EEG-BASED PERSON IDENTIFICATION USING MULTI-LEVEL WAVELET DECOMPOSITION WITH MULTI-OBJECTIVE FLOWER POLLINATION ALGORITHM

ZAID ABDI ALKAREEM YAHYA ALYASSERI

UNIVERSITI SAINS MALAYSIA

2020

EEG-BASED PERSON IDENTIFICATION USING MULTI-LEVEL WAVELET DECOMPOSITION WITH MULTI-OBJECTIVE FLOWER POLLINATION ALGORITHM

by

ZAID ABDI ALKAREEM YAHYA ALYASSERI

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

June 2020

ACKNOWLEDGEMENT

I am very grateful and thankful to Allah S.W.T for giving me strength to complete my research study. Although I am solely responsible for the study and its findings, I must acknowledge many external contributions coming from people who extended a helping hand throughout this research. I would also like to acknowledge here the unflagging efforts of my supervisor, Prof. Dr. Ahamad Tajudin Khader and co-supervisor, Assoc. Prof. Dr.Mohammed Azmi Al-Betar from the School of Computer Science at Universiti Sains Malaysia (USM) and Department of Information Technology, Al-Huson University College, Al-Balqa Applied University, Jordan, respectively in all aspects- from supervision, counselling, advice, to encouragement throughout my research; without whom the road of research would not have been sailing smoothly. I would also like to thank The World Academic Science (TWAS) and the Uni-versity Science Malaysia (USM) for supporting my Ph.D. study. My thanks go to my beloved parents for their love, patience, encouragement, and continuous support. Words alone cannot express the thanks I owe to my beloved wife Bashaer Musawi for supporting me during this tiring research task while at the same time taking care of our children Zahraa and Mohammed Baqer. Last but not least, I thank those who supported me in any respect during my re-search, especially my friends Dr. Osama Alomari, Ammar Kamal Abasi, Sharif Naser Makhadmeh, and many others that whose names I can not recall.

TABLE OF CONTENTS

ACKNOWLEDGEMENT ii

TABLE OF CONTENTS iii

LIST OF TABLES xi

LIST OF FIGURES xv

LIST OF ABBREVIATIONS xix

LIST OF APPENDICES xxii

ABSTRAK xxiii

ABSTRACT xxv

CHAPTER 1 INTRODUCTION

1.1 Background 1

1.1.1 Biometric User Identification 1

1.1.2 EEG Signals 2

1.2 Motivation and Problem Statement 3

1.3 Research Objectives 7

1.4 Research Contributions 8

1.5 Research Scope 8

1.6 Overview of Methodology 9

1.7 Overview of Thesis 10

CHAPTER 2 EEG-BASED BIOMETRIC IDENTIFIER: LITERATURE REVIEW

2.1 Introduction 12

2.2 Biometric System 12

2.2.1 Essential Criterion in a Biometric System 13
2.2.2 Modes of process in biometric systems 14
2.3 Biometric modalities 15
2.3.1 Behavioral modalities 17
2.3.2 Soft modalities 17
2.3.3 Hand Region modalities 18
2.3.4 Facial Region modalities 19
2.3.5 Ocular Region modalities 20
2.3.6 Medico-chemical modalities 20
2.3.7 Previous Biometric Security Vulnerabilities 21
2.4 EEG-based biometric system components 23
2.4.1 EEG Signals Acquisition 24
2.4.2 EEG Pre-Processing 24
2.4.3 EEG Feature Extraction 24
2.4.4 EEG dimensionality reduction 26
2.4.5 Classification 27
2.5 EEG-based person identification related works 27
2.6 Metaheuristics for EEG-based identification 39
2.7 Comparative analysis of biometric identification 40
2.8 Summary 43

CHAPTER 3 METHODOLOGY

3.1 Introduction 45
3.2 Schema of the Methodology 46
3.2.1 Phase I: EEG Signal Acquisition 48

3.2.2 Phase II: Preprocessing 48

3.2.3 Phase III: Features Extraction 49

3.2.4 EEG channel selection 49

3.2.5 Phase IV: Classification 50

3.3 EEG Standard Datasets 50

3.3.1 Keirn's EEG Dataset 51

3.3.2 EEG Motor Movement/Imagery Dataset 52

3.4 Evaluation Measures 54

3.4.1 EEG Signal Denoising Evaluation 54

3.4.2 Identification Measures 55

3.5 Summary 56

CHAPTER 4 EEG SIGNALS DENOISING USING OPTIMAL WAVELET TRANSFORM HYBRIDISED WITH METAHEURISTIC

4.1 Introduction 57

4.2 Wavelet Transform 58

4.2.1 Wavelet denoising principle for non-stationary signals 58

4.3 Adaption meta-heuristic algorithms and wavelet transform for EEG signal denoising: Proposed method 64

4.4 Results and Discussions 71

4.4.1 A Comparative Analysis of the Proposed Metaheuristic Methods . 72

4.4.2 Comparing the Proposed Method with State-of-Art Methods 79

4.5 Summary 84

CHAPTER 5 MULTIOBJECTIVE FLOWER POLLINATION ALGORITHM: A NOVEL TECHNIQUE FOR EEG SIGNAL DENOISING

5.1 Introduction 86

5.2 Multi-objective optimization 87

5.3 Proposed MOFPA with wavelet transform (WT) for denoising EEG signals 90

5.4 Illustrative example 96

5.5 Results and discussions 98

5.5.1 Sensitivity analysis of MOFPA-WT to its p and population size PoP parameters 99

5.5.2 Parameter Settings Used for MOFPA-WT 100

5.5.3 Evaluation of MOFPA-WT 101

5.5.3(a) Effect of multiobjective function in MOFPA-WT 101

5.5.3(b) Convergence evaluation 104

5.5.3(c) Pareto front evaluation 104

5.5.3(d) Comparative evaluation MOFPA-WT with other Multi-Objective techniques 107

5.5.3(e) Comparing the MOFPA-WT with State-of-Art Methods 110

5.6 Summary 112

CHAPTER 6 A NOVEL EEG FEATURE EXTRACTION METHOD USING A MULTI-OBJECTIVE FLOWER POLLINATION ALGORITHM AND MULTILEVEL WAVELET DECOMPOSITION

6.1 Introduction 114

6.2 Proposed method: EEG Feature Extraction using MOFPA-WT 115

6.2.1 EEG Feature Extraction 116

6.2.1(a) EEG Feature Extraction based on 5 decomposition level 117

6.2.1(b) EEG Feature Extraction based on 10 decomposition level 119

6.2.2 EEG Classification 120

6.3 Results and Discussions 120

6.3.1 Experiments and Parameters Settings 121

6.3.2 Results of feature extraction using MOFPA-WT based on 5 decomposition level 122

6.3.3 Results of feature extraction using MOFPA-WT based on 10 decomposition level 124

6.3.4 Results of accuracy rate using MOFPA-WT based on 5 and 10 decomposition level using 10 fold cross-validation 128

6.3.5 MOFPA-WT Results using 10fold cross-validation approach 130

6.3.6 Comparing with State-Of-Art Results 133

6.4 Summary 135

CHAPTER 7 EEG CHANNEL SELECTION USING HYBRIDISING FPAB-HC METHOD FOR PERSON IDENTIFICATION

7.1 Introduction 136

7.2 EEG channel selection problem 137

7.2.1 Features for EEG channel selection 137

7.2.2 Modelling of EEG Channel Selection features 141

7.2.3 Objective Function 144

7.3 Methodology 146

7.3.1 Phase IV: EEG Channel selection using hybridizing FPAβ-hc with (RBF-SVM) classifier 148

7.4 Illustrative example 152

7.5 Results and Discussions 154

7.5.1 Experimental setup 155

7.5.2 Comparing performance of standard FPA and hybridizing FPAβ-hc for EEG channels selection 156

7.5.3 Comparison with state-of-arts 162

7.5.4 Discussion 165

7.6 Summary 168

CHAPTER 8 CONCLUSIONS AND FUTURE WORK

8.1 Introduction 170

8.2 Summary of Contributions 170

8.3 Conclusions 173

8.4 Future Research 174

REFERENCES 176

APPENDICES

LIST OF PUBLICATIONS

LIST OF TABLES

Page

Table 2.1 Description of attack vectors 21

Table 2.2 Comparatives table for EEG-based person identification technique. 42

Table 3.1 Standard EEG databases properties 50

Table 4.1 The ranges of the wavelet denoising parameters 63

Table 4.2 Thresholding selection rules 63

Table 4.3 The wavelet thresholding rescaling methods 63

Table 4.4 Meta-heuristic algorithms parameters 72

Table 4.5 The optimal wavelet denoising parameters obtained by selected meta-heuristic Algorithms for PLN, EMG, and WGN noise for (Keirn & Aunon, 1990) EEG dataset 73

Table 4.6 The optimal wavelet denoising parameters obtained by selected meta-heuristic Algorithms for PLN, EMG, and WGN noise for Motor_Imaging EEG dataset 74

Table 4.7 Performance of denoising the EEG signals for 5 meta-heuristic Algorithms for PLN, EMG, and WGN for Kiern's Dataset 75

Table 4.8 Performance of denoising the EEG signals for WT-based meta-heuristic Algorithms according to PLN, EMG, and WGN for EEG Motor Imaging Dataset 77

Table 4.9 Wavelet Parameters Range for Al-Qazzaz and Kumari methods 79

Table 4.10 Comparing the proposed FPA-WT method with state-of-art methods for EEG signals denoising with different noises 81

Table 5.1 Some recorded iterations using MOFPA to achieve optimal WT parameters 97

Table 5.2	Sensitivity analysis of MOFPA-WT to its p and population size PoP parameters for PLN noises for motor imaging EEG dataset	100
Table 5.3	Parameters setting for MOFPA-WT	101
Table 5.4	Optimal WT parameters obtained by FPA-SNR-WT, MOFPA-WT, FPA-MSE-WT for PLN, EMG, and WGN noises for motor imaging EEG dataset	103
Table 5.5	Performance of MOFPA in denoising EEG signals according to PLN, EMG, and WGN for EEG motor imaging dataset	103
Table 5.6	Wilcoxon signed-rank test evaluation	103
Table 5.7	Comparative evaluation MOFPA-WT with NSGA-II (MOGA-WT) and MOPSO (MOPSO-WT).	109
Table 5.8	T-test evaluation.	110
Table 5.9	Comparing the proposed method (MOFPA-WT) with state-of-the-art methods for EEG signals denoising with different noises	111
Table 6.1	EEG rhythms characteristics using 5 decomposition levels.	119
Table 6.2	EEG rhythms characteristics using 10 decomposition levels.	120
Table 6.3	Total number of EEG features using 5 and 10 WT decomposition levels.	122
Table 6.4	Confusion matrix concerning the experiment of task 1 based on 5 decomposition levels.	123
Table 6.5	Confusion matrix concerning the experiment of task 1 based on 5 decomposition levels.	123
Table 6.6	Confusion matrix concerning the experiment of task 2 based on 5 decomposition levels.	123
Table 6.7	Confusion matrix concerning the experiment of task 2 based on 5 decomposition levels.	124
Table 6.8	Confusion matrix concerning the experiment of task 1 based on 10 decomposition levels.	125

Table 6.9 Confusion matrix concerning the experiment of task 1 based on 10 decomposition levels. 125

Table 6.10 Confusion matrix concerning the experiment of task 2 based on 10 decomposition levels. 126

Table 6.11 Confusion matrix concerning the experiment of task 2 based on 10 decomposition levels. 126

Table 6.12 Wilcoxon signed-rank test evaluation of MOFPA-WT 5 and 10 levels. 129

Table 6.13 Confusion matrix concerning the baseline task 5 level 130

Table 6.14 Confusion matrix concerning the baseline task 10 level 130

Table 6.15 Confusion matrix concerning the multiplication task. 130

Table 6.16 Confusion matrix concerning the multiplication task 2 with 10 level. 131

Table 6.17 Confusion matrix concerning the letter composing task 5 level. 131

Table 6.18 Confusion matrix concerning the letter composing task 10 level. 131

Table 6.19 Confusion matrix concerning the counting task 5 level. 131

Table 6.20 Confusion matrix concerning the counting task 10 level. 132

Table 6.21 Confusion matrix concerning the rotation task 5 level. 132

Table 6.22 Confusion matrix concerning the rotation task 10 level. 132

Table 7.1 parameters setting 155

Table 7.2 Comparing performance of standard FPA and FPAβ-hc with SVM-RBF classifier 161

Table 7.3 Wilcoxon signed-rank test evaluation. of standard FPA and FPAβ-hc 164

Table 7.4 Comparison of the performance the proposed method (FPAβ-hc) with state-of-arts using autoregressive with three different coefficients. 165

Table A.1 functionality of some electrodes 198

Table A.2 EEG Rhythms Characteristics 199

Table A.3 Comparative of EEG Artifacts 201

Table C.1 The optimization terms in the flower context 222

Table C.2 FPA applications 1 244

LIST OF FIGURES

Page

Figure 1.1 EEG signal recording 3

Figure 1.2 Proposed system diagram 11

Figure 2.1 Composition of biometric system 13

Figure 2.2 Biometric User Authentication Modalities Taxonomy 16

Figure 2.3 Behavioral modalities: (a) voice signal, (b) typing rhythm, (c) gait, (d) signature 18

Figure 2.4 hand modalities: (a) fingerprint, (b) palmprint, (c) hand geometry,(d)hand vein pattern, and (e) finger knuckle print 18

Figure 2.5 Facial modalities: (a,b) face, (c) ear shape,(d) tongue print 19

Figure 2.6 Ocular modalities: (a) iris, (b) retina, (c) sclera and vasculature 20

Figure 2.7 Ratha's framework of Various Attacks Vector 21

Figure 2.8 Indirect biometric spoofing examples are taken from (Marcel, Nixon, & Li, 2014) 23

Figure 2.9 EEG-based Authentication System Components. 24

Figure 3.1 Overview of research methodology 47

Figure 3.2 Electrodes locations of 6 EEG channels recording according to (Keirn & Aunon, 1990) 52

Figure 3.3 Electrodes locations for 64 EEG channels recording according to (Goldberger et al., 2000 (June 13)) 53

Figure 3.4 Identification error types. 55

Figure 4.1 EEG Denoising Process 61

Figure 4.2 Soft and hard thresholding methods 62

Figure 4.3 Flowchart of the Proposed Method for EEG Signal Denoising 65

Figure 4.4 Original EEG signal corrupted using PLN, EMG, and WGN 66

Figure 4.5 Solution of WT parameters for denoising EEG signals using meta-heuristic algorithms. 67

Figure 4.6 EEG denoising procedure 71

Figure 4.7 Performance of meta-heuristic algorithms for EEG signal denosing 75

Figure 4.8 EEG signal denoising using meta-heuristic algorithms for EMG noise. 76

Figure 4.9 EEG signal denoising using meta-heuristic algorithms for PLN noise. 76

Figure 4.10 EEG signal denoising using meta-heuristic algorithms for WGM noise. 76

Figure 4.11 EEG signal denoising using meta-heuristic algorithms 78

Figure 4.12 EEG signal denoising using meta-heuristic algorithms for PLN noise. 78

Figure 4.13 EEG signal denoising using meta-heuristic algorithms for EMG noise. 78

Figure 4.14 EEG signal denoising using meta-heuristic algorithms for WGN noise. 79

Figure 4.15 Comparative analysis between FPA-WT, Sym9 and db4 82

Figure 5.1 Flowchart of proposed method (MOFPA-WT). 91

Figure 5.2 Mechanism of MOFPA for selecting the optimal WT parameters for denoising EEG signals 94

Figure 5.3 Sol'_{opt} WT parameters for EEG denoising 98

Figure 5.4 EEG denoising process 99

Figure 5.5 EEG Decomposition process for five levels 99

Figure 5.6 Thresholding and Reconstruction steps 100

Figure 5.7 Comparison results of FPA-SNR, MOFPA-WT, and FPA-MSE for EMG, PLN, and WGN noises 104

Figure 5.8 Convergence results of PLN 105

Figure 5.9 Convergence results of EMG 105

Figure 5.10 Convergence results of WGN 106

Figure 5.11 Comparison results of Pareto front and MOFPA-WT for 106
PLN noises

Figure 5.12 Comparison results of Pareto front and MOFPA-WT for 107
EMG noises

Figure 5.13 Comparison results of Pareto front and MOFPA-WT for 108
WGN noises

Figure 5.14 Comparison results of MOFPA-WT with other Multi- 109
Objective techniques using PLN noises.

Figure 6.1 Flowchart of applied MOFPA-WT EEG-based person iden- 116
tification.

Figure 6.2 EEG feature extraction based WT decomposition with 5 and 118
10 levels.

Figure 6.3 Multi-layer back propagation ANN. 121

Figure 6.4 Comparison results of MOFPA-WT for 5 and 10 decompo- 127
sition levels.

Figure 6.5 10-fold Cross-validation approach. 128

Figure 6.6 Accuracy results for task 1 and task 2 using a 10-fold Cross- 129
validation.

Figure 6.7 Comparison of the accuracy results using Kiern's dataset. 133

Figure 6.8 Comparison of the accuracy results for task 1 and task 2 with 134
(Sharma & Vaish, 2016)

Figure 7.1 EEG dataset representation. 142

Figure 7.2 Solution representation of EEG channel selection. 145

Figure 7.3 Hybridizing Flower pollination algorithm with β-hill climb- 147
ing flowchart

Figure 7.4 Solution representation using the proposed method (FPAβ- 154
hc).

Figure 7.5 Convergence rate of hybridizing FPAβ-hc compared with that of standard FPA. 157

Figure 7.6 Distribution of FPA and FPAβ-hc. 158

Figure 7.7 Distribution of FPA and FPAβ-hc. 159

Figure 7.8 Performance results of FPA and FPAβ-hc using accuracy rate and number of channels selected. 163

Figure 7.9 Performance results of FPA and FPAβ-hc using sensitivity and specificity measures. 163

Figure 7.10 Performance results of FPA and FPAβ-hc using the F1-score measure. 164

Figure 7.11 Comparison of the accuracy rate and number of EEG channels selected using AR features. 166

Figure A.1 The anatomy of the human brain 194

Figure A.2 EEG recording components 196

Figure A.3 19 Electrodes placed based on 10-20 international system 197

Figure A.4 Single EEG raw taken from one electrode with its rhythms 198

Figure C.1 Distribution of published research articles on FPA 218

Figure C.2 Number of publications of FP algorithm per databases 219

Figure C.3 Number of publications of FP algorithm per year 219

Figure C.4 Flower Pollinators taken from (BEEImage, 2014; ParkSeed, 2017) 220

Figure C.5 Cross and Self Pollination CDA (2012) 221

Figure C.6 Flower Pollination Algorithm flowchart 225

Figure C.7 FPA applications 245

LIST OF ABBREVIATIONS

Acc Accuracy

AR Autoregressive

ANN Artificial Neural Networks

BCI Brain Computer Interface

BCSS Binary Charged System Search

BFFA Binary Firefly Algorithm

BFPA Binary Flower Pollination Algorithm

BGA Binary Genetic Algorithm

BHS Binary Harmony Search

BPSO Binary Particle Swarm Optimization

CCR Cross-Correlation

CSP Common Spatial Patterns

CWT Continuous Wavelet Transform

DWT Discrete Wavelet Transform

ECG Electrocardiogram

EEG Electroencephalogram

EER Equal Error Rate

EMG Electromyography

FAR False Accept Rate

FDF Frequency Domain Features

FPA Flower Pollination Algorithm

FMR False Match Rate

FNMR False Non-Match Rate

FRR False Reject Rate

GA Genetic Algorithm

HC Hill Climbing

HSA Harmony Search Algorithm

ICA Independent Components Analysis

ITR Information Transfer Rate

LDA Linear Discriminant Analysis

LVQ Learning Vector Quantization

No. Ch Number of channels selected

PCA Principle Components Analysis

PIN Personal Identification Number

PLN Power Line Noise

PSO Particle Swarm Optimization

REC Rest Eyes Closed

REO Rest Eyes Open

Sen Sensitivity

Spe Specificity

SVM Support Vector Machine

TDF Time Domain Features

T-FDF Time-Frequency Domain Features

WGN White Gaussian Noise

WT Wavelet Transform

LIST OF APPENDICES

APPENDIX A FUNDAMENTALS OF EEG SIGNALS

APPENDIX B METAHEURISTIC ALGORITHMS

APPENDIX C VARIANTS OF FLOWER POLLINATION ALGORITHM: A REVIEW

PENGENALAN ORANG EEG MENGGUNAKAN PENGURAIAN WAVELET MULTI-LEVEL DAN ALGORITMA PENGGANTIAN BUNGA BERBILANG OBJEKTIF

ABSTRAK

Dalam kehidupan moden, teknik mengenal pasti orang dianggap sebagai salah satu tugas yang paling penting dan mencabar. Oleh itu, banyak penyelidik telah mengembangkan beberapa teknik pengenalan untuk berurusan dengan masyarakat digital kita. Baru-baru ini, beberapa kajian menunjukkan bahawa isyarat aktiviti elektrik otak atau electroencephalogram (EEG) memberikan ciri unik yang boleh dianggap sebagai teknik pengenalan pengguna. Tetapi, ini adalah tugas yang mencabar di mana terdapat tiga perkara penting yang harus ditangani dengan teliti dalam pengenalan diri berdasarkan EEG. Pertama, salah satu cabaran penting yang dihadapi adalah pemerolehan isyarat, yang dilakukan dengan meletakkan beberapa elektrod di kepala seseorang. Walau bagaimanapun, tidak perlu meletakkan semua elektrod ini di kepala seseorang. Oleh itu, yang paling relevan untuk pengenalan diri seseorang dapat dikenal pasti dan kemudian menggunakan sebilangan kecil elektrod. Kedua, isyarat EEG mesti diproses untuk mendapatkan ciri EEG yang cekap kerana terdapat beberapa bunyi yang boleh merosakkan isyarat EEG yang asli semasa waktu rakaman. Ketiga, pilih ciri cekap yang dapat diambil dari isyarat EEG untuk mencapai kadar ketepatan tertinggi. Untuk menangani perkara-perkara ini, kaedah pengenalan orang baru yang menggunakan EEG dengan penguraian wavelet pelbagai peringkat dan algoritma pendebungaan bunga pelbagai objektif dicadangkan dalam tesis ini. Kaedah yang dicadangkan diuji menggunakan dua set data EEG standard, iaitu, Kiern's dan Motor Movement / Ima-

gery. Prestasi kaedah yang dicadangkan dinilai menggunakan dua kriteria iaitu ukuran penilaian kualiti isyarat dan langkah pengenalpastian orang. Menariknya, hasil eksperimen menunjukkan bahawa kaedah yang dicadangkan untuk denoising isyarat EEG dapat menghasilkan hasil yang lebih baik daripada konfigurasi manual berdasarkan strategi ad hoc. Selain itu, dibandingkan dengan literatur identifikasi orang berdasarkan EEG, kaedah yang dicadangkan dapat mencapai hasil yang lebih baik daripada yang dihasilkan oleh kaedah canggih menggunakan set data yang sama. Ringkasnya, kaedah yang dicadangkan dapat sangat bermanfaat untuk penggunaan isyarat EEG yang berkesan dalam aplikasi biometrik.

EEG-BASED PERSON IDENTIFICATION USING MULTI-LEVEL WAVELET DECOMPOSITION WITH MULTI-OBJECTIVE FLOWER POLLINATION ALGORITHM

ABSTRACT

In modern life, person identification technique is considered as one of the most important and challenging tasks. Therefore, many researchers have developed several identification techniques to deal with our digital society. Recently, several studies showed that the brain electrical activity or electroencephalogram (EEG) signals provide unique features that can be considered as user identification techniques. But, it is a challenging task where there are three important things must be addressed carefully in any EEG-based person identification. First, one of the significant challenges concerning is a signal acquisition, which is performed by placing several electrodes on a person's head. However, it is not necessary to put all these electrodes on a persons' head. Therefore, the most relevant ones for person identification can be identified and then use a smaller number of electrodes. Second, the EEG signals must be processed to obtain efficient EEG features because there are several noises can corrupt the original EEG signal during the recording time. Third, select efficient features that can be extracted from the EEG signal for achieving the highest accuracy rate. For addressing these points, a novel person identification method that is using EEG with multi-level wavelet decomposition and multi-objective flower pollination algorithm is proposed in this thesis. The proposed method is tested using two standard EEG datasets, namely, Kiern's and Motor Movement/Imagery. The performance of the proposed method is evaluated using two criteria which are signal quality evaluating measures and person

identification measures. Interestingly, the experimental results showed that the proposed method for EEG signal denoising can produce better results than manual configurations based on ad hoc strategy. Also, comparing with the literature of EEG-based person identification, the proposed method is able to achieve results better than those produced by the state-of-arts methods using the same datasets. In a nutshell, the proposed method can be very beneficial for effective use of EEG signals in biometric applications.

CHAPTER 1

INTRODUCTION

1.1 Background

1.1.1 Biometric User Identification

In past three decades, the world has been transformed into a digital society, where every individual is living with a unique digital identifier. The purpose of digital identifier is to distinguish one from the other and deal with digital machines that are surrounding the world (Kumari & Vaish, 2015). Simultaneously, the security level has become an important part in the modern digital society because the digital world with traditional authentication techniques will be highly exposed to fraud (Kumari & Vaish, 2014). Several user identification techniques has been proposed to verify the claimant and prevent imposters using password, token key, MAC address, and identification card. By contrast, the digital identifier that will be used for authentication should be based on physical and behavioural characteristics of the person. This kind of authentication is called biometric authentication.

In general, the origin word of ***biometric*** is referring to two Greek words, *bios* (life) and *metron* (to measure); however, the biometric system as we understand it in the real world is used to measure not life but the identity of a human individual by his or her unique physiological and behavioural characteristics (Ferdous, 2016). The biometric authentication protocol requires the user to do one or a few things, depending on a single or multi factor biometric identification, such as capture his or her face or say a

short phrase to record the authentication traits (Unar, Seng, & Abbasi, 2014). Scientists have developed a significant number of biometric methods that are used successfully worldwide. A biometric protocol can be used either as an *identification* or a *authentication (verification)* system. An identification system can be used to match a person's biometrics against a database to determine his or her identity by searching the closest match. This system is commonly referred to as (*1:N*) matching (Unar et al., 2014). Criminal watchlist application scenarios are a good example of these types of systems. If a person claims to be **X**, then the authentication system will match and compare that person's biometric identifiers with the stored biometrics of **X**; if it matches, then the user is verified, or he or she in **X**; this system is referred to as (*1:1*) matching (Unar et al., 2014). An access control application scenario is an example of an authentication system. Biometrics have several types, such as facial recognition, iris recognition, fingerprint, and voice recognition. A new biometric type is called electroencephalogram (EEG), which is based on the brain electrical activity (Del Pozo-Banos, Alonso, Ticay-Rivas, & Travieso, 2014; Ramadan & Vasilakos, 2017). A biometric user identification system based on EEG signals is proposed in this thesis.

1.1.2 EEG Signals

EEG is a graphical recording of the brain electrical activity that is recorded from the scalp. EEG represents the voltage fluctuations resulting from ionic current flows within the neurons of the brain (Abdulkader, Atia, & Mostafa, 2015). Electroencephalography has been utilised as a unique and valuable method of recording a brain's electrical signals. This method can be performed in two different ways (Tatum IV, 2014), either as invasive EEG or non-invasive EEG. Invasive/intracranial EEG is recorded directly

from the brain through a surgically implanted electrode placed at particular regions of human brain. Non-invasive/ extrarenal EEG is recorded from the surface or cortical layer of the human brain (Abdulkader et al., 2015). Figure 1.1 shows samples for

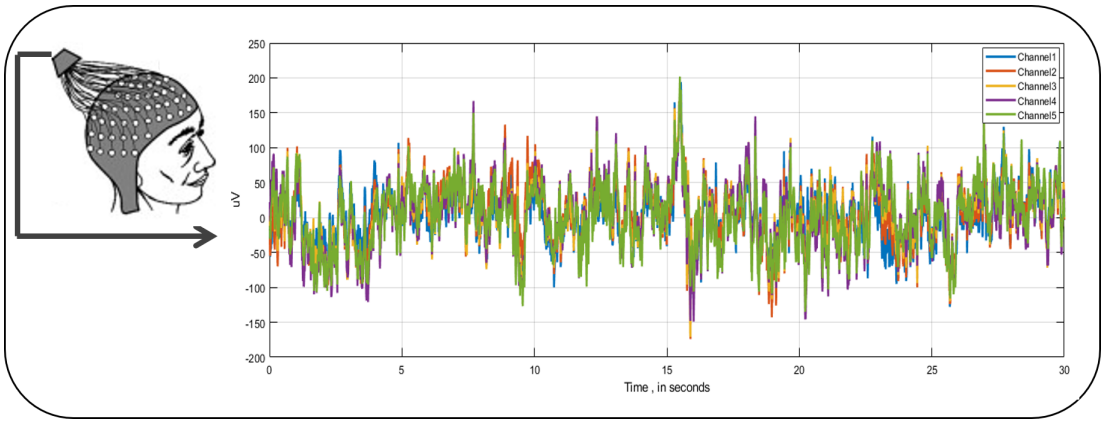

Figure 1.1: EEG signal recording

EEG signals that are recorded from five channels. The EEG signals provides most of the required information about the brain activity; it is efficient in diagnosing some brain diseases, disorders, coma, encephalopathies, and brain death. Non-invasive EEG type, is painless and harmless because it does not need to inject any electrical signal (Ramadan & Vasilakos, 2017).

1.2 Motivation and Problem Statement

Despite the efforts of scientists and researchers to develop a new biometric technique that provides a high level of security for keeping with the digital world, the existing techniques still have some problems. These problems can be classified into two categories: normal problems and spoofing attacks (Marcel et al., 2014).

On the one hand, the normal problems represents the trouble that every individual may face when using the biometric system, such as illumination with face recognition

system or diseases that affect the sound or the fingerprint with voice recognition and fingerprint system, respectively. This problem is not risky to the security systems because of it may prevent unauthorised people to enter the system. This error is called the false reject rate (Unar et al., 2014).

On the other hand, the second category of problems in biometric systems is the spoofing attack. Here, the imposters are trying to enter the system by using spoofing techniques. This type is classified as the most dangerous in security systems because it allows unauthorised persons to enter the system. This error is called the false accept rate (Unar et al., 2014).

Several spoofing attacks (Marcel et al., 2014) on the biometric systems in the real world have already occurred. Some examples of such attacks as given as follows:

1. Face recognition systems have been spoofed using several attacks, such as *'printed photo to spoof face recognition systems on 3 laptops'*,2D face spoofing, and 3D mask attack (Erdogmus & Marcel, 2013; Galbally, Marcel, & Fierrez, 2014; Määttä, Hadid, & Pietikäinen, 2011).

2. Fingerprint scanning has been attacked using *'Gummy Fingers'* (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002).

3. Finger-vein commercial systems have been spoofed by a piece of paper (Tome, Vanoni, & Marcel, 2014).

4. Iris recognition systems have been spoofed using an eyeball in front of an iris scanner (Gupta, Behera, Vatsa, & Singh, 2014).

5. Voice recognition has been spoofed by replaying a voice recording in front of a speaker recognition system (Marcel et al., 2014).

As mentioned above, the current biometric techniques are providing different security levels. Nevertheless, these systems use visible attributes, which provide opportunity for counterfeiting by attackers, such as in face recognition and finger print recognition in which the attackers know the key feature of the system (face or fingerprint matching). Therefore, a new biometric authentication system that can authorise a person depending on *invisible characteristics* and is unaffected by *external threat* should be developed. These two features can be provided using an identification method based on brain signal EEG.

The EEG signals figure as a great alternative for designing new biometric systems since several studies showed that such information presents uniqueness features, universality, and natural robustness to spoofing attacks. These signals represent the graphical recording of the brain electrical activity, which can be measured by placing electrodes (sensors) in different positions of the scalp (Rodrigues, Silva, Papa, Marana, & Yang, 2016). But, for designing an EEG-based person identification system there are some challenges must be addressed carefully which are as follows:

First, one of the significant challenges concerning EEG-based user identification technique is signal acquisition, which is performed by placing several electrodes (sensors) on a person's head. Besides, such a process is usually uncomfortable since it requires good knowledge to place the sensors in their correct positions. Additionally, some questions must be considered: "Is it really necessary to put all these electrodes on

a persons' head? If not, can we identify the most relevant ones for user identification and then use a smaller number of sensors?" (Rodrigues et al., 2016).

Second, the EEG signal denoising problem has been considered a challenging task because of several artifact noises, such as eye blinking, eye movement, muscle activity, and power line interference, which can corrupt the original EEG signal during the recording time. Therefore, to remove these noises, the EEG signals must be processed to obtain efficient EEG features. Accordingly, several techniques have been proposed to reduce EEG noises, such as EEG signal denoising using wavelet transform (WT) (Kumari & Vaish, 2015; Sharma & Vaish, 2016). The success of WT depends on the best configuration of its control parameters, which are often experimentally set. Fortunately, the optimality of the combination of these parameters can be measured in advance by using the mean squared error (MSE) and signal-to-noise ratio (SNR) function.

Third, for any real-world problem which is based on EEG signal, there are several kinds of feature which can be extracted from the EEG signal which can be categorised into three types: time domain features (TDF), frequency domain features (FDF), and time-frequency domain features (T-FDF) (Ang, Chin, Zhang, & Guan, 2012; Oskoei & Hu, 2006; Rechy-Ramirez & Hu, 2011). But for identification problem, it is not clear which kind of EEG features can provide a high accuracy rate. Therefore, these three challenges will be addressed as the main research questions in this thesis. Where the first three questions are intended to address the EEG signal denoising problem in the original signal. Question four and five are intended to address select best features and best channels select respectively.

1. *How can a meta-heuristic algorithm be adopted to find optimal wavelet parameters for EEG signal denoising for obtaining the minimum mean square error (MSE) between the original and denoised EEG signals?*

2. *Is a single objective function sufficient to obtain the best feature extraction?*

3. *What is the best decomposition level that can provide the best feature extraction for EEG rhythms?*

4. *What is the best kind of EEG features which can provide a high accuracy rate.*

5. *Which EEG channels are best in achieving the highest accuracy?*

1.3 Research Objectives

This thesis aims not only to propose a biometric person identification method using EEG signals but also to show the advantage of optimisation that can outperform other techniques in EEG based on biometric identification published in literature. Thus, new alternatives for biometric identification problems are provided. The main objectives of this thesis are provided as follows:

1. To adapt metaheuristic algorithms for finding the optimal wavelet parameters to solve EEG signal denoising problem using the following techniques:

    - Single-objective function to find optimal WT parameters using minimum mean squared error (MSE).
    - Multi-objective function to find optimal WT parameters using two measurement criteria for the denoised signals, namely, minimum mean squared error (MSE) and maximum signal-to-noise ratio (SNR).

2. To extract new EEG features using multilevel wavelet decomposition.

3. To hybridise the flower pollination algorithm (FPA) with β-hill climbing (FPAβ-hc) for improving the quality of the solution in channel selection step.

1.4 Research Contributions

The main contributions of this thesis are given as follows:

1. Adaption metaheuristic algorithms to find the optimal wavelet parameters for solving EEG signal denoising problem.

2. Proposing a multi-objective function of flower pollination algorithm (FPA) to obtain the optimal wavelet parameters.

3. Proposing new method to extract the EEG features using multilevel wavelet decomposition.

4. Hybridising FPA with β-hill climbing (FPAβ-hc) to select the optimal EEG channels that can provide the highest accuracy.

1.5 Research Scope

This thesis focuses on proposing an optimisation method for EEG-based biometric identification technique. FPA, which was proposed by (X.-S. Yang, 2012), is used as an alternative technique to address EEG signal denosing problems with EEG-based person identification system. On the basis of the initial results of adapting FPA with single objective function, multi-objective technique of FPA is proposed to solve the diversity problem encountered by the FPA in tackling the identification system. The

performance of the single and multi-objective FPA techniques are compared against each other and then with those of some comparative techniques in literature with the same datasets.

The FPA is hybridised with the β-hill climbing algorithm to select the optimal EEG channels that can provide the highest accuracy with the identification system (i.e. the best channels from 64 channels for each cognitive task). This way enhances the exploitation capability of FPA to cope with the hugeness of the solution search.

Two standard EEG datasets from previous studies are used (Keirn & Aunon, 1990; Schalk, McFarland, Hinterberger, Birbaumer, & Wolpaw, 2004) to evaluate the performance of FPA. The performance of the proposed method is evaluated using several criteria, such as signal quality evaluating measures, classification accuracy, sensitivity, f-score, specificity and number of channels selected. The obtained results of this thesis are compared with those of state-of-art methods for addressing EEG-based identification problems. In summary, the proposed method can be very beneficial for effective use of EEG signals in biometric applications.

The current research is limited to optimisation in an offline environment with an EEG-based identification system using standard EEG datasets with different cognitive and mental tasks.

1.6 Overview of Methodology

The main goal of the proposed method is to analyse EEG signals for providing the highest performance for user identification. The proposed method is categorised un-

der brain-computer interfacing (BCI) applications; therefore, it involves four phases as shown in Figure 1.2.

Phase I: *EEG signal acquisition*. This phase records EEG signals from the brain activity using electrodes that are placed on the scalp. During the recording, several mental tasks will stimulate the human brain. The EEG signal will be archived in the database for use in the next phase.

Phase II: *preprocessing*. This phase removes EEG artefacts due to corruption of the original EEG signal during recording. The raw EEG signal may contain one or more different noise types that occur due to eye blinking, muscle artefacts and power line noise.

Phase III: *feature extraction and channel selection*. This phase searches and extracts features to reduce the dimensionality of EEG features. The features can be extracted from original EEG signals in the different domains, namely, time domain, frequency domain, and time-frequency domain features. The channel selection process selects relevant channels of the EEG signal by omitting channels with low or no predictive information.

Phase IV: *classification*. This phase uses the selected features as inputs to classify data by using efficient techniques, such as support vector machine (SVM) or linear discriminant analysis (LDA) (Nguyen, Tran, Huang, & Ma, 2013; Nguyen, Tran, Huang, & Sharma, 2012; Nieves & Manian, 2016).

1.7 Overview of Thesis

The thesis is organised into nine chapters as follows:

Chapter 2 provides an overview of the biometric problems and presents the litera-

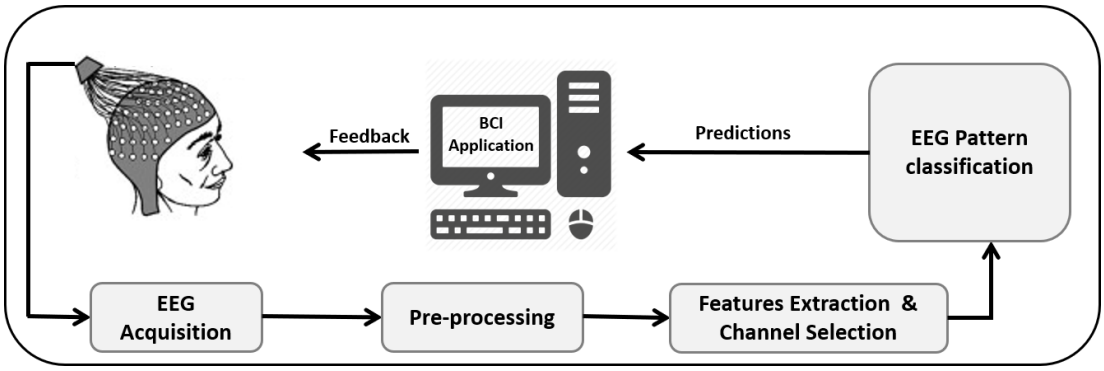

Figure 1.2: Proposed system diagram

ture review of user identification techniques. **Chapter 3** presents the modelling of the problems tackled in this thesis with a thorough description of the methodology and procedures. **Chapter 4 and 5** present the single-objective FPA (FPA-WT) and multi-objective FPA (MOFPA-WT) for solving EEG signal denoising problem. Each chapter describes a particular proposed technique and compared its results with those of state-of-art methods. **Chapter 6** presents the implementation of multi-objective FPA with wavelet (MOFPA-WT) to extract new EEG features for the identification system. **Chapter 7** presents the hybridisation between FPA and β-hill climbing (FPAβ-hc) for selecting the optimal EEG channels that can provide the highest accuracy rate in the identification process. The research conclusion together with some possible future research directions are provided in **Chapter 8**.

CHAPTER 2

EEG-BASED BIOMETRIC IDENTIFIER: LITERATURE REVIEW

2.1 Introduction

This chapter presents biometric user identification techniques in general and EEG based identification system in particular. The techniques tackling EEG based identification system are surveyed and a comprehensive comparative analysis to the existing EEG based identification system techniques is reported.

2.2 Biometric System

A biometric system defined as a technique which uses physical and behavioral characteristics of the person to identify that person, such as face recognition, fingerprint, voice recognition..etc (Unar et al., 2014). Therefore, there are standard steps which must be included in an typical biometric system, where these steps explained as the following:

- **Sample acquisition**: This step, involves capturing of biometric patterns which is passed to the system for processing.
- **Pre-processing**: The main purpose of this step is to remove the noises or unwanted artifacts from the acquired sample by using filters or applying some noise reduction methods for processing the acquired sample.
- **Features extraction**: In this step the system will search for the unique features

from the acquired pattern and the digital representation of these features will be stored in dataset using a templates.

- **Matching step**: matches the extracted features of acquired sample with those of testing sample to obtain a match score. An embedded decision making module *accepts* or *rejects* the claimed identity based on the match score.

Figure 2.1 illustrates the composition of a typical biometric system.

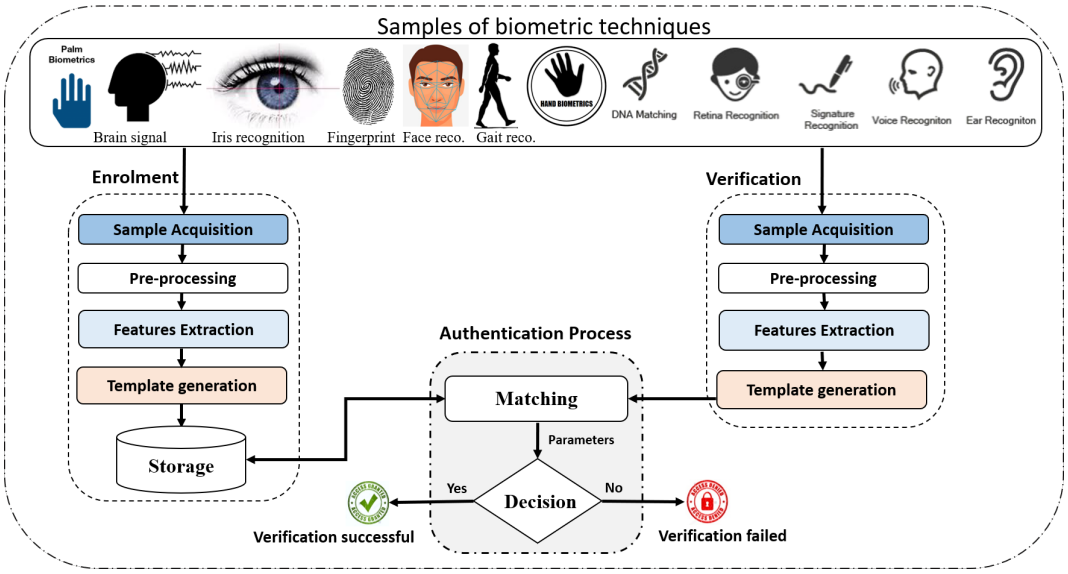

Figure 2.1: Composition of biometric system

2.2.1 Essential Criterion in a Biometric System

According to (A. K. Jain & Kumar, 2012), any biometric system must include the following characteristics:

1. **Universal:** A characteristic every person possesses.

2. **Persistent:** Constant over an extended period, *the attribute should not change as a result of age or chronic disease.*

3. **Distinct:** The pattern must be unique, or at least have another parameter which can be used to distinguish every individual from the other.

4. **Measurable:** The trait should be possible to capture measurements easily in a short time.

5. **Accepted:** The acquitting process should be considered acceptable by a large percentage of the population as being *harmless and painless*.

6. **Processed:** The acquired trait should be dealt with in a format that can be easily accessed, used, compared, and saved.

7. **Attributed:** The properties of capturing data should ensure high reliability and a low error acceptance rate.

8. **Privacy:** the capturing process should not violate the privacy of the person.

9. **Inexpensive:** A highly secured system is expensive technology. Therefore, it is wonderful to have is security system that is economic.

2.2.2 Modes of process in biometric systems

In general, any biometric system should be operated in one of the following modes:

1. ***Verification***, This kind of biometric modes called a 1:1 (one-to-one) system, where the matching process is done by comparing between the extracted features from the user and the enrolled features with that particular identity. The applications include computer logins, ATMs, e-commerce, access control and user authentication on mobile devices (A. K. Jain & Kumar, 2012; Unar et al.,

2014).

2. ***Identification***, in this mode, the system tries to recognize the user by comparing the submitted biometric signature to all the enrolled signatures in the database by making 1:N (*one-to-many*) comparisons without specific identity claim from the user. Identification is a crucial component in negative recognition where the user denies of holding a particular identity. In fact, negative recognition prevents an individual from using multiple identities. The applications include issuance of ID cards, passports, driving licenses, border crossing and welfare disbursements (A. K. Jain & Kumar, 2012; A. K. Jain, Ross, & Prabhakar, 2004).

3. ***Screening***, this is an extension to identification where the biometric system assures that a particular individual does not belong to a watch list of identities by performing 1:N (*one-to-many*) comparisons throughout the database. Example applications include airport security, surveillance activities, public place and public events security etc. (A. K. Jain, Pankanti, Prabhakar, Hong, & Ross, 2004)

2.3 Biometric modalities

This section provides a comprehensive review of the user authentication techniques, while Figure 2.2 presents the most common biometric authentication modalities. In general, for biometric user authentication, it is classified into six types which are i) behavioral modalities such as gait, voice, keystrokes, and signature; ii) Soft modalities such as gender, height, ethnicity, and tattoo; iii) Hand region modalities such as fingerprint, hand geometry, palmprint, finger knuckle print, and hand vein pat-

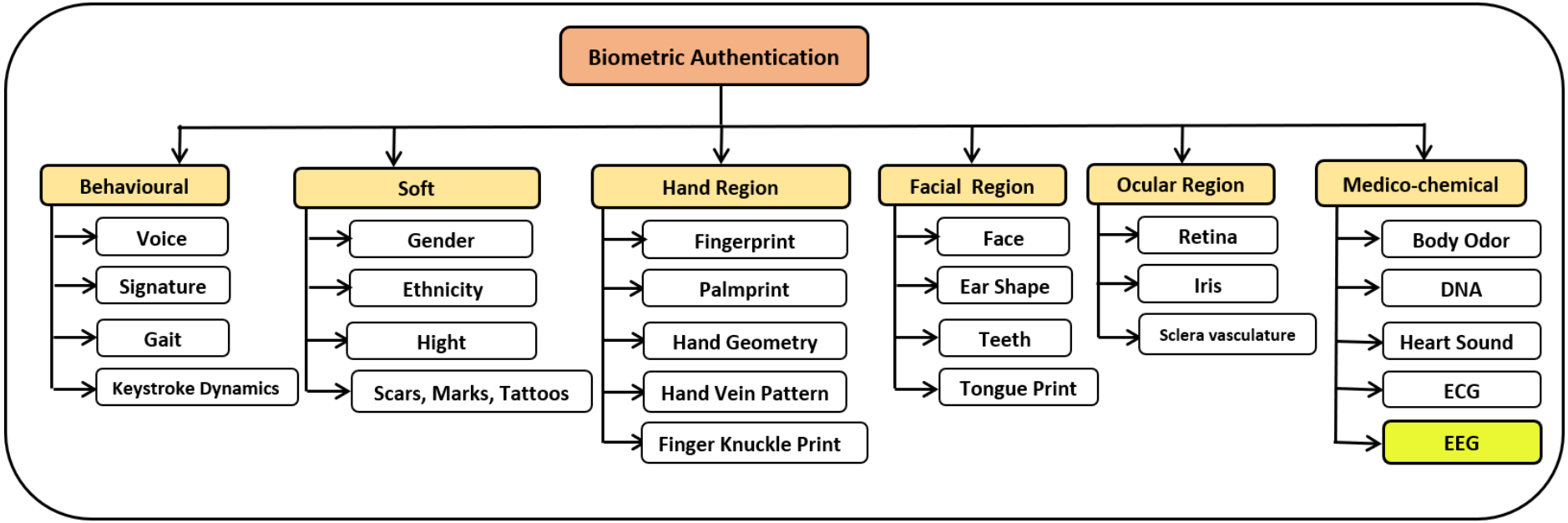

Figure 2.2: Biometric User Authentication Modalities Taxonomy

tern; iv) ; v); vi) Medico-chemical modalities. This chapter will be more focused on biometric techniques because in general and the EEG signal in particular.

2.3.1 Behavioral modalities

Another approach for human authentication has been established based on analysis the behaviour of the humans such as typing styles (keystroke dynamics), vocal characteristics (voice), signature dynamics and the way humans walk (gait). The authentication process in a keystroke dynamics system is through analyzing the typing rhythms of an individual (Karnan, Akila, & Krishnaraj, 2011). A speaker verification system uses the vocal characteristics of an individual to establish the identity either by imposing the fixed vocabulary constraints (text dependent) or in a dynamic way i.e. without imposition of vocabulary constraints on the individuals (Nemati & Basiri, 2011). A signature recognition system establishes the identity based on the analysis of an individual's signature characteristics produced to the system either in static or dynamic modes (Vivaracho-Pascual, Faundez-Zanuy, & Pascual, 2009). Human identification through gait requires the analysis of human motion features such as the shape and dynamics information (Venkat & De Wilde, 2011). Figure 2.3 shows the behavioral modalities.

2.3.2 Soft modalities

The performance of hard biometric systems (face, iris etc.) can be improved by using soft modalities. Several researchers suggested to combine soft biometrics (gender, ethnicity, height etc.) with hard biometric modalities. Nevertheless, several studies claimed to achieve significant improvements in recognition accuracy by combining

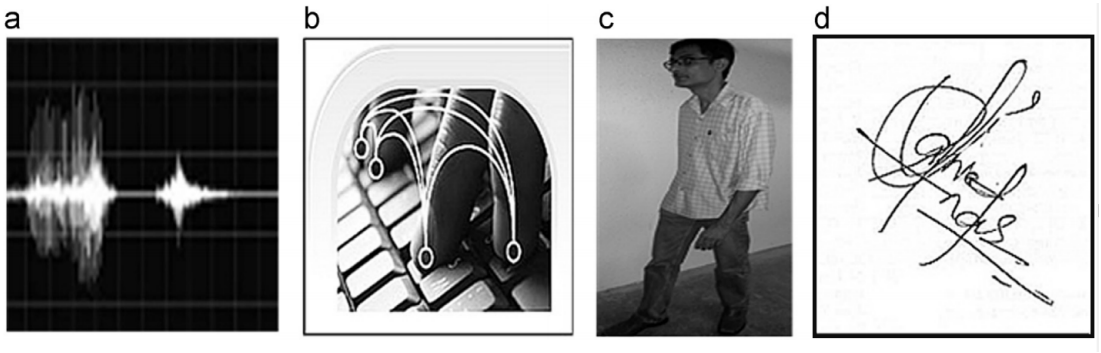

Figure 2.3: Behavioral modalities: (a) voice signal, (b) typing rhythm, (c) gait, (d) signature

soft biometrics with hard biometric modalities (Lyle, Miller, Pundlik, & Woodard, 2010; Park & Jain, 2010).

2.3.3 Hand Region modalities

The human hand contains unique characteristics which can be used to identify user recognition systems. There are several hand based attributes that have been identified and tested such as fingerprint, palmprint, hand geometry, finger knuckle print, finger nail bed and hand vein pattern. However, all these attributes provides different identification level but the best technique in hand region modalities is a fingerprint technology because it can obtain the highest recognition accuracy (Unar et al., 2014). Figure 2.4 shows the hand region modalities.

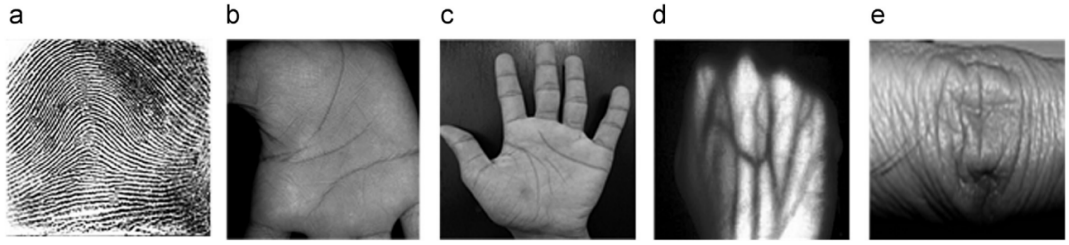

Figure 2.4: hand modalities: (a) fingerprint, (b) palmprint, (c) hand geometry,(d)hand vein pattern, and (e) finger knuckle print

2.3.4 Facial Region modalities

From several decades, human facial region has been an interesting topic for computer vision researchers to discover new features that can be used to recognize such as the face, ear shape, tongue print (A. K. Jain & Kumar, 2012). Although being the most natural biometric characteristic, the non-linear structure of human face makes it complex pattern recognition problem as well as an active area of research in computer vision applications (Abate, Nappi, Riccio, & Sabatino, 2007). However, human facial region biometric systems cannot guarantee reliable identification in presence of artifacts such as application of cosmetics and plastic surgery. Moreover, a person's face may change or be changed over time which may have a significant impact on the accuracy of such systems. In addition, the expensive imaging hardware is another factor which limits the use of such systems. In order to develop robust face recognition systems, the research community proposed the idea of human recognition based on facial thermograph which shows the heat radiation patterns of human face due to the presence of vascular structure beneath the human skin (Unar et al., 2014). Figure 2.5 shows the facial region modalities.

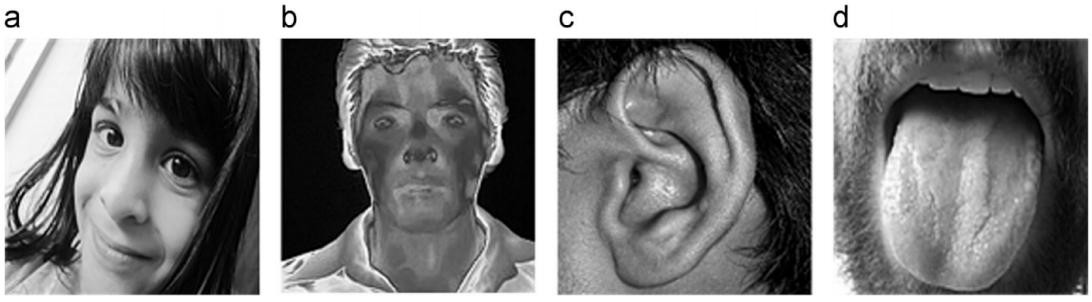

Figure 2.5: Facial modalities: (a,b) face, (c) ear shape,(d) tongue print

2.3.5 Ocular Region modalities

Human ocular region attained considerable attention of researchers in the past decade due to the fact that this region possesses most accurate, highly reliable, well protected, stable and almost impossible to forge biometric signatures, for instance, retina, iris and sclera vein pattern. Figure 2.6 shows ocular region modalities.

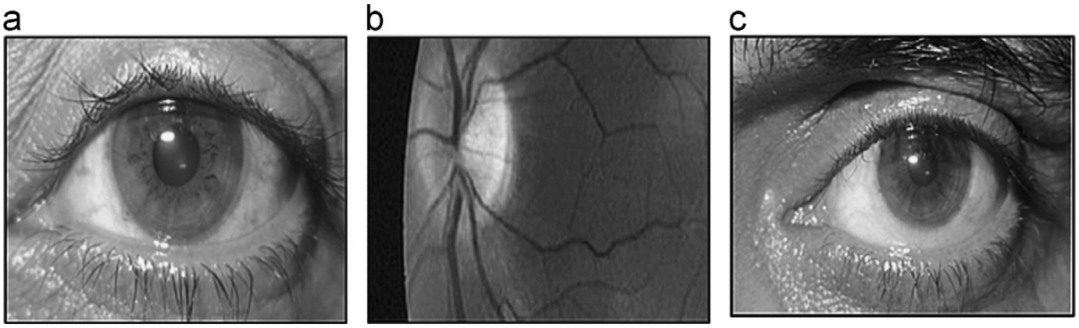

Figure 2.6: Ocular modalities: (a) iris, (b) retina, (c) sclera and vasculature

2.3.6 Medico-chemical modalities

One of the classical classification that we classify body odor, Deoxyribonucleic Acid (DNA), heart sound and Electrocardiogram (ECG) as medico-chemical biometrics due to the fact that the recognition process requires specialized medical/chemical sensors for data acquisition. Nevertheless, the authenticity of DNA is well established whereas identification based on the analysis of heart sound and ECG signals need conformity through large scale studies. Consequently, DNA being a well-established and most accurate biometric signature dominates other group members (Unar et al., 2014).

Table 2.1: Description of attack vectors

Attack	Description
Fake Biometric	in this point attacker can provide a fake biometric pattren and can gain access to system.
Modify biometric data	at this point attackers are able to modify the data and submit the further processing.
Override feature extractor,	this type of attack overrides the feature which are extracted from genuine .
Modify feature vector	at this stage modifications are possible with various algorithms in feature vector which are extracted from the genuine biometric trait
Override matcher	this threat vector could attack where matching software works and manipulate the result and falsely produce the result.
Modify template	this threat vector could modify the template by the reconstruction samples.
Modify template data	in the threat unauthorized changes are made astemplates are modified, replaced or added to the system for further processing
Override final decision	this type of attack overrides the decision data or injects a false acceptance between the system and the end device.

2.3.7 Previous Biometric Security Vulnerabilities

According to (Kumari & Vaish, 2014), the current biometric systems have various prone area where an attacker can attack easily. Figure 2.7 shows the most significant attack points which can be used by imposters. Table 2.1 provides more description of these attacks.

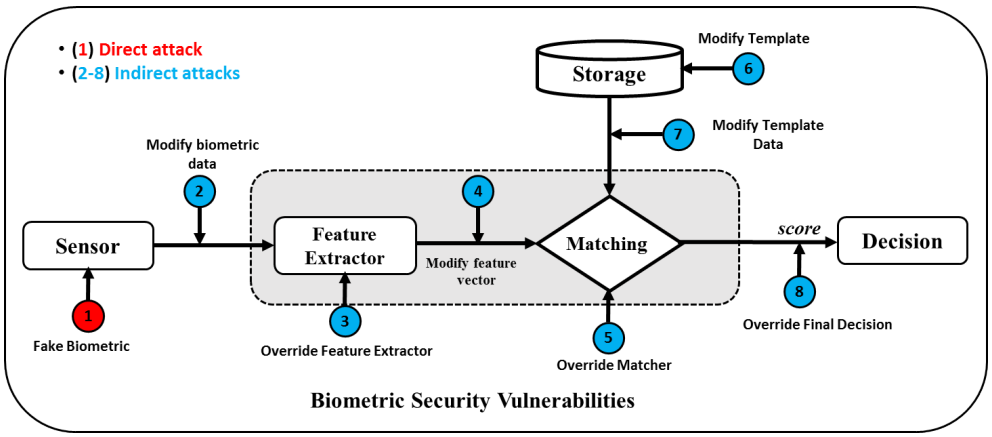

Figure 2.7: Ratha's framework of Various Attacks Vector

On the other hand, (Marcel et al., 2014) presents several spoofing attacks on the biometrics systems in the real world which is described as follows:

1. Face recognition system spoofed using several attacks such as *"printed photo to spoof face recognition systems on 3 laptops"*,2D face spoofing, and 3D mask attack (Erdogmus & Marcel, 2013; Galbally et al., 2014; Määttä et al., 2011).
2. Fingerprints scanning has been attacked using *Gummy Fingers* (Matsumoto et al., 2002).
3. Finger-vein commercial system spoofed by a piece of paper (Tome et al., 2014).
4. Iris recognition system spoofed by presenting an eyeball in front of a iris scanner (Gupta et al., 2014).
5. Voice recognition spoofed by replaying a voice recording in front of a speaker recognition system (Marcel et al., 2014).

Figure 2.8 shows the most significant spoofing attacks on the biometrics systems in the real world.

As aforementioned, the current biometric systems are providing different security level. But, these systems uses visible attributes, which provides an opportunity for counterfeiting by attackers such as in the faces recognition and finger print where the attackers know the key-feature of the system (face or fingerprint match). Therefore, we are looking to a new biometric authentication system which is able to authorize a person based on *invisible characteristics* and can not affected by an *external threat*. The use of these features can be confusion by using authentication method based on

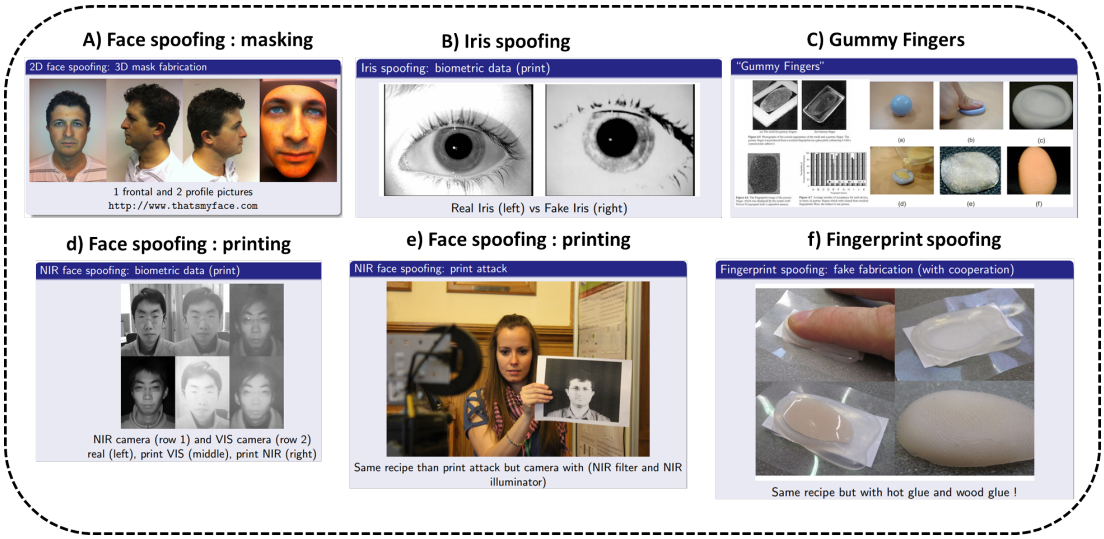

Figure 2.8: Indirect biometric spoofing examples are taken from (Marcel et al., 2014)

brain signals (EEG). Where the attackers can not manipulate the brain signals because there is no known method 'Indirect attacks' that enables the attackers to access and control the brain signals. In addition, the brain signals are not affected by any external threat, because with any fear or stress the value of EEG rhythms (δ,θ,α,β, and γ) will be suddenly increasing, which will inform the system there is something abnormally happened to the genuine person. Finally, for all the these advantages which are provided by EEG, in this dissertation a new biometric user authentication based on EEG signal has been proposed.

2.4 EEG-based biometric system components

To design an authentication system using EEG, there are four phases should be carefully selection to achieve the best accuracy rate. These phases includes: EEG signal acquisition, Pre-processing, Features extraction and feature selection, and Classification. Figure 2.9 shows the visualization of these phases. Therefore, the main objective of this section is to explain in details of each phases as well as to review what are the most important techniques have been applied.

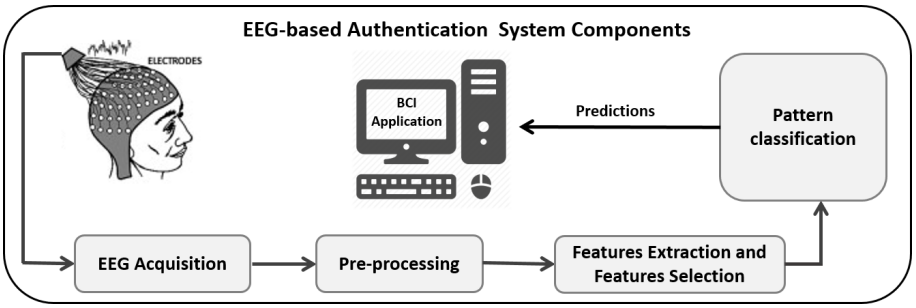

Figure 2.9: EEG-based Authentication System Components.

2.4.1 EEG Signals Acquisition

EEG signals are recorded from the brain using *invasive* or *non-invasive* techniques (Ramadan & Vasilakos, 2017). The main difference between these techniques is that the invasive approach involves the use of electrode arrays implanted inside the brain, such as *ECoG BCI* for arm movement control. For noninvasive approach, there are several techniques to record the brain activity using different types of signal captures devices such as, electrical activity from the scalp which is called EEG (Rao, 2013).

2.4.2 EEG Pre-Processing

In general, the preprocessing is a technique that always used to remove unwanted artifacts from the EEG signal and hence improve the signal to noise ratio (SNR). A pre-processing phase aids in improving the performance of the system by separating the noise from the actual signal. There are several techniques for the pre-processing such as using filters or applying some noise reduction methods (Mammone, 2018).

2.4.3 EEG Feature Extraction

The feature extraction stage involves the transformation of the raw signal to relevant data structure, called feature vector, by deleting noise and highlighting important