Google Playstore, was installed on the mobile phone and paired with the bracelet. We used the FitPro app to capture heart rate recordings from the smart bracelet. The M3 smart bracelet and the FitPro application are shown in Figure 31. The subject started the rope skipping exercise, and the heart rate recording started. The exercise continued until a defined desired heart rate value was reached. The subject was then given three (3) trials to authenticate, and the results were recorded.

Table 5. *Heartrate results after the robe skipping exercise*

Subject	Age	Max Heart Rate	Target Heart Rate (70%)	Actual Heart Rate
S1	19	194.7	136.29	155
S2	21	193.3	135.31	150
S3	20	194	135.8	148
S4	28	188.4	131.88	145
S5	28	188.4	131.88	152
S6	33	184.9	129.43	149
S7	29	187.7	131.39	145
S8	23	191	133.7	143
S9	29	187.7	131.39	149
S10	29	187.7	131.39	151



Measure

78 unit: bpm

Spo2 (sp02) 95%

Blood (mmHg) 74/101

START MEASURE

2019-10-02	Heart	Blood	Spo2
21:24:52	78	74/101	95%

Figure 31. M3 Smart Bracelet Fitness Tracker (left) and FitPro App (right)

Chapter 5. Results and Discussion

5.0 Introduction

This chapter presents detailed results of the experiments conducted in Chapter 4. A discussion of these results is also done in this chapter. Three main experiments were conducted in the previous chapter. The first experiment investigated the performance of the proposed algorithm. The results and discussion of that experiment in Section 4.2 and 4.3 form the first section of this chapter. The second section of this chapter entails results and discussion of the experiment investigating the effect of emotions on the proposed algorithm in Section 4.4 of the previous chapter. The third section of this chapter entails results and discussion of the experiment that investigated the effect of exercise on the proposed algorithm in Section 4.5 of the previous chapter. The last section of this chapter outlines a summary of results and discussions.

5.1 Performance Results

The algorithm performance results are shown in this section. Table 6 below depicts authentication results for ten (10) subjects and ten (10) impostors for the experiment mentioned in Section 4.2 and 4.3 of Chapter 4. These results are plotted in a bar graph, as depicted in Figure 32.

Table 6 depicts the authentication results recorded from the experiment mentioned above. It shows the ten (10) trials that each participant was engaged in. Two (2) categories of participants are shown in the table, denoted as “s_#” and “i_#” for subject identification number and impostor identification number, respectively. The table depicts authentication results for the ten subjects and ten impostors. The last column shows the average results of the ten (10) trials of each participant. The second column depicts the total number of blinks per trial used to formulate an authentication pattern.

Table 6. *Authentication algorithm results*

Subject ID	No of blinks	Trial 1	Trial 2	Trial 3	Trial 4	Trial 5	Trial 6	Trial 7	Trial 8	Trial 9	Trial 10	Average
s_ 1	4	77	77	91	77	70	70	77	77	84	25	72.5
i_1	-	61	46	68	61	76	61	62	69	54	54	61.2
s_2	11	94	97	94	97	94	85	94	97	97	88	93.7
i_2	-	0	0	0	82	0	0	63	0	0	63	20.8
s_3	8	84	87	84	81	84	90	87	87	78	84	84.6
i_3	-	33	0	0	33	26	0	57	29	32	32	24.2
s_4	6	85	85	90	95	90	90	95	95	100	100	92.5
i_4	-	60	55	60	55	0	60	45	40	50	30	45.5
s_5	8	92.5	92.5	96.25	88.75	92.5	92.5	92.5	92.5	100	96.25	93.6
i_5	-	47.5	25	62.5	58.75	28.75	25	58.75	25	73.5	62.5	46.7
s_6	8	92.5	92.5	88.75	88.75	88.75	92.5	96.25	96.25	92.5	96.25	92.5
i_6	-	58.75	58.75	40	32.5	47.5	28.75	32.5	32.5	40	17.5	38.7
s_7	6	85	100	90	95	90	90	90	100	100	100	94.0
i_7	-	30	90	30	55	40	35	40	35	50	40	45.5
s_8	9	88.75	85	88.75	88.75	85	92.5	88.75	88.75	92.5	92.5	89.1
i_8	-	0	55	66.5	58.75	62.6	47.5	0	62.5	47.5	51.25	45.1
s_9	8	85	92.5	92.5	92.5	85	81.25	96.25	96.25	100	96.25	91.7
i_9	-	0	0	58.75	0	0	0	58.75	66.25	58.75	70	31.3
s_10	5	82	70	94	88	82	88	82	88	88	100	86.2
i_10	-	64	40	58	46	40	64	34	82	64	0	49.2

Figure 32 shows a summary of the authentication results in Table 6. The vertical axis represents the average algorithm score of ten (10) trials per subject. The horizontal axis represents the subjects who took part in the experiment.

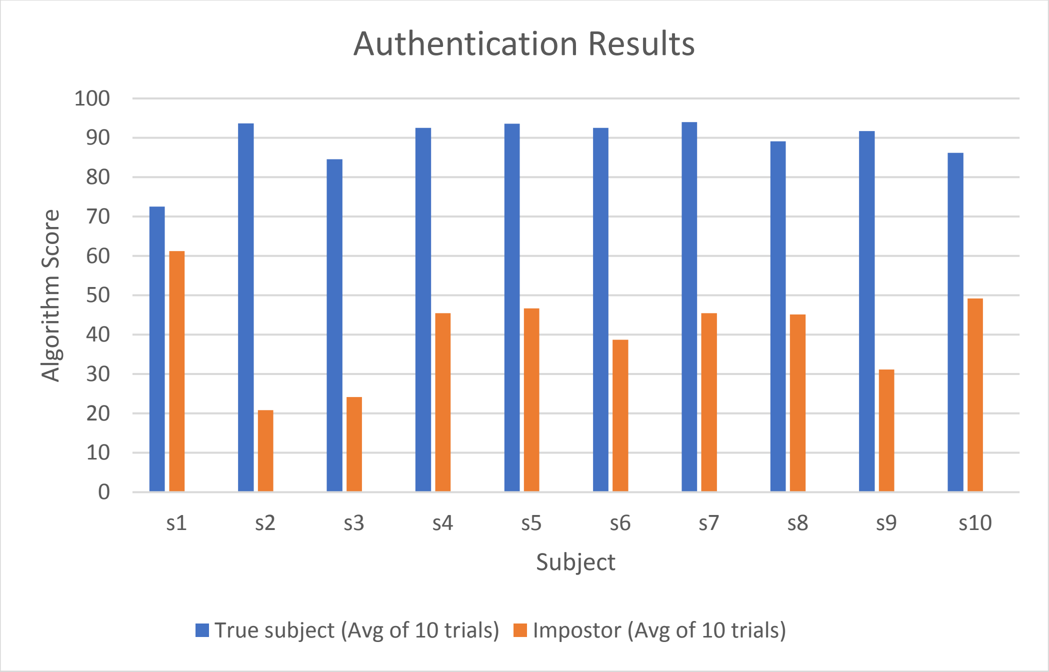


Figure 32. Authentication algorithm results (summary)

The blue bars in Figure 32 represent the algorithm results of a true subject who authenticated over an average of 10 trials per session. The orange bars represent the algorithm results of an impostor who attempted to authenticate over an average of 10 trials per session. The chart summarizes the authentication results of ten (10) subjects, of which ten (10) were true subjects, and ten (10) were impostors. The total number of authentication attempts was two hundred (200). The chart shows a record for the results obtained from an experiment discussed in sections 4.2 and 4.3. It shows the results of all the ten (10) trials that each “true subject” and “impostor” obtained. The average of all the ten (10) trials is displayed in the average column in Table 6. This average was used to plot the chart above.

The highest average score for the impostor is “61.2” and “49.2” for impostor 1 and 10, respectively. The scores obtained are related to the complexity of the authentication pattern of a subject. The number of blinks for a particular person is related to the complexity of the pattern. A fewer number of blinks in a pattern indicates a less complex pattern. It can be observed from Table 6 that the highest recorded impostor scores have the lowest number of blinks associated with a pattern. Subject 1 recorded the lowest number of blinks of four (4), and impostor 1, who corresponds to subject 1, scored the highest score of “61.2”. Similarly, subject 10 with the second-lowest number of blinks of five (5) corresponds to impostor 10 with the second-highest scores of 49.2. This indicates that the complexity of the pattern affects the performance of the algorithm.

It can also be observed that the last two (2) sessions being “trial 9” and “trial 10”, recorded higher scores for subjects other than impostors. Subject 4, 5, 7, and 9, recorded maximum scores of 100 in trial 9. Subject 4, 7, and 10 recorded maximum scores in trial 10. This scores indicates that the more subjects practice their pattern, the more they get better at getting it right. These results imply that for better performance or higher accuracies, subjects need more training sessions, as it can be seen that it improves their scores.

Table 7 shows the True Positive, False Negative, False positive, and True Negative denoted as TP, FN, FP, and TN, respectively. These are the four (4) fundamental performance metric components, as discussed. The figures in the table below are derived from Table 6. They are the figures that are essential for calculating FAR, FRR, and Accuracy.

Table 7. *Performance metric results (TP, FN, FP, TN)*

Subject	TP	FN	FP	TN
1	9	1	1	9
2	10	0	1	9
3	10	0	0	10
4	10	0	0	10
5	10	0	1	9
6	10	0	0	10
7	10	0	1	9
8	10	0	0	10
9	10	0	1	9
10	10	0	0	10
Total	99	1	5	95

Table 8 shows the False Acceptance Rate, False Rejection Rate, and Accuracy denoted as FAR, FRR, and ACC, respectively. These values are calculated using the formulas discussed in Section 4.1. The table shows the FAR, FRR, and ACC for each of the ten (10) subjects who took part in the experiment.

Table 8. *Performance metric results (FAR, FRR & ACC)*

Subject	FAR	FRR	ACC
1	10%	10%	90%
2	10%	0%	95%
3	0%	0%	100%
4	0%	0%	100%
5	10%	0%	95%
6	0%	0%	100%
7	10%	0%	95%
8	0%	0%	100%
9	10%	0%	95%
10	0%	0%	100%

Table 9 depicts the mean results for all the ten (10) subjects. It shows the mean False Acceptance Rate, False Rejection Rate, and Accuracy.

Table 9. *Mean performance metric results (FAR, FRR & ACC)*

Performance Metric	Results
FAR	5%
FRR	1 %
ACC	97%

Results depicted by Tables 7, 8, and 9 carry significant insights. It can be observed in Table 8 that at least 50% of subjects being subject 3, 4, 6, 8, and 10 achieved an accuracy of 100% with 0% FAR and FRR. This performance indicates that the proposed approach has the potential of achieving the maximum average accuracy. These are the expected results since similar studies [7], [16], [17], [18], and [19] indicated in Chapter 2 also achieved the same maximum accuracy. It is difficult to compare the performance with other studies because various studies evaluate performance differently. However, with the few studies that evaluated their performance similar to this study; ACC, FAR, and FRR, [47] reported ACC of 86.1%; FAR of 13.9%; FRR of 13.9%. Our study showed better mean performance. Another study by [55], reported ACC of 97.5%, FAR of 3.9%, and FRR of 3.87%. The performance is higher in terms of ACC and FAR; however, our study reported a better FRR of 1%.

With regards to ACC alone, studies [47] and [48] reported ACC of 86.1% and 92%, respectively. The said studies showed lower accuracy than our proposed authentication algorithm. However, there are other EEG based authentication studies [7], [19], [46], and [50] that recorded and accuracy above 97%. In comparison with existing studies, the accuracy we achieved is good and is promising. Training sessions can be increased to improve the overall performance of the proposed algorithm.

5.2 Effect of Emotions Results

The results of an experiment discussed in Section 4.4 regarding the effect of emotions on the performance of the proposed algorithm are shown and discussed in this section. Table 10 depicts the recorded results from the said experiment.

Table 10. *Authentication results for excited, sadness, and calm emotions*

Subject ID	**Algorithm Score (Excited)**				**Algorithm Score (Calm)**				**Algorithm Score (Sadness)**			
	t_1	t_2	t_3	Avg	t_1	t_2	t_3	Avg	t_1	t_2	t_3	Avg
S1	77	70	70	**72.3**	70	80	70	**73.3**	70	77	70	**72.3**
S2	97	94	88	**93**	94	97	88	**93**	88	94	97	**93**
S3	81	84	90	**85**	87	78	84	**83**	81	84	90	**85**
S4	90	90	95	**91.7**	90	100	85	**91.7**	90	95	95	**93.3**
S5	96.25	88.75	92.5	**92.5**	92.5	92.5	96.25	**93.75**	92.5	96.25	92.5	**93.6**
S6	88.75	92.5	96.25	**92.5**	92.5	92.5	88.75	**91.25**	92.5	92.5	92.5	**92.5**
S7	85	100	100	**95**	90	95	95	**93.3**	90	100	90	**93.3**
S8	88.75	85	92.5	**88.75**	88.75	88.75	92.5	**90**	85	92.5	92.5	**90**
S9	92.5	96.25	85	**91.25**	85	92.5	96.25	**91.25**	92.5	92.5	96.25	**93.75**
S10	82	94	82	**86**	82	82	94	**86**	88	100	82	**90**

Table 10 shows authentication results for the ten (10) subjects who participated in the said experiment. The first column indicates subject identification. The second, third, and fourth columns denoted as “t_1”, “t_2” and “t_3” indicate the subject’s scores for the “excited” category during trials 1, 2, and 3, respectively. The fifth column is the average of the scores for the mentioned three (3) trials. The same analogy applies to the rest of the two categories being “calm” and “sadness”.

From Table 10, it was observed that the average algorithm score for all the three emotions is not equal for all trial sessions except for subject 2. That is expected. It is important to note that the difference does not necessarily imply that emotions impacted the performance of the algorithm. The difference is caused by how hard or complex the authentication pattern was for the subject. It has been observed during the training session that subjects had a challenge in matching their pattern with the pattern previously recorded in the database. For this reason, with every attempt, subjects strived to improve their performance, therefore making some adjustments to score the best possible scores hence the difference.

However, this research presents an ideal way to analyse these results despite the challenge mentioned above. We shy away from using the average as a basis for comparison; instead, we compare individual values for every trial conducted. It can be observed that subject 1 scored 70 at least twice in each category (excitement, calm, sadness). Subject 2 scored the same scores on average across all the three categories. It was observed that in subject 4 scored 90 for every first attempt in each category. Based on these facts, we can conclude that if emotions had an impact on the performance of the algorithm, we could not be having these matching scores across every category of emotions.

Furthermore, subject 4 obtained a score of 100 in the excited and sadness category. These scores indicate that the emotions of excitement and stress have no impact on the performance of the algorithm. Adding on to that, subject 4 also scored 100 in the calm category. This score also indicates that the emotion of calmness does not have a negative impact on the performance of the algorithm. Based on these facts, we can conclude that emotions of excitement, calmness, and stress have no significant negative impact on the performance of our proposed algorithm because the experiment recorded a maximum score for that particular emotion and subject.

5.3 Effect of Exercise Results

This section shows and discusses the experiment results mentioned in Section 4.5 regarding the effect of emotions on the performance of the proposed algorithm. Figure 33 depicts the recorded results from the said experiment.

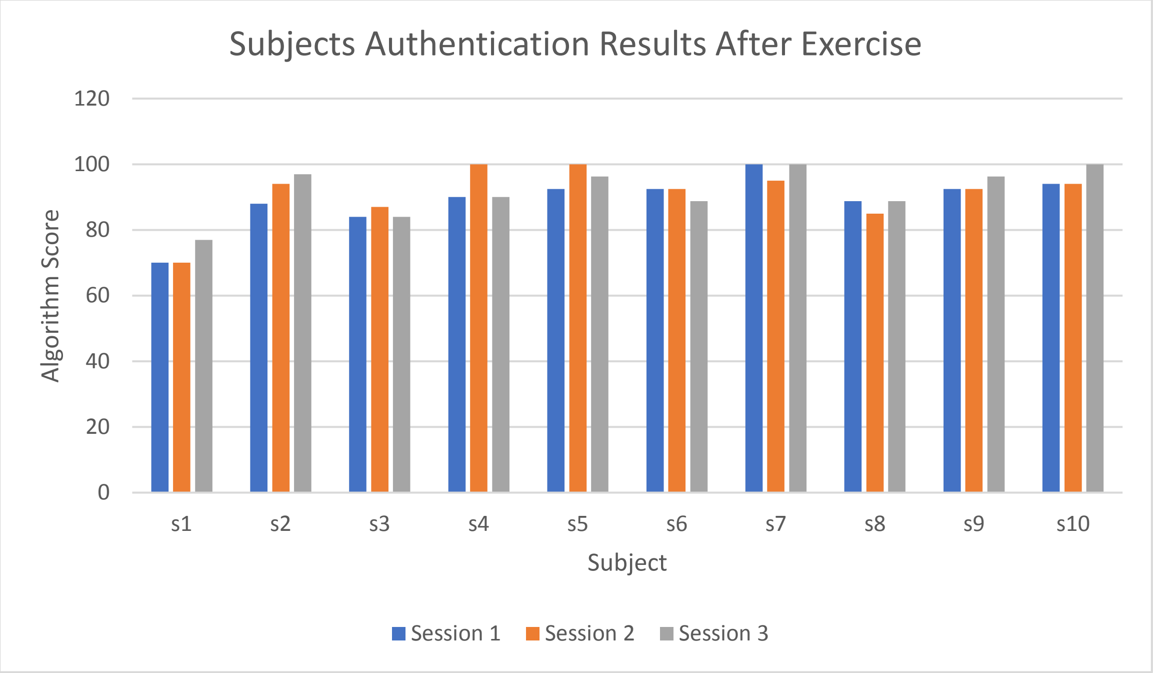


Figure 33. Subjects authentication results after exercise

Figure (33) depicts results recorded after a rope skipping session for the ten (10) subjects who took part in the experiment. The vertical axis represents the average algorithm score, while the horizontal axis represents the subjects who took part in the experiment for the three (3) exercise sessions. The blue, orange, and grey bars in the chart above represent the algorithm results for sessions 1, 2, and 3 respectively for a given subject. The chart summarizes the authentication results of 10 subjects, where each subject took three (3) trials for each session. The total number of trials for the results shown in the chart above is 30. From the graph above, this study observed that for a specific subject, scores obtained from each trial were not consistent. However, this does not imply that exercising affects the scores. It is associated with the complexity of the subject’s authentication pattern, as already discussed.

In all trials conducted as depicted in the graph above, all subjects were able to authenticate. Furthermore, the subject “s4”, “s5” and “s7” recorded at most 100. Therefore, we can safely conclude that exercising conducted for this experiment had no negative impact on the performance of our proposed approach. However, this does not mean that exercising has no impact at all. It may have a positive impact since it is associated with improved mental focus. The positive impact of exercising cannot be discussed because it is beyond the scope of this study.

5.4 Summary

The overall results for our proposed authentication algorithm depict an accuracy of 97%. EEG based authentication studies [47] and [48] reported an accuracy of 86.1% and 92%, respectively. The said studies showed lower accuracy than our proposed authentication algorithm. However, there are other EEG based authentication studies [7], [19], [46], and [50] that recorded and accuracy above 97%. In comparison with existing studies, the accuracy we achieved is good and is promising. We found out that more training sessions have a significant improvement in the performance. We found out that the major contributing factor in the performance lies in the complexity of the authentication pattern. Simple patterns are more prone to false positive (FP) which means illegitimate users being accepted by the system. Furthermore, our proposed approach was evaluated against the effect of emotions and exercise and results showed that there was no significant negative impact on the performance. This indicates that our approach has proven its practicability and usability.

6.0 Conclusion & Further Work

In this chapter, we review a summary of the work performed in this study and present suggestions for further work.

6.1 Conclusion

EEG based biometric authentication methods face a significant challenge that arises from the effect of physiological artefacts being emotions and exercising. These physiological artefacts inherently alter the EEG waveform leading to an increase in false rejection rate for EEG authentication systems. Therefore, making them less practical despite their high-security advantage. This study was set out to address this gap by using the EEG blink artefact to formulate a biometric authentication method that has the security advantage of conventional EEG authentication methods, yet overcoming the challenges of emotions and exercising. Experimental results described in Chapter 5 depicts that we achieved the specific objectives outlined in Chapter 1.

The EEG signal was collected using a Neurosky Mindwave Mobile 2 device. The acquired signal went through the pre-processing stage where Notch filter, High-pass filter, and Low-pass filter were applied. The data were sampled at a rate of 512Hz. Three data features being blink time, blink number, and blink strength were selected. A pattern-matching algorithm (authentication algorithm) was developed. This algorithm matched the data recorded at the authentication phase against the data from the database that was previously recorded at the enrolment stage, and authentication results were output on a scale of zero to one hundred (0 - 100). The algorithm is comprised of three sub-algorithms. The first sub-algorithm matched the number of blinks, and the second algorithm matched blink strength while the third sub-algorithm matched the blink time. A score distribution was defined at 10%, 30%, and 60%, respectively, and an overall score threshold of 70 was set to authenticate a subject.

Three sets of experiments were conducted to evaluate the performance of the developed algorithm. In the first experiment, we used the False Acceptance Rate and False Rejection rate as the performance metric. The results achieved were 5% and 1%, respectively. The accuracy was also calculated, and the results showed an accuracy of 97%. In the second and third experiments, we evaluated the performance of the algorithm against the effect of human emotions and exercise, respectively. The three emotions that we focused on included stress, calmness, and excitement. Subjects authenticated against these emotions, and the algorithm results were recorded. We also made an investigation against the effect of exercising. We engaged subjects in a vigorous rope skipping exercise, and immediately after exercise, they were asked to authenticate. There was no significant change in the results obtained.

The accuracy of 97% shows good performance as compared to other related studies already discussed in Chapter 2. However, three aspects can be modified to improve overall accuracy. The first aspect is increasing training session. Results indicated that in the last three trials, most subjects recorded their highest scores. This indicates that more training help subjects to master their authentication pattern. The second aspect is the threshold. As training session duration is increased, the threshold can also be increased coherently, reducing FAR and FRR. The third aspect is the recording device. A device with more electrodes in the frontal lobe may increase blink detection accuracy, making it even easier for subjects to seamlessly formulate their authentication pattern. We conducted an experiment to evaluate the effect of emotions and exercise on our proposed approach. Results indicated that emotions and exercising have no significant effect on the performance of our proposed algorithm. The overall results of this study indicate that our proposed approach is ideal and practical with regards to biometric authentication for real-world use.

Although significant work has been done in this study, it is important to outline the limitations encountered throughout this study. One of the significant limitations was time constraints. The availability of subjects at the desired time was a limitation since subjects had other engagements elsewhere. This restricted us to limited time to conduct our experiments. Since our EEG recording device is not a common thing to the subjects, a considerable amount of time was dedicated to the description and familiarisation of the device to the subjects. The other limitation was the budget. Due to limited funds, we resorted to engaging subjects who willingly volunteered to be part of the study without being paid. This resulted in having subjects less committed to availing themselves at a time of need, therefore also limiting us in the number of subjects to participate in this study. The scope of our study was also a limitation in investigating the effect of emotions and exercising on the performance of the proposed approach. The emotions were limited to only excitement, calmness, and sadness, while the type of exercise was limited to robe skipping exercise. Other types of emotions, like anger as well as other types of prolonged exercises, could be further investigated.

6.2 Further Work

The use of more advanced, sophisticated EEG recording devices could be investigated. Such devices like Emotive Epoc+ have more frontal lobe electrodes, more processing power, advanced built-in filters, more processed data. All these features can have a considerable impact on the performance of the algorithm and the accuracy of results. A device used in this study was a limitation in terms of outputting fewer data features, which inherently limited our algorithm design, hence the need for further investigation of advanced recording devices.

As already discussed, it has been observed that subjects recorded the highest scores in their last trials. This indicated that the more trials, the higher the scores. We concluded that this was because the more subjects practised their pattern, the more they got better at it. Another factor could be that the more they used the recording device, the more they got familiar with how to use it. These two factors possess a common variable, which is the duration of the trial or training session. Therefore, we state that the duration of the trial or training session per subject be investigated further as these two aspects could have a significant impact on the performance or accuracy of the algorithm.

As already discussed, the scope of this study was limited to the robe skipping exercise within a short period of time (approximately 5 minutes). A number of studies indicated that regular exercise is related to improved concentration, mental focus, and performance. One of the key aspects of our pattern formation is concentration and focus during the experiment session. Since regular exercise affects these aspects, they may affect the performance and accuracy of the proposed algorithm. Further investigation can be conducted regarding regular exercise and other types of exercise.

The eye blink data used in this study is output by the TGAM module as calculated values, as discussed in section 3.4. Therefore, other EEG artefacts like epilepsy and seizure that may produce a peak similar to that of eye blinks in the EEG waveform were not investigated, even though they are likely to trigger false positive. Further investigation may be conducted to evaluate the effect of these artefacts in the performance of the proposed algorithm.

References

[1] S.-H. Liew, Y.-H. Choo, Y. F. Low, and Z. I. Mohd Yusoh, “EEG-based biometric authentication modelling using incremental fuzzy-rough nearest neighbour technique,” *IET Biometrics*, vol. 7, no. 2, pp. 145–152, 2018.

[2] P. Wang, Y. Yang, and J. Li, “Development of parkour game system using EEG control,” *Proc. - 2018 Int. Symp. Comput. Consum. Control. IS3C 2018*, pp. 258–261, 2019.

[3] K. Yao, S. Lan, C. Xu, R. Su, and X. Liu, “A wearable EEG-based control network and emergency medical assistance system,” *2017 Int. Symp. Antennas Propagation, ISAP 2017*, vol. 2017-Janua, pp. 1–2, 2017.

[4] C. C. Lo, T. Y. Chien, J. S. Pan, and B. S. Lin, “Novel Non-Contact Control System for Medical Healthcare of Disabled Patients,” *IEEE Access*, vol. 4, pp. 5687–5694, 2016.

[5] Ericsen, K. P. Thomas, and A. P. Vinod, “EEG-based biometric authentication using selfreferential visual stimuli,” *2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017*, vol. 2017-Janua, pp. 3048–3053, 2017.

[6] M. Bassi and P. Triverbi, “Human Biometric Identification through Brain Print,” in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2018, pp. 1514–1518.

[7] Y. Chen *et al.*, “A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 12, pp. 2635–2647, 2016.

[8] Z. A. A. Alyasseri, A. T. Khader, M. A. Al-Betar, J. P. Papa, and O. A. Alomari, “EEG-based Person Authentication Using Multi-objective Flower Pollination Algorithm,” *2018 IEEE Congr. Evol. Comput. CEC 2018 - Proc.*, 2018.

[9] I. Jayarathne, M. Cohen, and S. Amarakeerthi, “BrainID: Development of an EEG-based biometric authentication system,” *7th IEEE Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEEE IEMCON 2016*, 2016.

[10] A. V H, “A Review on Noises in EMG Signal and its Removal,” *Int. J. Sci. Res. Publ.*, vol. 7, no. 5, pp. 23–27, 2017.

[11] T. Gebrehiwot, R. Paprocki, M. Gradinscak, and A. Lenskiy, “Extracting Blink Rate Variability from EEG Signals,” *Int. J. Mach. Learn. Comput.*, vol. 6, no. 3, pp. 191–195, 2016.

[12] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, “State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals,” *IET Biometrics*, vol. 4, no. 3, pp. 179–190, 2015.

[13] H. L. Chan, P. C. Kuo, C. Y. Cheng, and Y. S. Chen, “Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition,” *Front. Neuroinform.*, vol. 12, no. October, pp. 1–15, 2018.

[14] Q. Gui, Z. Jin, and W. Xu, “Exploring EEG-based biometrics for user identification and authentication,” *2014 IEEE Signal Process. Med. Biol. Symp. IEEE SPMB 2014 - Proc.*, 2015.

[15] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, “I think, therefore I am: Usability and security of authentication using brainwaves,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7862 LNCS, pp. 1–16, 2013.

[16] D. La Rocca *et al.*, “Human brain distinctiveness based on EEG spectral coherence connectivity,” *IEEE Trans. Biomed. Eng.*, vol. 61, no. 9, pp. 2406–2412, 2014.

[17] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, “Low-cost electroencephalogram (EEG) based authentication,” *2011 5th Int. IEEE/EMBS Conf. Neural Eng. NER 2011*, pp. 442–445, 2011.

[18] R. Palaniappan, “Electroencephalogram Signals from Imagined Activities: A Novel Biometric Identifier for a Small Population,” pp. 604–611, 2006.

[19] M. V Ruiz-blondet, Z. Jin, and S. Laszlo, “CEREBRE : A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification,” vol. 6013, no. c, pp. 1–13, 2016.

[20] S. Marcel and J. del R. Millan, “Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.

29, no. 4, pp. 743–748, 2007.

[21] B. Hu, Q. Liu, Q. Zhao, Y. Qi, and H. Peng, “A real-time electroencephalogram (EEG) based individual identification interface for mobile security in ubiquitous environment,” *Proc. - 2011 IEEE Asia-Pacific Serv. Comput. Conf. APSCC 2011*, no. 60973138, pp. 436–441, 2011.

[22] S. Yang and F. Deravi, “On the Usability of Electroencephalographic Signals for Biometric Recognition: A Survey,” *IEEE Trans. Human-Machine Syst.*, vol. 47, no. 6, pp. 958–969, 2017.

[23] I. Jayarathne, M. Cohen, and S. Amarakeerthi, “Survey of EEG-based biometric authentication,” *2017 IEEE 8th Int. Conf. Aware. Sci. Technol.*, no. iCAST, pp. 324–329, 2017.

[24] N. Thammasan, K. Moriyama, K. ichi Fukui, and M. Numao, “Familiarity effects in EEG-based emotion recognition,” *Brain Informatics*, vol. 4, no. 1, pp. 39–50, 2017.

[25] L. Orgo, M. Bachmann, J. Lass, and H. Hinrikus, “Effect of negative and positive emotions on EEG spectral asymmetry,” *Eng. Med. Biol. Soc. (EMBC), 2015 37th Annu. Int. Conf. IEEE*, pp. 8107–8110, 2015.

[26] K. Choktanomsup, W. Charoenwat, and P. Sittiprapaporn, “Changes of EEG power spectrum in moderate running exercises,” *ECTI-CON 2017 - 2017 14th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, pp. 9–12, 2017.

[27] G. Chuang, J. Chuang, M. San, and J. High, “Passthoughts on the Go : Effect of Exercise on EEG Authentication,” p. 2013, 2013.

[28] A. Chiuzbaian, J. Jakobsen, and S. Puthusserypady, “Mind Controlled Drone: An Innovative Multiclass SSVEP based Brain Computer Interface,” *7th Int. Winter Conf. Brain-Computer Interface, BCI 2019*, pp. 1–5, 2019.

[29] K. Das, T. T. Leong, S. Suresh, and N. Sundararajan, “Meta-cognitive interval type-2 fuzzy controller for quadcopter flight control- An EEG based approach,” *2016 IEEE Int. Conf. Fuzzy Syst. FUZZ-IEEE 2016*, pp. 2501–2507, 2016.

[30] Y. An, T. Shi, L. Ren, W. Liu, and X. Jiang, “UAV control in 2D space based on brain

computer interface," *2017 4th Int. Conf. Syst. Informatics, ICSAI 2017*, vol. 2018-Janua, no. Icsai, pp. 594–598, 2017.

[31] M. Wang, S. Chen, W. Chai, and X. Qin, "EEG control method for fire extinguishing UAV based on improved subband filter bank," in *2019 IEEE International Conference on Unmanned Systems (ICUS)*, 2019, pp. 611–615.

[32] F. Enrique and S. Burgos, "Interactive Visualization of the Cranio-Cerebral," pp. 424–431, 2016.

[33] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A novel biometric approach for human identification and verification using eye blinking signal," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 876–880, 2015.

[34] "EMOTIV EPOC+ 14 Channel Mobile EEG - Emotiv." [Online]. Available: https://www.emotiv.com/product/emotiv-epoc-14-channel-mobile-eeg/#tab-description. [Accessed: 19-Jun-2019].

[35] "MindWave." [Online]. Available: https://store.neurosky.com/pages/mindwave. [Accessed: 19-Jun-2019].

[36] "EMOTIV Insight 5 Channel Mobile EEG - Emotiv." [Online]. Available: https://www.emotiv.com/product/emotiv-insight-5-channel-mobile-eeg/. [Accessed: 19-Jun-2019].

[37] "Muse^{TM} - Meditation Made Easy with the Muse Headband." [Online]. Available: https://choosemuse.com/. [Accessed: 18-Sep-2019].

[38] Y. Sun and X. B. Yu, "Capacitive Biopotential Measurement for Electrophysiological Signal Acquisition: A Review," *IEEE Sens. J.*, vol. 16, no. 9, pp. 2832–2853, 2016.

[39] A. J. Casson, "Wearable EEG and beyond," *Biomed. Eng. Lett.*, vol. 9, no. 1, pp. 53–71, 2019.

[40] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 7, pp. 1618–1629, 2016.

[41] P. Kumari and A. Vaish, "Brainwave based user identification system: A pilot study in

robotics environment," *Rob. Auton. Syst.*, vol. 65, pp. 15–23, 2015.

[42] P. Kumari Sharma and A. Vaish, "Individual identification based on neuro-signal using motor movement and imaginary cognitive process," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2143–2148, 2016.

[43] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new biometric modality for human authentication using eye blinking," *Proc. 7th Cairo Int. Biomed. Eng. Conf. CIBEC 2014*, no. d, pp. 174–177, 2015.

[44] E. Gupta, M. Agarwal, and R. Sivakumar, "Blink to Get In : Biometric Authentication for Mobile Devices using EEG Signals," 2020.

[45] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new multi-level approach to EEG based human authentication using eye blinking," *Pattern Recognit. Lett.*, vol. 82, pp. 216–225, 2016.

[46] A. Riera, S. Dunne, I. Cester, and G. Ruffini, "STARFAST: a Wireless Wearable EEG / ECG Biometric System based on the ENOBIO Sensor," *Proc. Int. Work. Wearable Micro Nanosyst. Pers. Heal.*, no. May 2014, pp. 3–6, 2008.

[47] S. K. Yeom, H. Il Suk, and S. W. Lee, "Person authentication from neural activity of face-specific visual self-representation," *Pattern Recognit.*, vol. 46, no. 4, pp. 1159–1169, 2013.

[48] S.-H. Liew, Y.-H. Choo, Y. F. Low, Y. Fen Low, Z. Izzah, and M. Yusoh, "Identifying Visual Evoked Potential (VEP) electrodes setting for person authentication Development Of An EEG Amplifier For Real-Time Acquisition View project Investigation on Parametric and Non-Parametric Features of Wheeze Signals for the Classification of Asthma Severity using Respiratory Acoustic Sounds and Machine Learning Algorithms View project Identifying Visual Evoked Potential (VEP) Electrodes Setting for Person Authentication," *Int. J. Adv. Soft Compu. Appl*, vol. 7, no. 3, 2015.

[49] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis," *EURASIP J. Adv. Signal Process.*, vol. 2008, 2008.

[50] R. Palaniappan and D. P. Mandic, “Biometrics from brain electrical activity: A machine learning approach,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 738–742, 2007.

[51] F. Al-Shargie, M. Kiguchi, N. Badruddin, S. C. Dass, A. F. M. Hani, and T. B. Tang, “Mental stress assessment using simultaneous measurement of EEG and fNIRS,” *Biomed. Opt. Express*, vol. 7, no. 10, p. 3882, 2016.

[52] T. Pham, W. Ma, D. Tran, T. D. Su, and D. Phung, “A Study on the Stability of EEG Signals for User Authentication,” *2015 7th Int. IEEE/EMBS Conf. Neural Eng.*, pp. 122–125, 2015.

[53] Y. Y. Lee and S. Hsieh, “Classifying different emotional states by means of eegbased functional connectivity patterns,” *PLoS One*, vol. 9, no. 4, 2014.

[54] P. Uengtrakul, S. Lookhanumanchao, and P. Sittiprapaporn, “Effect of Qigong exercise indexed by lightweight electroencephalography,” *ECTI-CON 2017 - 2017 14th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, pp. 17–20, 2017.

[55] Q. Wu, Y. Zeng, C. Zhang, L. Tong, and B. Yan, “An EEG-based person authentication system with open-set capability combining eye blinking signals,” *Sensors (Switzerland)*, vol. 18, no. 2, pp. 1–18, 2018.

[56] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, “A new multi-level approach to EEG based human authentication using eye blinking,” *Pattern Recognit. Lett.*, vol. 82, pp. 216–225, 2016.

[57] A. Patel and N. Patel, *Soft Computing and Signal Processing*, vol. 900, no. February. Springer Singapore, 2019.

[58] F. Gondesen, M. Marx, and D. Gollmann, *EEG-based biometrics*. 2018.

[59] “Mobile Mental Health & Mindfulness.” [Online]. Available: http://neurosky.com/2016/08/mobile-mental-health-mindfulness/. [Accessed: 14-Aug-2020].

[60] S. N. Abdulkader, A. Atia, and M.-S. M. Mostafa, “Authentication systems: principles and threats,” *Comput. Inf. Sci.*, vol. 8, no. 3, 2015.

[61] S. Sugrim, C. Liu, M. McLean, and J. Lindqvist, “Robust Performance Metrics for Authentication Systems,” no. February, 2019.

[62] “Mobile Mental Health & Mindfulness.” .

[63] J. Posner and J. A. Russell, “The circumplex model of affect : An integrative approach to affective neuroscience , cognitive development , and psychopathology,” pp. 715–734, 2017.

[64] H. Xu and K. N. K. Plataniotis, “Affect Recognition Using EEG Signal.”

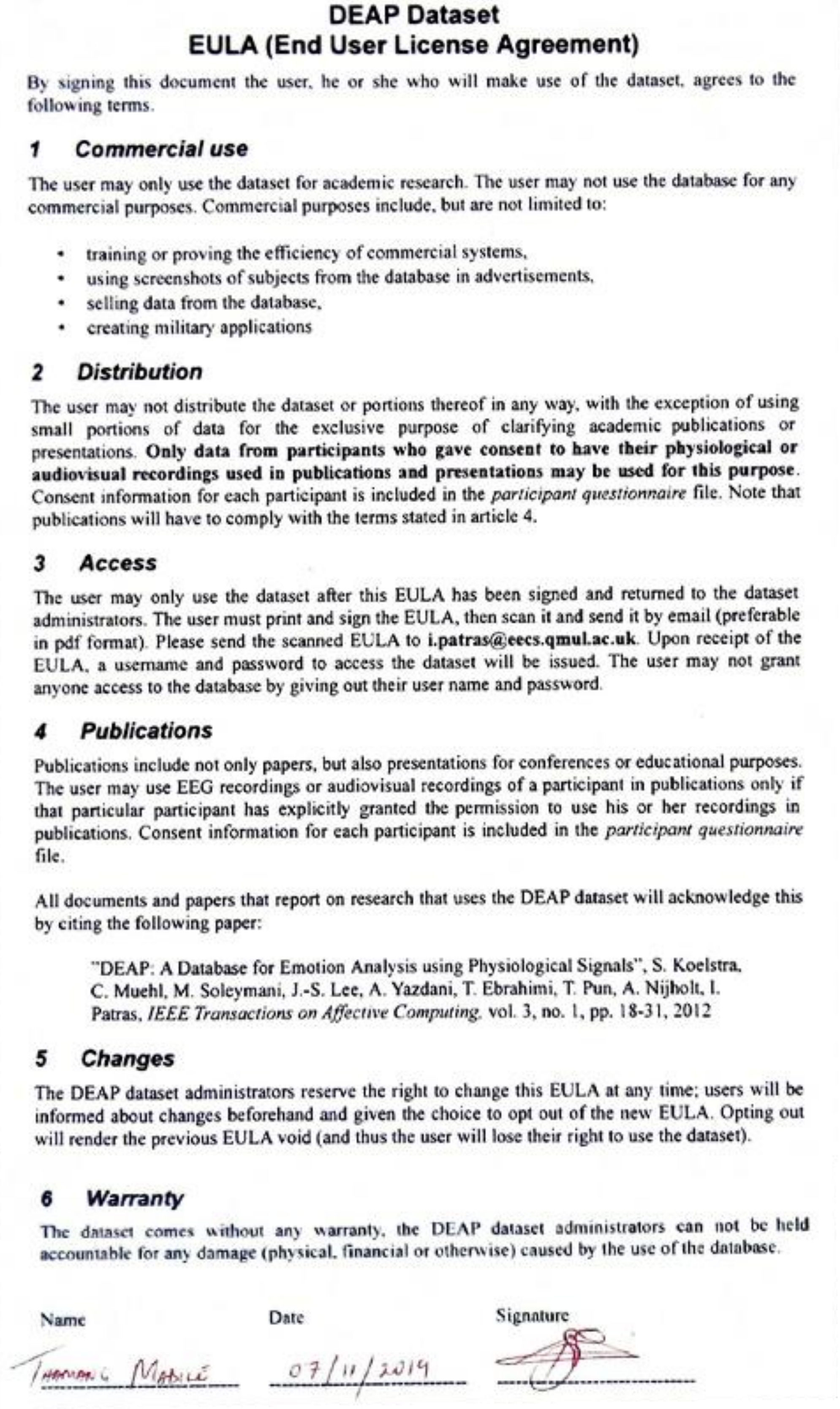
[65] T. F. Bastos-filho, “Evaluation of Feature Extraction Techniques in Emotional State Recognition,” 2012.

[66] S. A. Hosseini and M. A. Khalilzadeh, “Emotional Stress Recognition System Using EEG and Psychophysiological Signals: Using New Labelling Process of EEG Signals in Emotional Stress State,” no. November 2014, 2010.

[67] M. Soleymani, S. Member, and J. Lee, “DEAP : A Database for Emotion Analysis Using Physiological Signals,” vol. 3, no. 1, pp. 18–31, 2012.

[68] H. Tanaka, K. D. Monahan, and D. R. Seals, “Age-predicted maximal heart rate revisited,” *J. Am. Coll. Cardiol.*, vol. 37, no. 1, pp. 153–156, 2001.

Appendix A



DEAP Dataset
EULA (End User License Agreement)

By signing this document the user, he or she who will make use of the dataset, agrees to the following terms.

1 Commercial use

The user may only use the dataset for academic research. The user may not use the database for any commercial purposes. Commercial purposes include, but are not limited to:

- training or proving the efficiency of commercial systems,
- using screenshots of subjects from the database in advertisements,
- selling data from the database,
- creating military applications

2 Distribution

The user may not distribute the dataset or portions thereof in any way, with the exception of using small portions of data for the exclusive purpose of clarifying academic publications or presentations. **Only data from participants who gave consent to have their physiological or audiovisual recordings used in publications and presentations may be used for this purpose**. Consent information for each participant is included in the *participant questionnaire* file. Note that publications will have to comply with the terms stated in article 4.

3 Access

The user may only use the dataset after this EULA has been signed and returned to the dataset administrators. The user must print and sign the EULA, then scan it and send it by email (preferable in pdf format). Please send the scanned EULA to **i.patras@eecs.qmul.ac.uk**. Upon receipt of the EULA, a username and password to access the dataset will be issued. The user may not grant anyone access to the database by giving out their user name and password.

4 Publications

Publications include not only papers, but also presentations for conferences or educational purposes. The user may use EEG recordings or audiovisual recordings of a participant in publications only if that particular participant has explicitly granted the permission to use his or her recordings in publications. Consent information for each participant is included in the *participant questionnaire* file.

All documents and papers that report on research that uses the DEAP dataset will acknowledge this by citing the following paper:

> "DEAP: A Database for Emotion Analysis using Physiological Signals", S. Koelstra, C. Muehl, M. Soleymani, J.-S. Lee, A. Yazdani, T. Ebrahimi, T. Pun, A. Nijholt, I. Patras, *IEEE Transactions on Affective Computing*, vol. 3, no. 1, pp. 18-31, 2012

5 Changes

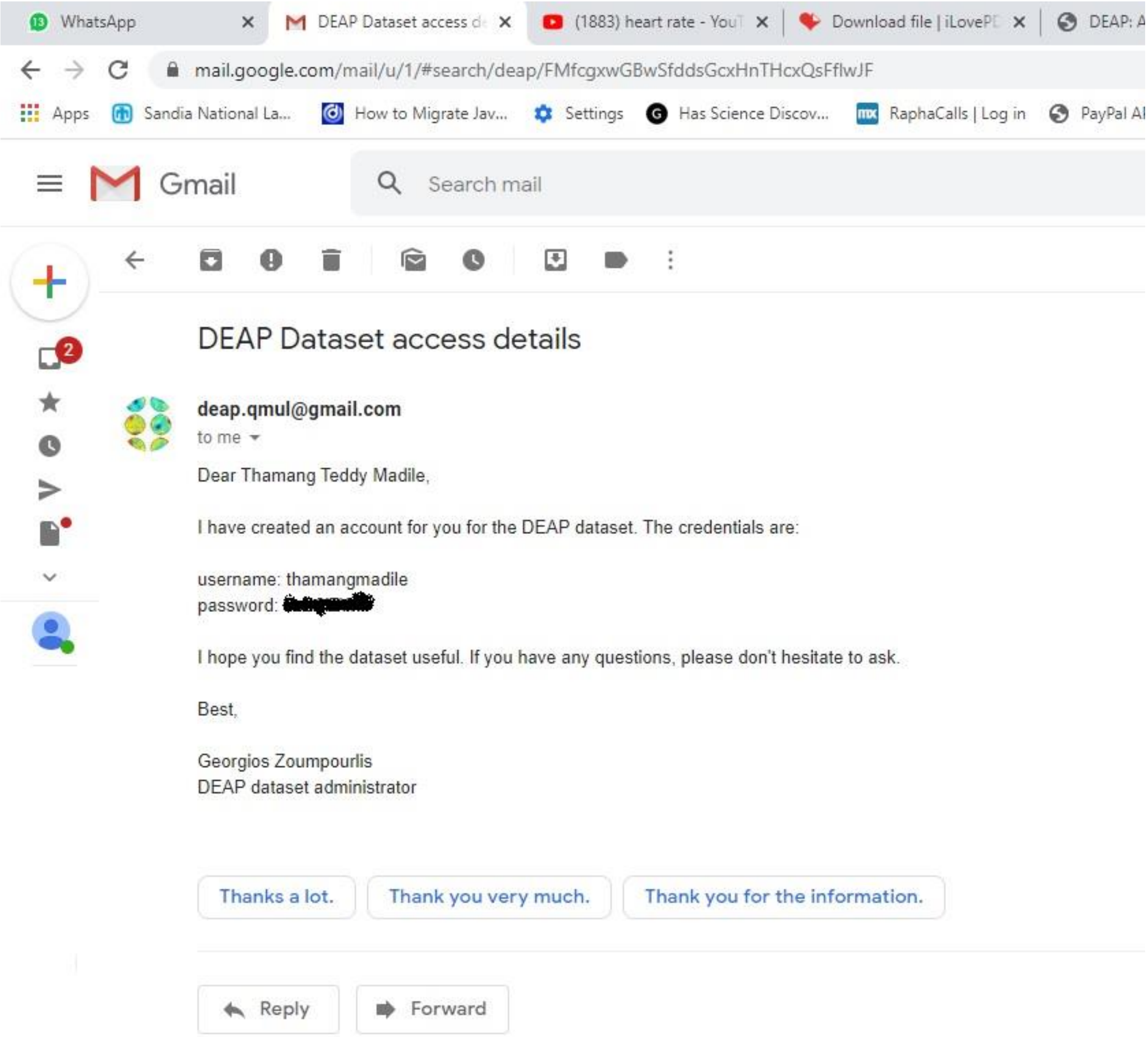
The DEAP dataset administrators reserve the right to change this EULA at any time; users will be informed about changes beforehand and given the choice to opt out of the new EULA. Opting out will render the previous EULA void (and thus the user will lose their right to use the dataset).

6 Warranty

The dataset comes without any warranty, the DEAP dataset administrators can not be held accountable for any damage (physical, financial or otherwise) caused by the use of the database.

Name	Date	Signature
THAMAN C MABILÉ	07/11/2019	

Figure 34. DEAP dataset application form.



DEAP Dataset access details

deap.qmul@gmail.com
to me

Dear Thamang Teddy Madile,

I have created an account for you for the DEAP dataset. The credentials are:

username: thamangmadile
password: [redacted]

I hope you find the dataset useful. If you have any questions, please don't hesitate to ask.

Best,

Georgios Zoumpourlis
DEAP dataset administrator

Figure 35. DEAP dataset request approval.

Appendix B

BIUST
BOTSWANA INTERNATIONAL UNIVERSITY
OF SCIENCE & TECHNOLOGY

Consent for Participation in a Research Experiment

I volunteer to participate in a research project conducted by Thamang Teddy Madile [supervisee] and Dr. Hlomani Hlomani [supervisor] from **Botswana International University of Science & Technology**. I understand that the project is about brainwave authentication and that my brainwave data is needed for this project. I commit myself to be used for this purpose in this research.

1. My participation in this project is voluntary. I understand that I will not be paid for my participation. I may withdraw and discontinue participation at any time without penalty. If I decline to participate or withdraw from the study, no one on my campus will be told.

2. I understand that participant may find the experiment interesting and thought-provoking. If, however, I feel uncomfortable in any way during the experiment, I have the right to decline or withdraw from the experiment.

3. Participation involves being interviewed, my brainwave data measured using Neurosky Mindwave Mobile 2 device and formulating blink patterns according to the instructions of the researchers of this project. The experiment may last several days depending on the level of satisfactory of the project coordinators, and I may discontinue or withdraw if I want to, for whatever reason.

4. I understand that the researcher will not identify me by name in any reports using information obtained from this interview, and that my confidentiality as a participant in this study will remain secure. Subsequent uses of records and data will be subject to standard data use policies which protect the anonymity of individuals and institutions.

5. Faculty and administrators from my campus will neither be present at the interview nor have access to raw notes or transcripts. This precaution will prevent my individual comments from having any negative repercussions.

6. I have read and understand the explanation provided to me. I have had all my questions answered to my satisfaction, and I voluntarily agree to participate in this study.

7. I have been given a copy of this consent form.

Full Name ____________________________

Signature ____________________________

Date ____________________________

Coordinator Name ____________________________

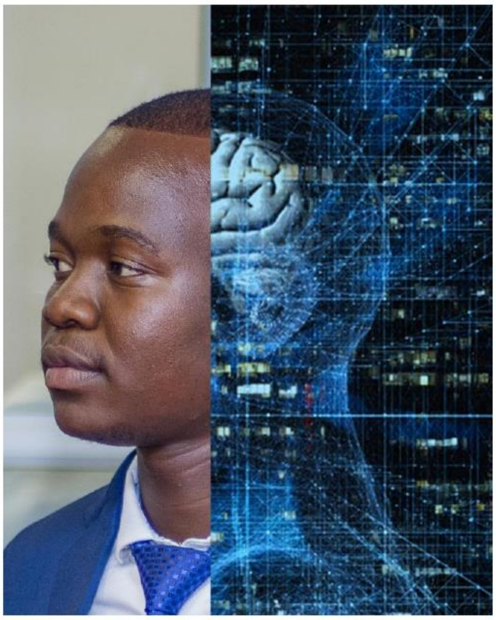
Coordinator Signature ____________________________

Date ____________________________

Appendix C

BIUST

BOTSWANA INTERNATIONAL UNIVERSITY
OF SCIENCE & TECHNOLOGY



Experiment Guide

Instruction Manual

ABSTRACT

This document entails some guidelines and instructions for participants engaged in the EEG Biometric Authentication experiment. All participants are expected to go through this guide prior to the day of the experiment. For questions related to this matter please contact the coordinator.

Thamang Madile
thamang.madile@studentmail.biust.ac.bw

Contents

Introduction 2

Preliminary actions 2

Arrival of a participant at the experiment room 2

Experiment Setup 2

Demonstration of pattern formation 3

Using the system 4

- **Registering Subjects** 4
- **Enrolling and Authentication** 5

Introduction

This document entails guidelines and instructions for the participants of EEG biometric authentication experiment. It entails the preliminary section which states the actions that subjects are to carry out prior to the experiment. The second section states procedures subjects should expect upon arrival. The experiment setup section gives subjects the overall picture of how the experiment is arranged and the tools to be used. The next section gives subjects an idea of how the authentication pattern is generated. The last section entails instruction on how to use the system.

Preliminary actions

Preliminary actions are a set of tasks that participants are expected to undertake prior to the experiment session. Participants are excepted to be in a good normal state both mentally and physically. You are expected to have enough resting/sleeping time (a minimum of 6 hours) the night before the experiment. Do not engage in a labour intensive physically or mentally.

Arrival of a participant at the experiment room

Upon your arrival, you will be expected to sign the consent form. You will be given time to seek any clarification concerning the experiment. You will also be requested to fill in the registration form. Any electrical or electronic device like cell phones should remain switched off thought the experiment session. You will be expected to remove hats or caps if you are putting on one.

Experiment Setup

The setup involves a laptop placed on top of the office desk with a comfortable office chair. There is also an EEG device called NeuroSky Mindwave Mobile 2 headset shown in figure 1 below. This headset is used to measure brain activity from the scalp. The subject is expected to wear the headset, the front electrode attached to the forehead slightly to the left and above the left eye and the reference electrode which is the ear clip is attached to the earlobe as depicted in figure 2 below. There is a coordinator to guide and instruct you throughout the experiment session. The coordinator is also there to record notes. Before installing the EEG headset on the subject, the area where electrodes come in contact with the subject’s skin is cleaned with alcohol and cotton wool to remove dirt, oil and dead skin cells. You will be registered into the system. Your basic information like name, surname, email and profile image will be input by the subject into the system.

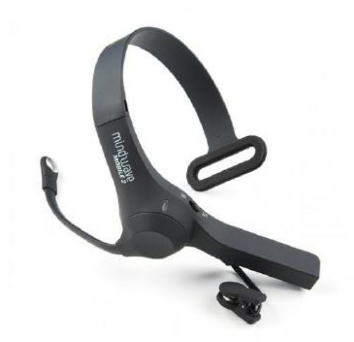


Figure 1. NeuroSky Mindwave Mobile 2

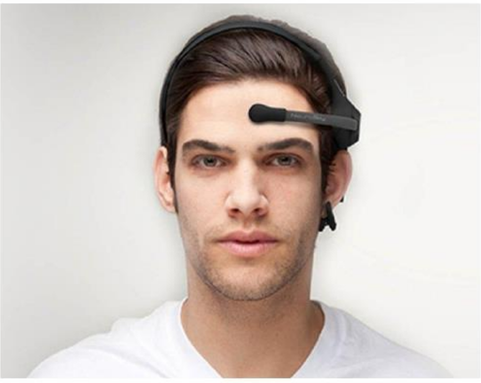


Figure 2. Demonstration of how to wear the headset

Demonstration of pattern formation

We demonstrate to the subjects how the authentication pattern is formed using figure 3 below. The coordinator will clarify further if you have trouble in understanding this task.

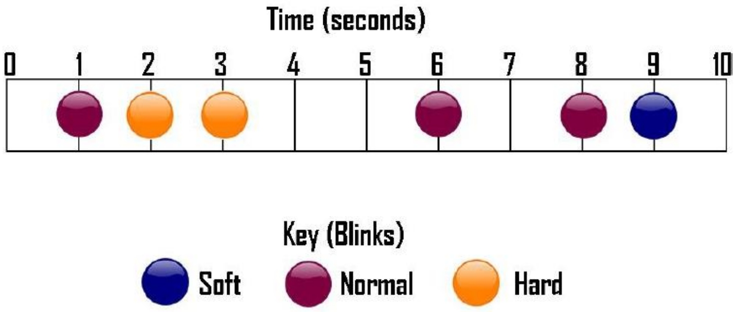


Figure 3. A diagram to demonstrate pattern formation

Figure 3 above shows a demonstration of pattern formation. The numbers 1 to 10 indicates the duration of the session in seconds. The coloured dots symbolise a blink that occurred at a given time. The colours of the dots depict the type of strength a blink has. A blue dot indicates a soft blink. A maroon dot indicates a normal blink. An orange dot indicates a hard blink. The figure indicates that there was a normal blink a second from the start of the session followed by two hard blinks on the second and third second. Another normal blink occurred at the 6th and 8th second followed by a soft blink at the 9th second.

Using the system

Registering Subjects

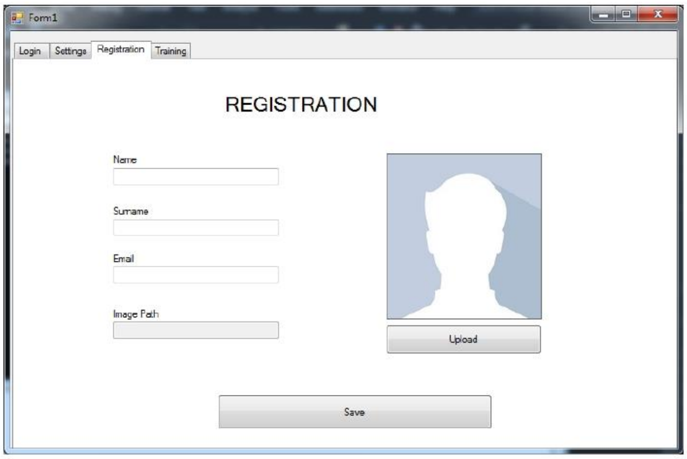
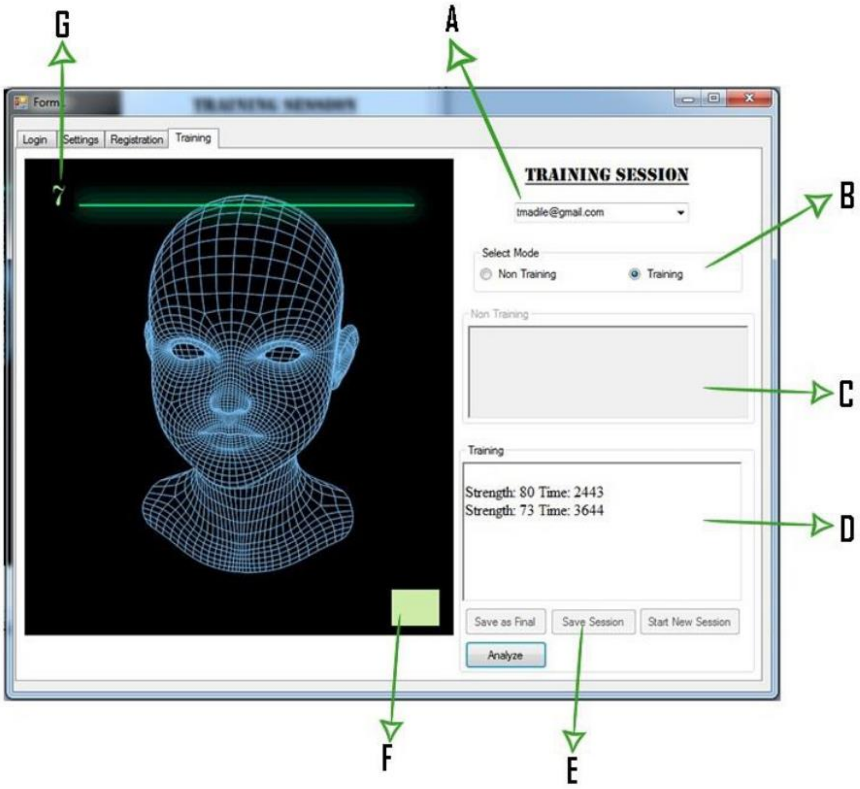


Figure 4. A form to capture basic details

Figure 4 above depicts the systems registration form. All field are required, only the image upload is optional. Click the save button when you have filled the required fields.

Enrolling and Authentication



tmadile@gmail.com

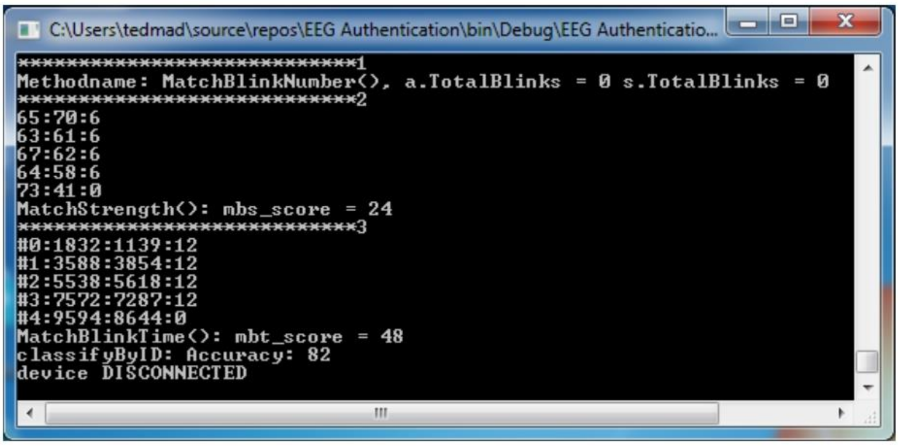
```
Strength: 80 Time: 2443
Strength: 73 Time: 3644
```

Figure 5. Layout of the system

The first thing to do after registering on the system is to select your email. "Part A" shows where to make that selection. Select the training mode to train or practice your authentication pattern. This section is also meant to make you familiarize yourself with the system. "Part B" shows where to make that selection. A subject can perform as many trials as he/she desires to get a feel of how the application and the device respond to his/her actions. The data output by the system during training mode is displayed in an area depicted by "Part D". "Part F" changes color with every successfully detected blink, in order to help you easily track which blinks were detected and which ones were not.

When you are confident with your pattern, proceed to the next stage, which is the enrolment stage. This is the stage where you set or create your password. To start the enrolment stage, select the “non-training” mode. By making that selection you will notice that the system outputs your data in part C. To begin, click the “start new session” button. The system will give you 10 seconds to create your pattern using eye blinks. The duration is indicated by a countdown timer shown by “Part G”. If you are satisfied with the pattern click “save session” button. This will save your data to the database

To login to the system, click the start session button, and repeat your password. When the countdown timer times out, click save as final button. This button saves your login data into memory. Then click the analyse button. This will trigger the system to invoke the algorithm to compute and validate your login data. Your results will be printed on a console window as indicated by figure 6 below.


C:\Users\tedmad\source\repos\EEG Authentication\bin\Debug\EEG Authenticatio...

```
*****************************1
Methodname: MatchBlinkNumber(), a.TotalBlinks = 0 s.TotalBlinks = 0
*****************************2
65:70:6
63:61:6
67:62:6
64:58:6
73:41:0
MatchStrength(): mbs_score = 24
*****************************3
#0:1832:1139:12
#1:3588:3854:12
#2:5538:5618:12
#3:7572:7287:12
#4:9594:8644:0
MatchBlinkTime(): mbt_score = 48
classifyByID: Accuracy: 82
device DISCONNECTED
```

Figure 6. Authentication results

Appendix D

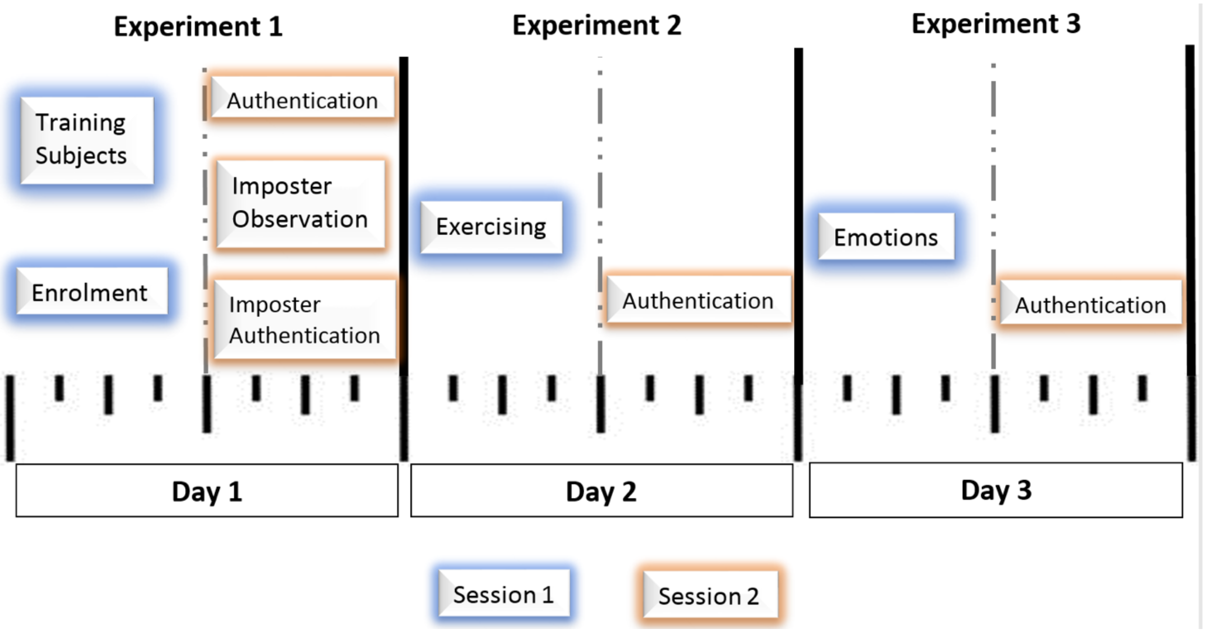


Figure 36. Experiment session timeline