Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Timo Briddigkeit

Überprüfung der Eignung von Elektroenzephalografiedaten eines Brain-Computer-Interfaces zur computergestützten Authentifizierung

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Timo Briddigkeit

Überprüfung der Eignung von Elektroenzephalografiedaten eines Brain-Computer-Interfaces zur computergestützten Authentifizierung

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Wolfgang Fohl
Zweitgutachter: Prof. Dr.-Ing Martin Hübner

Eingereicht am: 15. September 2014

Timo Briddigkeit

Thema der Arbeit
Überprüfung der Eignung von Elektroenzephalografiedaten eines Brain-Computer-Interfaces zur computergestützten Authentifizierung

Stichworte
Brain-Computer-Interface, Neurofeedback, Authentifikation, Signalverarbeitung

Kurzzusammenfassung
Dieses dokument behandelt die Überprüfung der Eignung von Elektroenzephalografiedaten eines Brain-Computer-Interfaces zur computergestützten Authentifizierung. Darüber hinaus wird ein Überblick über die Arbeitsweise mit Brain-Computer-Interfaces gegeben.

Timo Briddigkeit

Title of the paper
Examinating the suitability of electroencephalography data of a brain-computer interface to computer-assisted authentication

Keywords
Brain-Computer-Interface, neurofeedback, authentication, signal processing

Abstract
This document deals with examinating the suitability of employing electroencephalography data of a brain-computer interface to computer-assisted authentication. In addition, an overview of how to work with brain-computer interfaces will also be provided.

Inhaltsverzeichnis

1 Einleitung

Brain-Computer-Interfaces (kurz BCI) sind in den letzten Jahren für den Massenmarkt erschwinglich geworden und erfreuen sich inzwischen auch im Unterhaltungsbereich zunehmender Beliebtheit. Forschungsgebiet der letzten Jahre ist unter anderem die Frage, ob sich mit Hilfe von Elektroenzephalografiedaten eines Brain-Computer-Interfaces Benutzer so präzise voneinander unterscheiden lassen, dass dies für die computergestützte Authentifikation verwendbar ist. Zu diesem Thema hat es in den letzten Jahren eine Reihe von Untersuchungen mit sehr unterschiedlichen Ergebnissen gegeben. Diese Arbeit soll einen Beitrag leisten, die Eignung von Elektroenzephalografiedaten eines Brain-Computer-Interfaces zur computergestützten Authentifizierung aus aktuellen Standpunkten zu analysieren und zu bewerten.

1.1 Thema dieser Arbeit

Im Rahmen dieser Arbeit wird eine bestehende Open-Source Software für die Aufzeichnung von Elektroenzephalografie-Rohdaten des Neurosky Mindwave Mobile BCIs erweitert und eine vorhandene Studie der University of California in Berkeley betrachtet. Die Ergebnisse werden dann anhand der allgemeinen Anforderungen an biometrische Merkmale bewertet.

1.2 Aufbau

Zunächst werden die fachlichen Grundlagen erläutert, auf denen diese Arbeit aufbaut. Anschließend werden einige der heute üblichen Authentifikationsmechanismen in ihren Unterarten beschrieben. Ebenso findet sich eine allgemeine Einführung in die Arbeit mit Brain-Computer-Interfaces, bevor es anschließend zu einer speziellen Betrachtung der in dieser Arbeit eingesetzten Hardware kommt.
Daraufhin wird die Eignung von Elektroenzephalografiedaten für die computergestützte Authentifikation anhand einer Referenzstudie untersucht und bewertet.
Abschließend werden die Ergebnisse und die gewonnenen Erkenntnisse zusammengefasst sowie eine Reihe von Vorschlägen unterbreitet, mit denen diese in dieser Arbeit gewonnenen Erkenntnisse erweitert werden können.

2 Authentifikation

Wann immer ein Nachweis einer behaupteten Identität gegenüber einem System gefordert ist, wird eine Authentifikation durchlaufen. Dabei authentisiert sich ein Subjekt (z.B. ein Mensch) oder ein Objekt (z.B. ein Prozess) gegenüber einem System, welches daraufhin authentifiziert. Eine korrekte Authentifizierung erfordert eine Charakterisierung durch wohldefinierte Eigenschaften zur zweifelsfreien und eindeutigen Identifizierung. Diese Eigenschaften werden häufig als Credentials bezeichnet.

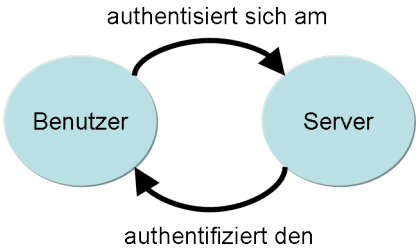

Abbildung 2.1: Authentifikationsvorgang gegenüber einem System

In der Praxis existieren unterschiedliche Authentifikationstechniken, welche zum Beispiel auf ein spezifisches Wissen, auf einen persönlichen Besitz oder auf ein biometrisches Merkmal zurückgreifen. Es treten auch häufig Kombinationen aus zwei oder mehreren Authentifizierungstechniken auf, man spricht dann von einer Mehr-Faktor-Authentifikation. Ein Beispiel aus dem alltäglichen Leben wäre ein Bankautomat, bei dem man sowohl etwas wissen als auch etwas besitzen muss. [Eck13]

Im Rahmen der Authentifikation werden sensible Daten übertragen, die unter Umständen von einem Angreifer abgehört werden können, um so eine falsche Identität vorzutäuschen. Um diese sensiblen Daten vor unbefugtem Zugriff zu schützen, werden kryptographische Verfahren eingesetzt. [Har08]

2.1 Authentifikation durch Wissen

Authentifikationstechniken, die ein spezifisches Wissen des Benutzers voraussetzen, sind heute immer noch am häufigsten verbreitet. Hierbei kommen sogenannte Challenge-Response-Systeme zum Einsatz. Bei diesem Verfahren wird einem Teilnehmer des Systems eine Aufgabe gestellt, welche der andere Teilnehmer lösen muss, um die Kenntnis eines bestimmten Geheimnis zu beweisen, ohne diese Information selbst zu übertragen. Charakteristisch für Authentifikation durch Wissen ist die Tatsache, dass sich das geheime Wissen leicht mit weiteren Teilnehmern teilen und duplizieren lässt. Allerdings könnte dieses geheime Wissen auf dem Transportweg kompromittiert werden.
Den wohl bekanntesten Vertreter dieser Authentifikationsmethode stellt das passwortbasierte Verfahren dar. Hierbei authentifiziert sich ein Benutzer gegenüber einem System mit einem vorher vereinbarten Geheimnis, dem Passwort. Das im System hinterlegte Passwort würde eine sehr sensible Information darstellen und wird daher aus Sicherheitsgründen mit kryptographischen Verfahren - zum Beispiel kryptographischen Hashfunktionen - geschützt. Der eigentliche Hashwert wird neben dem Passwort mit Informationen, die den Benutzer charakterisieren (zum Beispiel Benutzerkennung, Vor- und Nachnamen), errechnet und in einer Passwortdatei gespeichert.

Kryptographische Hashfunktionen bieten zudem die Eigenschaft, dass sie kollisionsresistent oder eine Einwegfunktion (oder beides) sind.
Eine mathematische Einwegfunktion $f : X \to Y$ muss folgende Eigenschaften aufweisen:

1. Die Berechnung $y = f(x)$ ist wenig rechenintensiv, d.h. in Polynomialzeit lösbar.
2. Für die Rückberechnung eines bekannten Funktionswertes y zur beliebigen Inversen $f(x) = y$ existiert allerdings kein Algorithmus, der in Polynomialzeit läuft.[KL14]

Für ein gegebenes Passwort einen Hashwert zu berechnen, ist nach diesen Merkmalen sehr einfach. Die Wiederherstellung eines Passwortes aus einem bekannten Hashwert ist allerdings nicht ohne erheblichen Rechenaufwand möglich. Zusätzlich ist eine solche Passwortdatei mit Zugriffsrechten des Betriebssystems geschützt und verhindert so das unautorisierte Überschreiben von Hashwerten oder durch Beschränkung der Lesezugriffe sog. Passwort-Cracking-Angriffe.
Die Sicherheit der im System hinterlegten Hashwerte hängt demnach von zwei Faktoren ab:

1. Die Stärke der kryptographischen Hashfunktion

2. Die Qualität der Rechtevergabe und Zugriffskontrolle

Ein weiterer Angriffspunkt der Authentifikation durch Wissen besteht darin, dass das geheime Wissen eventuell erraten werden kann. Die Benutzer eines Systems neigen häufig aus Bequemlichkeit dazu, einfache und oft sehr kurze Passwörter zu wählen. So zeigen Untersuchungen, dass Passwörter häufig nur aus fünf Groß- oder Kleinbuchstaben bestehen. [Eck13, S. 470] Dies erhöht die Angreifbarkeit für sog. Dictionary-Angriffe, bei denen eine Liste mit häufig verwendeten Passwörtern durchprobiert wird. Bei sehr kurzen Passwörtern könnte auch eine sog. Brute-Force-Methode - das Ausprobieren aller möglichen Kombinationen - in annehmbarer Zeit zum Erfolg führen. Schutz auf Benutzerseite bieten spezielle Datenbanken für Passwörter, sog. Passwort-Manager, welche lange und zufällige Passwörter für jeden Dienst einzeln generieren und kryptographisch gesichert abspeichern. Die Entschlüsselung der Datenbank erfolgt mit einem sog. Masterpasswort. Der Benutzer muss sich somit nur noch ein sicheres Passwort merken, um auf alle anderen Passwörter zuzugreifen.

Eine weitere häufig empfohlene Methode [Eck13, S. 471] besteht darin, von einem beliebigen Satz die Anfangsbuchstaben zu nehmen. So wird z.B. aus dem Satz *Gibt es denn jeden Freitag Fisch in der Mensa?* das Passwort *GedjFFidM?*.

2.1.1 Einmal-Passworte

Eine weitere Möglichkeit der Authentifikation besteht in der Nutzung von Einmal-Passwörtern. Jedes Passwort ist bei diesem Verfahren - wie der Name bereits erahnen lässt - nur für eine einmalige Verwendung gültig. Jede Authentifikation erfordert also ein neues Einmal-Passwort. Dieses Verfahren bietet Schutz gegen sog. Replay-Attacken, bei denen der Angreifer die verschlüsselte Authentifikation aufzeichnet und anschließend selbst sendet, um so eine fremde Identität vorzutäuschen. Die Kenntnis der entschlüsselten Daten ist bei dieser Angriffsmethode nicht nötig.

Ein Beispiel für ein solches Authentifikationsverfahren aus dem Alltag sind Kennwortlisten bzw. Transaktionslisten (TAN-Listen) beim Online-Banking. Dabei werden vorgefertigte Listen mit Kennwörtern bei beiden Teilnehmern hinterlegt und entweder der Reihe nach abgearbeitet oder ein noch nicht verwendetes Kennwort frei gewählt. Das Kennwort wird übermittelt und anschließend von beiden Teilnehmern aus der Liste entfernt.

Ein weiteres Beispiel wäre das S/Key-Verfahren [HMNS96], dass für client-server-artige Anwendungsfälle entwickelt wurde. Das Verfahren setzt eine kryptographisch sichere Hashfunktion

voraus und ist in eine Initialisierungsphase, welche nur einmal durchzuführen ist und in die einzelnen Authentifizierungsschritten aufgeteilt. Der Benutzer überlegt sich sein geheimes Passwort s, das dem Server nicht bekannt sein muss.
Wie bereits bei der herkömmlichen Passwort-Authentifikation wird hier ein Nutzen aus der Einwegfunktion der kryptographischen Hashfunktion f gezogen und es werden auf Clientseite aus dem geheimen Passwort s und einem Seed-Wert k die einzelnen Einmal-Passworte $p_1, ..., p_n$ berechnet.

$$p_i = f^i(s|k) \text{ für } i = 1, ..., n$$

Übertragen werden nur die jeweiligen Einmalpasswörter p_i. Zum Abschluss der Initialisierung wird von der Clientseite das letzte erstellte Passwort p_n zusammen mit dem für den Benutzer eindeutigen Seed-Wert k an den Server übertragen. Durch den Seed ist es möglich dasselbe geheime Passwort s an unterschiedlichen Rechnern zu verwenden. Der Seed-Wert maskiert also das geheime Passwort und übernimmt seine Funktion.

Für die letzten i erfolgreichen Authentifikationen des Clients gegenüber dem Server gilt, dass dieser das i-te Passwort p_i bereits überprüft und indiziert hat. Bei einer erneuten Authentifikation durch den Client fordert der Server vom Client das $(i-1)$-te Passwort, indem er die laufende Nummer $i-1$ sowie den vorher vereinbarten Seed-Wert k übermittelt.

Der Client wählt daraufhin das entsprechende Passwort $p_i - 1$ und überträgt es zum Server. Der Server wiederum kann nun aus dem Wert p_i den korrekten Wert $p_i - 1$ durch $i-1$-maliges Anwenden der kryptographischen Hashfunktion f auf $p_i - 1$ überprüfen, da gilt:

$$p_i = f^i(s|k) = f(f^{(i-1)}(s|k)) = f(p_{i-1})$$

Somit ist zu überprüfen:

$$f(p_{i-1}) \stackrel{?}{=} p_i$$

Angesichts der Eigenschaften von Einwegfunktionen (siehe oben) lässt sich $f(p_i - 1)$ effizient berechnen. Die Authentifikation ist erfolgreich, sofern die Überprüfung positiv verläuft. Der Server ersetzt nun den aktuellen Wert p_i durch das zuvor verbrauchte Passwort $p_i - 1$ und dekrementiert den Sequenzzähler. [Eck13]

2.2 Authentifikation durch Besitz

Eine weitere Möglichkeit der Authentifikation bietet die Verwendung eines speziellen Besitztums. Mit der elektronischen Gesundheitskarte, dem elektronischen Reisepass oder der

Mobilfunkkarte haben derartige Authentifikationstechniken längst Einzug in unseren Alltag gehalten.
Besitzbasierte Authentifikation bedient sich meistens intelligenter Chipkarten (sog. Smartcards) oder USB-Tokens. Diese Smartcards und Tokens können überreicht und weitergegeben, in manchen Fällen auch dupliziert werden. Die Verwaltung des Besitzes ist relativ unsicher, da das Besitztum verloren gehen oder entwendet werden kann. Außerdem ist es mit höherem Aufwand verbunden, da der Benutzer das Besitztum bei jeder Authentifikation mit sich führen muss. Auch die Verwaltung der Benutzer unterliegt einem deutlich höheren Aufwand, weshalb diese Art der Authentifikation häufig als Zwei-Faktor-Authentifikation in Verbindung mit einem geheimen Wissen eingesetzt wird. Bei smartcardbasierten Authentifikationen unterscheidet man drei Schritte:

1. Der Benutzer authentifiziert sich gegenüber der Karte mit einer Personal Identification Number (kurz PIN).
2. Die Authentifikation mit dem Zielsystem (z.B. Kartenlesegerät)
3. Das Zielsystem authentifiziert sich gegenüber der Karte.

[Eck13]

2.3 Biometrische Authentifikation

Das Wort Biometrie leitet sich von den griechischen Worten *bios* für Leben und *metron* für Maß ab. Biometrische Authentifikation bezeichnet die physiologischen oder verhaltenstypischen Eigenschaften, welche eine Person eindeutig charakterisieren. Die Biometrie hat im Sicherheitsbereich eine längere Entwicklungsgeschichte hinter sich, oft gebremst durch hohe Kosten, bedingt durch zusätzlich benötigte Geräteausstattung. Heute findet Biometrie zum Beispiel Anwendung in Hochsicherheitsbereichen der Strafverfolgung und vereinzelt in modernen Smartphones als Alternative zur herkömmlichen PIN- oder Muster-Authentifikation. Biometrische Techniken zur Authentifikation lassen sich grob in zwei Kategorien unterscheiden: physiologisch-statische Eigenschaften sowie verhaltenstypisch-dynamische Eigenschaften einer Person. Beispiele für physiologische Merkmale sind Fingerabdrücke oder die Retinamerkmale im Augenhintergrund. Beispiele für verhaltenstypische Merkmale sind das Tippverhalten, z.B. der Rhythmus oder Satzbau, sowie die Stimme. Dieses Themengebiet umfasst viele weitere Merkmale. Noch in der Forschung befinden sich z.B. der Hautwiderstand oder Körpergeruch als statisches Merkmal [Eck13, S. 496] oder Gehirnwellen [CNWJ13] [ABTV11] [MM07] als

dynamisches Merkmal.
Letztere liegen im Rahmen der Untersuchung auf Eignung im Fokus dieser Arbeit, da es in den letzten Jahren diverse Publikationen zu diesem Thema gegeben hat.
Biometrische Techniken arbeiten alle nach folgendem Schema:

1. Referenzwerte der zu analysierenden biometrischen Eigenschaften werden sensorisch erfasst und digitalisiert.

2. Aus den Referenzwerten werden charakteristische Eigenschaften extrahiert und abgespeichert.

3. Mit einem speziellen Gerät (z.B. Videokamera oder Fingerabdrucksensor) wird das entsprechende biometrische Merkmal erfasst.

4. Die soeben erfassten Daten werden mit den gespeicherten Referenzdaten verglichen.

Die Hauptproblematik biometrischer Authentifikation besteht im Wesentlichen darin zu entscheiden, ob die erfassten Werte mit den Referenzwerten übereinstimmen. Generell wird ein solcher Abgleich zwar auch bei anderen Authentifikationstechniken angewandt, jedoch handelt es sich da um die Prüfung auf Korrektheit einer PIN, eines gehashten Passworts oder eines Challenge-Response-Protokolls. Hierbei ist es technisch möglich eine 100-prozentige Übereinstimmung zu überprüfen. Bei biometrischen Eigenschaften hingegen kommt es oft zu Messungenauigkeiten, beispielsweise durch Lichtverhältnisse, Verschmutzungen, Stimmungsschwankungen (Stimme oder Gesichtsmotorik sind verändert), Stresssituationen (Tippverhalten oder Unterschrift sind verändert) oder Verletzungen, welche Auswirkungen auf diverse biometrische Verfahren haben könnten. Da es praktisch nie zu einer 100-prozentigen Übereinstimmung wie bei anderen Authentifikationsverfahren kommen kann, ist es notwendig gewisse Toleranzschwellen festzulegen. Eine exakte Übereinstimmung des Messergebnisses mit den Referenzdaten, kann mit hoher Wahrscheinlichkeit als Fälschung eingestuft werden. Bei der Überprüfung wird mit Hilfe von Korrelationstests die Abweichung der jeweiligen Referenzwerte ermittelt und dann mit Auswertungsalgorithmen überprüft.

statisch	dynamisch
Fingerabdruck	Tippverhalten
Gesichtserkennung	Stimmerkennung
Iriserkennung	Handschrift
Retinamerkmale	Sitzverhalten
Handgeometrie	Gehirnwellen
Venenmuster	
Erbinformation	

Tabelle 2.1: Übersicht einiger kategorisierter biometrischer Merkmale

2.4 Anforderungen an biometrische Merkmale

Um als biometrisches Merkmal im Rahmen einer Authentifikation zu genügen, muss das Merkmal folgenden allgemeinen Anforderungen entsprechen: [Eck13, S. 497]

1. **Universalität**: Jede Person verfügt über das Merkmal.
2. **Eindeutigkeit**: Das Merkmal ist für jede Person verschieden.
3. **Beständigkeit**: Das Merkmal ist unveränderlich.
4. **Quantitative Erfassbarkeit**: Das Merkmal ist sensorisch erfassbar.
5. **Performanz**: Die Erfassung des Merkmals ist mit einer erforderlichen Genauigkeit performant durchführbar.
6. **Akzeptanz**: Die Erfassung des Merkmals wird von den Benutzern akzeptiert.
7. **Fälschungssicherheit**: Das Merkmal lässt sich nur mit hohem Aufwand duplizieren.

Diese Anforderungen sind allgemein gehalten und teilweise unpräzise. Untersucht man die Eignung von Fingerabdrücken als geeignetes biometrisches Merkmal anhand dieser Anforderungen, stellt man fest, dass sie teilweise diesen Anforderungen nicht oder nur bedingt genügen. Zwar verfügt jede Person über dieses Merkmal (Universalität) und es erfüllt auch die Eindeutigkeit, aber problematisch ist die Anforderung der quantitativen Erfassbarkeit und Performanz. Fingerabdrücke sind nicht bei jedem Menschen sensorisch erfassbar, z.B. weil sie zu wenige erfassbare Eigenheiten aufweisen. Die Arbeit mit Klebstoff aus dem Modellbau kann z.B. dazu führen, dass sich die Porenstruktur vorübergehend verändert. Auch ist die Fälschungssicherheit nur bedingt gegeben. Fingerabdrücke werden überall hinterlassen, z.B.

Abbildung 2.2: Aufnahme eines Fingerabdrucks [Eck13]

Abbildung 2.3: Bearbeitung und Auswertung eines Fingerabdrucks [Eck13]

durch Anhaften von Fett und Schweiß der Haut an den berührten Gegenständen. Diese Fingerabdrücke können sichtbar gemacht und in Form einer Attrappe[1] gefälscht werden. Im Vergleich zu anderen Körpermerkmalen dürfte der Fingerabdruck jedoch eine sehr hohe Akzeptanz unter den Nutzern hervorrufen. Die körpereigenen Merkmale erfüllen die oben genannten Anforderungen also mit unterschiedlicher Qualität, was wiederum als Indikator für die Qualität des Merkmals herangezogen werden kann.

[1] http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren.de abgerufen am 10.09.2014

2.5 Fehlerraten

Angesichts der vorher erläuterten Problemstellung biometrischer Authentifikation werden zwei Arten von Fehlern unterschieden:

1. Abweisung eines eigentlich berechtigten Benutzers
2. Authentifizierung eines unberechtigten Benutzers

Fehler der ersten Kategorie sprechen für zu strenge Toleranzschwellen und führen bei häufigem Auftreten zu Unbehagen der Benutzer. Bei Fehlern der zweiten Kategorie sind die Toleranzschwellen zu niedrig und unberechtigte Benutzer erhalten Zugriff oder Zugang zu sicherheitskritischen Bereichen.
Die Güte eines Erkennungssystems ermittelt man mit Fehlerraten zur Abweisung eines eigentlich autorisierten Nutzers (engl. *false rejection rate* FRR) bzw. FAR (engl. *false acceptance rate*) für fälschlich autorisierte Benutzer. Den Schnittpunkt beider Fehlerraten, also der Punkt, an dem FRR und FAR gleich groß sind, bezeichnet man als Gleichfehlerrate EER (engl. *equal error rate*), wobei dieser Wert möglichst gering sein sollte.

Derzeit werden internationale Standards zur Überprüfung der Leistungsfähigkeit der einzelnen Sensoren entwickelt und sind bereits teilweise verabschiedet. Diese Standards resultieren aus der Tatsache, dass die Hersteller die Werte selbst für ihre jeweiligen Geräte ermittelt haben und so ein Vergleich zwischen unterschiedlichen Geräten nur schwer möglich ist, bzw. es keine Informationen über das Zustandekommen der Werte gibt.

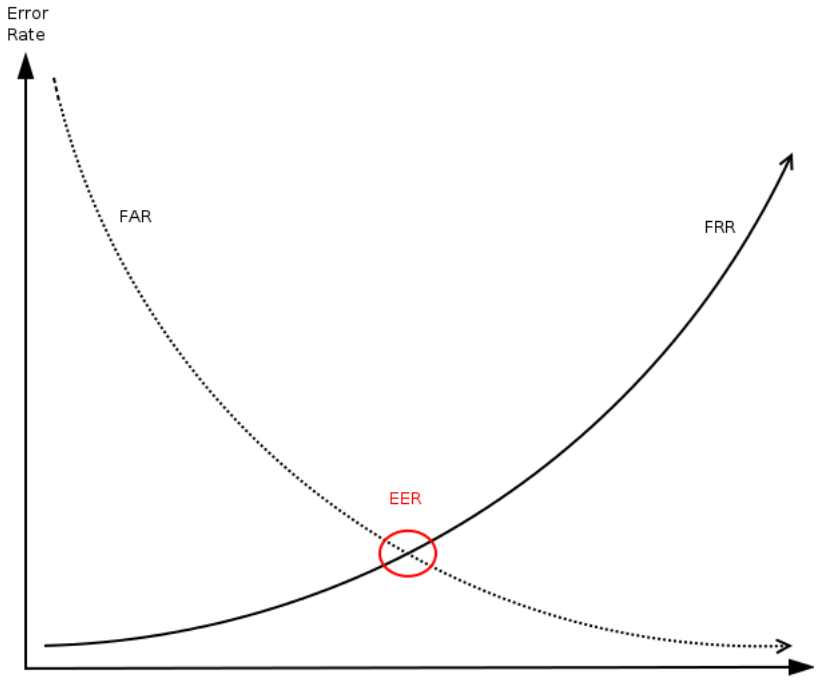

Abbildung 2.4: Zusammenhang zwischen FAR und FRR [Eck13]

3 Brain-Computer-Interfaces

Als Brain-Computer-Interfaces (kurz BCI) bezeichnet man in der Neurotechnik ein System, welches aus einem gemessenen Biosignal einer Person abstrakte Aussagen (in Echtzeit oder einmalig) über den momentanen kognitiven Zustand dieser Person treffen kann. Brain-Computer-Interfaces wurden ursprünglich entwickelt, um Menschen mit Behinderung eine alternative Möglichkeit zu bieten, mit einer Maschine auch ohne Nutzung des peripheren Nervensystems zu kommunizieren. Allgemein lassen sich Brain-Computer-Interfaces in drei Kategorien aufteilen [Kot12]:

1. **Aktive Brain-Computer-Interfaces**: leiten ihre Ausgabe direkt von einem bewussten (Kontroll-)Gedanken des Benutzers ab, unabhängig von externen Einflüssen.

2. **Reaktive-Brain-Computer-Interfaces**: leiten ihre Ausgabe von der externen Stimulation des Benutzers auf ein Ereignis ab (z.B. ein Farbflimmern).

3. **Passive Brain-Computer-Interfaces**: erfassen jegliche Hirnaktivität, ohne dass sich der Benutzer auf etwas fokussieren muss und fügen diese Information einer Anwendung hinzu. Es ist hierbei möglich, viele passive BCIs parallel zu betreiben, da der Benutzer nicht aktiv oder reaktiv eine Anwendung oder Maschine steuert.

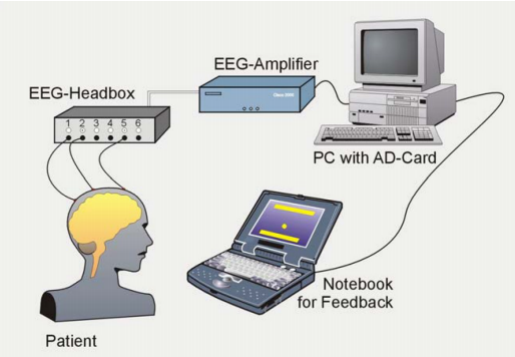

Abbildung 3.1: Traditioneller Aufbau eines BCI-Experiments [Kot12]

Um Rückschlüsse auf die momentane Hirnaktivität zu schließen, wird meistens die elektrische Aktivität im Gehirn mittels nichtinvasiver Elektroden (Elektroenzephalografie) aufgezeichnet. Es besteht aber auch die Möglichkeit, die hämodynamische Aktivität des Gehirns mittels Magnetresonanztomographie oder Nahinfrarotspektroskopie zu messen. Die erfassten Signale werden digitalisiert und mittels Mustererkennung von Computern analysiert und anschließend in Steuersignale oder Informationen umgewandelt. [Wol12]

3.1 Elektroenzephalografie

Die Elektroenzephalografie wurde 1924 von dem Psychiater und Neurologen Hans Berger an der Universität Jena entwickelt und 1929 publiziert[Ber91]. Elektroenzephalografie wird zur Diagnose von z.B. Epilepsie, Hirntod, Koma- und Narkosetiefe, aber auch in der Schlafmedizin eingesetzt. Die Signale entstehen durch Potentialschwankungen in der Großhirnrinde (*lat. Cortex cerebri*). Die Nervenzellen des Gehirns produzieren durch ihre elektrischen Zustandsänderungen zur Informationsverarbeitung sogenannte Aktionspotenziale. Da viele der sehr großen Nervenzellen senkrecht zur Oberfläche ausgerichtet sind, verstärken sich die elektrischen Felder und lassen sich somit an der Kopfoberfläche in Größenordnungen von 5 bis 100 μV messen [HP]. Elektroenzephalografie ist die inzwischen standardmäßige Untersuchungsmethode in der Neurologie, wobei sich in klinischen Untersuchungen Elektroenzephalografie-Geräte mit mindestens 15 Ableitungspunkten [ZH11] etabliert haben. Die Elektroenzephalografie zeichnet sich im Vergleich zu anderen Untersuchungsmethoden der Neurologie, zum Beispiel der Magnetresonanztomographie, durch eine sehr hohe zeitliche Auflösung aus. Die Ortsauflösung hingegen liegt üblicherweise im Bereich von mehreren Zentimetern.

3.1.1 Gehirnwellen

In seiner Arbeit [Ber91] publizierte Berger erstmals die Entdeckung von elektrischen Hirnaktivitäten, die rhythmischer Aktivität gleichen. So entdeckte Berger beispielsweise, dass bei einem gesunden erwachsenen Menschen im entspannten Zustand ein bestimmter Rhythmus mit einer Frequenz von 8–13 Hz vorliegt und die Signalamplitude über den okzipitalen Hirnregionen am größten ist. Berger bezeichnete diese Entdeckung als α-Rhythmus und nummerierte folgende Entdeckungen entsprechend durch.

Über die entsprechenden Wellen lassen sich sehr wage Rückschlüsse auf den kognitiven Zustand des erwachsenen Probanden schließen. Bei Kleinkindern und Säuglingen verhalten sich die Gehirnwellen teilweise anders. Ein erhöhter Anteil an α-Wellen wird mit einem entspannten Wachzustand bei geschlossenen Augen assoziiert. Die Signalamplitude ist dabei über

Bezeichnung	Frequenzbereich in Hz
δ-Wellen	0,1 bis unter 4
θ-Wellen	4 bis unter 8
α-Wellen	8 bis 13
β-Wellen	über 13 bis 30
γ-Wellen	über 30

Tabelle 3.1: Gehirnwellen und ihre Frequenzbereiche [Psc90, S. 418]

den okzipitalen Hirnregionen am größten. Berger entdeckte außerdem, dass α-Wellen beim Öffnen der Augen blockiert und durch β-Wellen ersetzt werden. In der Neurologie spricht man vom sogenannten Berger-Effekt. Das Auftreten von β-Wellen kann unterschiedlichste Ursachen haben, von aktiver kognitiver Aktivität bis zu Muskelanspannungen. γ-Wellen entstehen vermehrt bei starker Konzentration und Lernprozessen. δ-Wellen sind charakteristisch für die traumlosen Tiefschlafphase, während θ-Wellen üblicherweise bei Schläfrigkeit und leichten Schlafphasen vermehrt auftreten.
Teilweise werden die Frequenzbereiche noch weiter aufgeteilt. So wird zum Beispiel teilweise zwischen hohem und tiefem Alpha unterschieden. Im klinischen Umfeld gibt es noch weitere Wellenmuster, welche zum Beispiel charakteristisch für verschiedene Formen der Epilepsie sind. Diese Wellenformen spielen im Bereich von Brain-Computer-Interfaces aber eine sehr untergeordnete Rolle. Die klinische Auswertung erfolgt in der Regel durch einen geschulten Neurologen. Bei Brain-Computer-Interfaces kommen Software-Algorithmen zur Mustererkennung zum Einsatz.

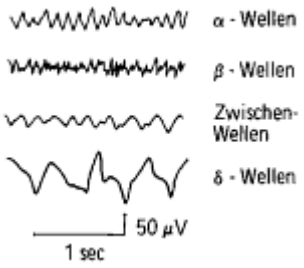

Abbildung 3.2: Grafische Darstellung einiger charakteristischer Wellen [Psc90]

3.2 Artefakte

Bei seinen frühen Experimenten bemerkte Hans Berger, dass gelegentlich fremde Ströme in den Aufnahmekreis gelangten und so seine Ableitung verfälschten. Man spricht hier von sogenannten Artefakten. Dies können zum einen technische Ströme wie das sogenannte *Netzbrummen* bei 50 Herz sein. Allerdings treten auch häufig sogenannte Muskelartefakte auf. Berger schätzt hier den Schläfenmuskel (lat. Musculus temporalis) als besonders gefährlich ein, da viele Probanden die Angewohnheit haben, die Zähne aufeinander zu beißen [Ber91, S.183]. Ferner sind aber noch der Stirnmuskel (lat. Musculus frontalis) sowie die Nacken- und Augenmuskulatur als potentielles Muskelartefakt zu nennen. Im Bereich der Brain-Computer-Interfaces kommen zur Unterdrückung von Artefakten Filter in Form von digitalen Signalprozessoren (DSP) zum Einsatz. Im klinischen Umfeld [Wel11] hat sich folgendes Filterverfahren etabliert:

1. Lowpass-Filter im Bereich von 60 Herz zur Filterung von Muskelartefakten
2. Notch-Filter im Bereich von 50 Herz zur Filterung der Netzspannung
3. Bandstop-Filter im Bereich von 1 bis 3 Herz zur Filterung der Bewegungsartefakte

3.3 Auswertung

Die Auswertung von EEG-Daten erfolgt über sogenannte ereigniskorrelierte Potentiale, die betrachtet werden, nachdem der Proband eine Aufgabe (zum Beispiel Rechenaufgabe oder Bilderkennung) gelöst hat. Der Grundrhythmus an zum Beispiel α- und β-Wellen wird dabei als Hintergrundaktivität (Rauschen) betrachtet. Zur Analyse der spezifischen Hirnaktivität bei einer Aufgabe (zum Beispiel Bilderkennung) ist die Hintergrundaktivität jedoch so stark, dass keine Auswertung möglich ist. Die Aufgabe wird daher mehrfach wiederholt und die aufgezeichneten Ergebnisse werden gemittelt. Daraus lässt sich dann eine charakteristische Abfolge von positiven und negativen Ausschlägen bei bestimmten Vorgängen betrachten. Mit dieser Methode lassen sich präzisere Aussagen über Vorgänge im Gehirn treffen, besonders über zeitliche Abfolgen, da die hohe zeitliche Präzision ein Vorteil der Elektroenzephalografie im Vergleich zu anderen Methoden ist. [HP]

3.4 10-20 System

In den Jahren nach der Pionierarbeit von Hans Berger im Bereich der Elektroenzephalografie [Ber91] hat es verschiedene Vorschläge zur Positionierung und Benennung der Ableitungselektroden gegeben. Angesichts der Tatsache, dass aber Schädelform und -größe von Mensch zu

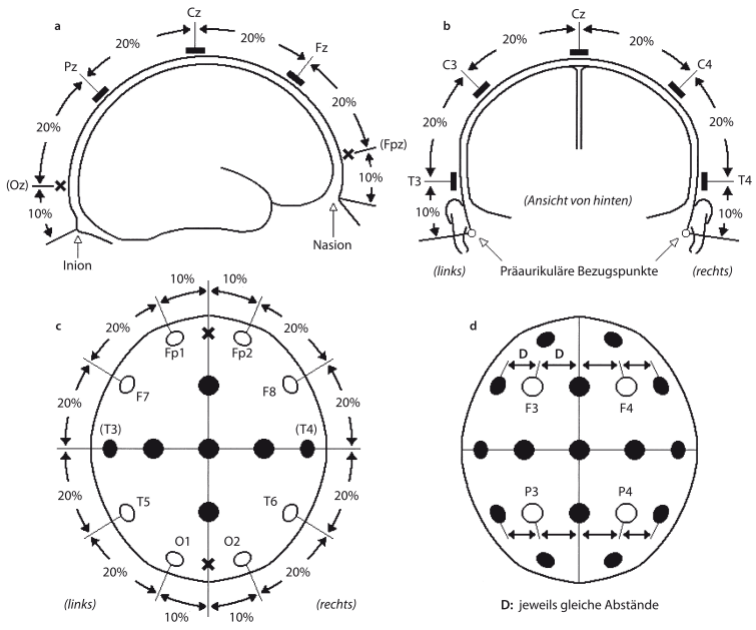

Abbildung 3.3: Festlegung und Abstände der Messpunkte des 10-20 Systems [ZH11]

Mensch unterschiedlich sind, musste für vergleichbare Ergebnisse ein relatives System definiert werden. Eine heute allgemeingültige Methode ist das sogenannte 10-20 System von H.H. Jasper aus dem Jahre 1957 [ZH11], welches 19 Ableitungspunkte definiert, die mit relativen Abständen positioniert werden. Der Schädel wird dabei vom Ansatz des Nasenbeins (Nasion) über den Schädelknochen bis zum Hinterkopf (Inion) vermessen. Diese Strecke repräsentiert fortan einen Wert von 100 Prozent. Danach teilt man die Strecke in Zehner- bzw. Zwanzigerschritte prozentual von Nasion in Richtung Inion auf, wodurch sich der Name des Systems herleitet. Ebenso wird auf einer Linie zwischen den beiden Ohren verfahren. Die daraus resultierenden Koordinaten ergeben die Positionen für die Ableitungselektroden. Je nach Position der jeweiligen Ableitungselektrode in Bezug auf die Hirnlappen wird ein Buchstabe verwendet. Die rechte und linke Gehirnhälfte werden mit geraden bzw. ungeraden Zahlen identifiziert.

3.5 Neurofeedback

Mit Neurofeedback bezeichnet man eine spezielle Form des Biofeedbacks. Hierbei werden Elektroenzephalografie-Signale von einem Computer aufgezeichnet und in Echtzeit ausgewertet. Das EEG-Signal wird dabei in die einzelnen Frequenzteile zerlegt und anschließend der

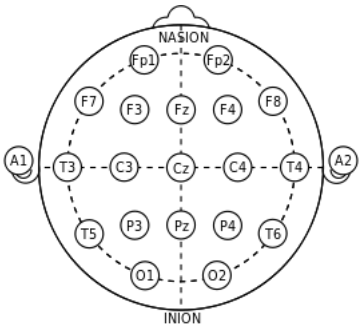

Abbildung 3.4: Bezeichnung der Messpunkte des 10-20 Systems [CNWJ13]

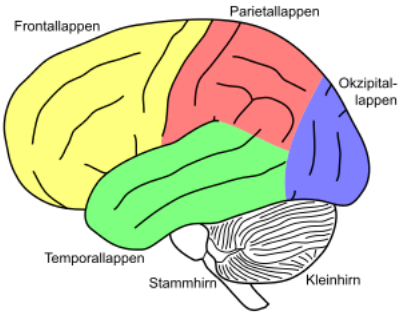

Abbildung 3.5: Einteilung des Großhirns in Hirnlappen

kognitive Zustand (zum Beispiel wach, entspannt, gestresst, schläfrig) des Probanden abgeleitet. Durch eine akustische und/oder visuelle Rückmeldung des Hirnmusters an den Probanden soll es somit möglich sein, Entspannungs- oder Konzentrationstechniken effektiv zu trainieren. Im Jahre 1967 veröffentlichte M. Barry Sterman eine Studie, in der er beschreibt Katzen mittels Neurofeedback so trainiert zu haben, dass diese immun gegen epileptische Anfälle seien, welche bei untrainierten Katzen mittels Monomethylhydrazin-Dämpfen ausgelöst wurden. 1974 führte Sterman aus, dass sich Epilepsie durch Neurofeedbacktraining auch beim Menschen unter Kontrolle bringen lasse[SE06].
Neurofeedbacktraining wird heute auch zur Behandlung diverser Krankheiten, wie zum Beispiel Aufmerksamkeitsdefizit-/Hyperaktivitätsstörung (ADHS), Autismus, Epilepsie und Schlaganfällen oder zum Training zur Stressbewältigung und bzw. -reduktion eingesetzt. Da die Behandlung praktisch keine Nebenwirkungen hat, bedarf eine Therapie mit Neurofeedback keine medizinische Ausbildung seitens des Therapeuten. Neurofeedback ist im wissenschaftlichen Umfeld

Buchstabe	Bezeichnung
C	central
F	frontal (Frontlappen)
O	occipital (Okzipitallappen)
P	parietal (Parietallappen)
T	temporal (Temporallappen)

Tabelle 3.2: Bedeutung der Abkürzungen im 10-20-System

umstritten und ist in abgewandelter Form auch im esoterischen und parawissenschaftlichen Umfeld zu finden.

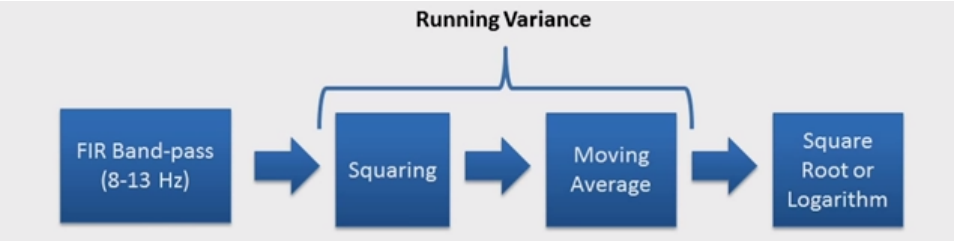

Abbildung 3.6: Implementierung eines Neurofeedbacks für α-Wellen [Kot12]

3.6 Werkzeuge

Inzwischen existieren einige umfangreiche Softwarewerkzeuge zur Analyse und Auswertung von BCI-Signalen. EEGLAB [DM04] ist eine Erweiterung für MATLAB, die zum Beispiel Funktionen zur Artefakt-Filterungen, Zeit-Frequenz-Analyse und visuellen Darstellung der Signale liefert. EEGLAB legt seinen Fokus eher auf klinische Untersuchungen und ist daher eher auf die Arbeit mit mehreren Kanälen ausgelegt. Ein weiteres nennenswertes Werkzeug ist OpenViBE [RLG+10], mit dem sich mittels grafischer Programmierung - im sogenannten Designer - diverse Experimente (in OpenViBE Szenarien genannt) erstellen, durchführen und anschließend analysieren lassen. Beide Softwarewerkzeuge sind unter Open-Source-Lizenzen erhältlich.

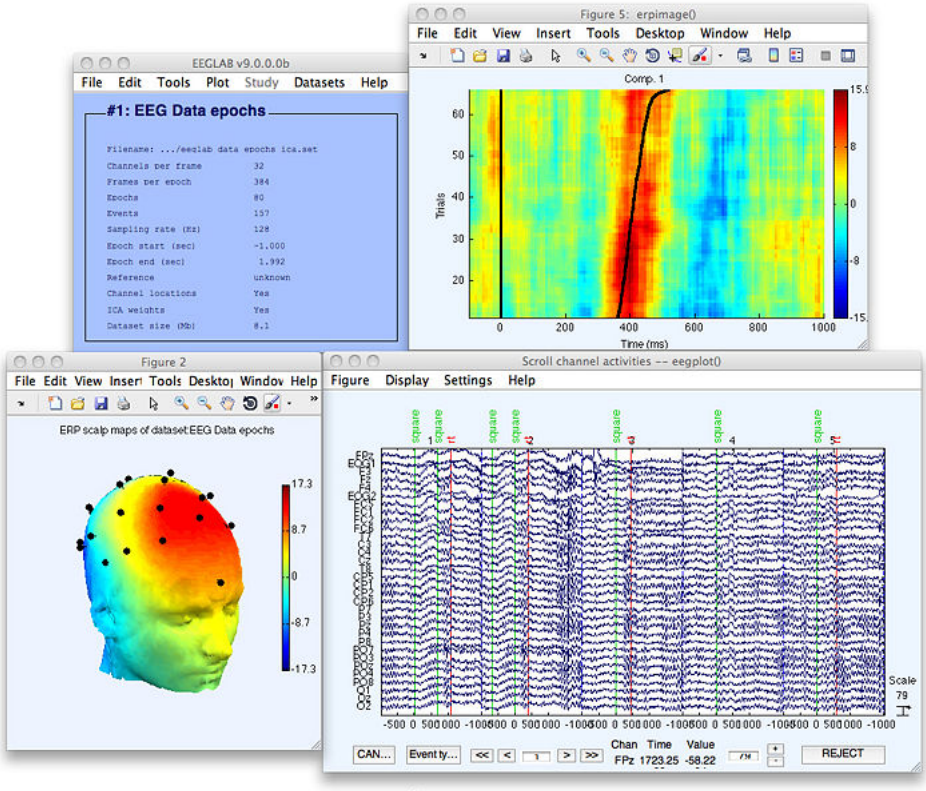

Abbildung 3.7: Screenshot von EEGLAB [DM04]

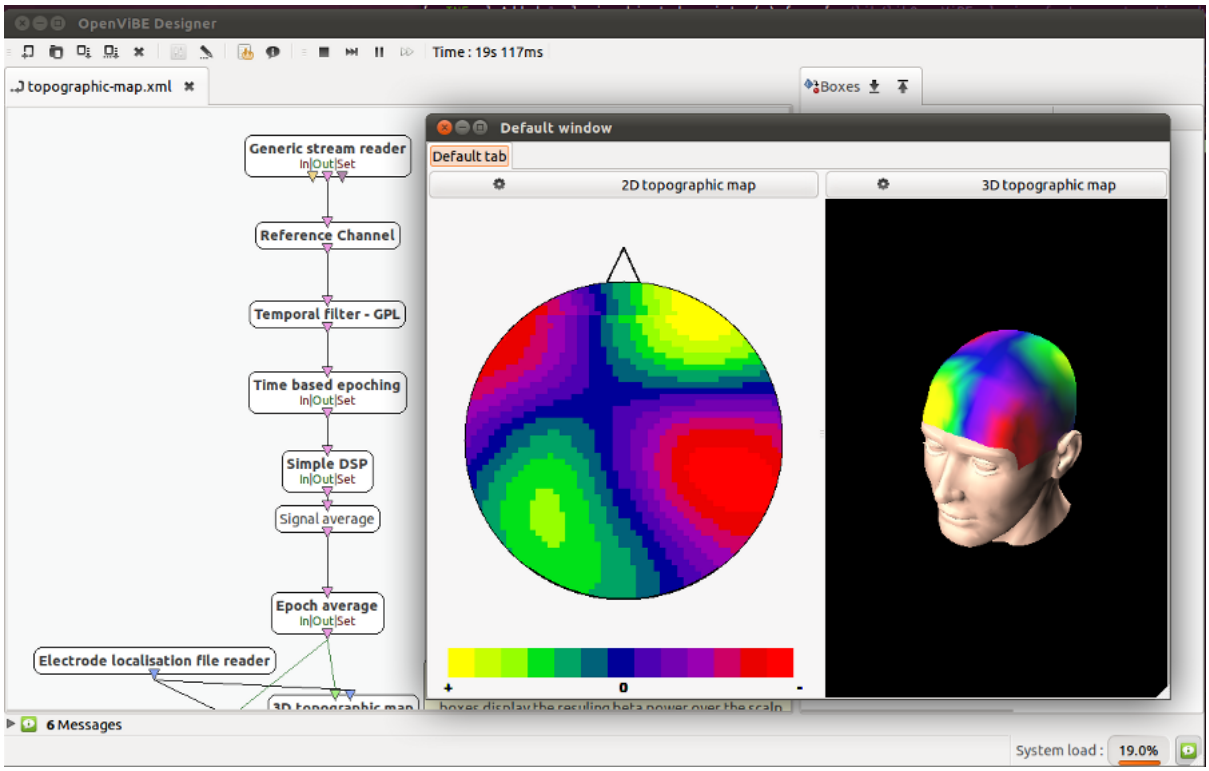

Abbildung 3.8: Screenshot von OpenViBE [RLG+10]

4 Neurosky Mindwave Mobile

Mindwave ist eine Produktserie der Firma Neurosky für passive Brain-Computer-Interfaces, welche im Jahr 2010 in China und 2011 in den USA und der EU vorgestellt wurde. Mit einem Preis um einhundert Euro bedient Neurosky mit der Mindwave-Serie primär den Bildungs- und Unterhaltungsbereich. Das Mindwave Mobile unterscheidet sich von der herkömmlichen Mindwave-Serie primär durch die Datenübertragung per Bluetooth, um so auch mobile Geräte wie Smartphones und Tablets bedienen zu können. Es ist der offizielle Nachfolger des Neurosky Mindwave Headsets. Neurosky bietet zusätzlich ein Software-Development-Kit für die Plattformen Windows, Mac OS X, iOS und Android an, mit dem Programme oder Apps entwickelt werden können.

Abbildung 4.1: Neurosky MindWave Mobile [Neu12]

4.1 Spezifikation

Das BCI besteht aus einem Plastikgestell mit einem einstellbaren Bügel am Kopf sowie einem justierbaren Sensorarm mit einer Elektrode für den frontalen temporalen Punkt *Fp1* des 10-20 Systems. Unten am BCI befindet sich ein Ohrclip für die Referenzspannung. Das Neurosky Mindwave Mobile bietet laut Hersteller [Neu12] folgende Spezifikation:

- Bluetooth v2.1 Class 2
- UART(Serial): VCC, GNC, TX, RX
- UART Baudrate: 57,600 Baud
- Zugriff auf aufbereitete (d.h. gefilterte) EEG Daten (Alpha, Beta, etc.)
- Zugriff auf aufbereitete (d.h. gefilterte) eSense [Neu12, S.12 ff.] Daten für Aufmerksamkeit und Meditation
- Zugriff auf EEG Rohdaten
- Zugriff auf EEG/ECG Signalstärke

Der Hersteller macht leider keine Angaben über die eingesetzen Filterverfahren oder die Berechnung der eSense Werte.

4.2 ThinkGear Connector

Die Firma Neurosky stellt mit der Software *ThinkGear Connector* eine Software bereit, welche im Hintergrund als Serverprozess die Kommunikation mit dem Headset abstrahiert. Dabei wartet der Prozess auf TCP Port 13854 auf eingehende Verbindungen und erlaubt es so weiteren Anwendungen nach erfolgreicher Verbindung Informationen des BCIs zu beziehen. Dieser Vorgang ist für alle ThinkGear-kompatiblen Geräte des Herstellers identisch und auf Grund der TCP-Verbindung auf Clientseite sowohl plattform- als auch programmiersprachenunabhängig. Der ThinkGear Connector und die Clientanwendung kommunizieren über das ThinkGear Socket Protocol.[Neu14a]

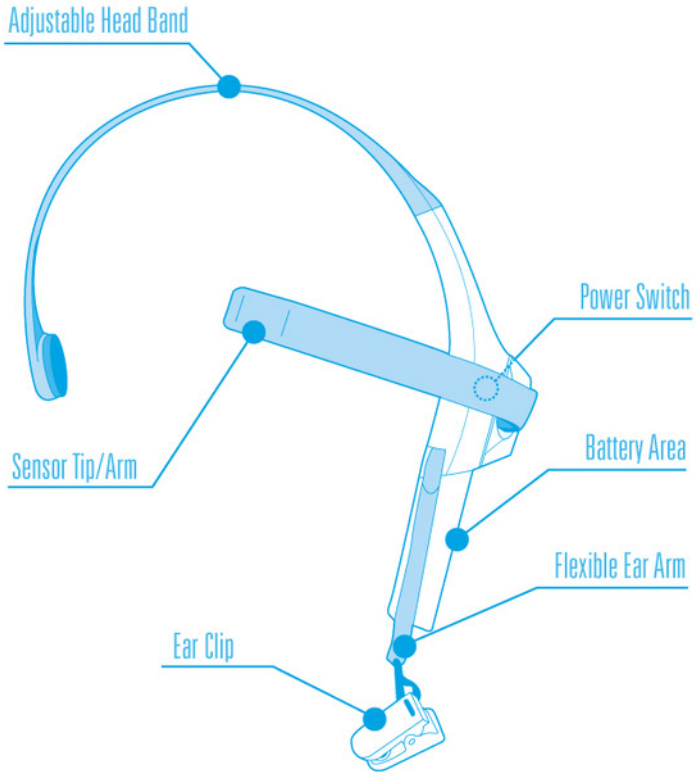

Abbildung 4.2: Neurosky MindWave Mobile Einheiten [Neu12]

4.3 ThinkGear Socket Protocol

Das ThinkGear Socket Protocol (TGSP) ist ein JSON-basiertes[1] Protokoll zur Steuerung der ThingGear Software und zur Übertragung von Daten des Brain-Computer-Interfaces zwischen Client und Server. Das Protokoll wurde so designt, dass es auch Programmiersprachen oder Frameworks ohne API für serielle Schnittstellen (z.B. Adobe Flash[2]) ermöglicht, Zugriff auf die Daten des ThinkGear-kompatiblen BCIs zu erhalten. Zum Lesen der Daten des BCIs müssen von der Software folgende Schritte durchlaufen werden:

1. Herstellen der Socket-Verbindung
2. Anmeldung am ThinkGear Server

[1] http://www.json.org/ abgerufen am 11.09.2014
[2] https://www.adobe.com/products/flashruntimes.html abgerufen am 11.09.2014

3. Konfiguration des Servers
4. Lesen der Daten
5. Beenden der Socket-Verbindung

Nachdem die Socket-Verbindung hergestellt wurde, erfolgt laut Dokumentation [Neu14b] eine Anmeldung der Clientsoftware am ThinkGear Server. Dazu übersendet die Clientsoftware ihren Namen im Klartext und als SHA1-Hashwert im JSON Format an den ThinkGear Server.

```
{
"appName":"SkyScraper",
"appKey":"6eb718a1c06e88e2e1290a2bb7d7dd6d8afa7528"
}
```

Obwohl diese Anmeldung laut Dokumentation zwingend erforderlich ist um Daten zu erhalten, ist im Rahmen dieser Arbeit keine Anmeldung notwendig gewesen. Auch in Codebeispielen des Herstellers [Neu14a] wird darauf verzichtet. Anschließend wird der ThinkGear Server konfiguriert. Dabei steht zur Auswahl, ob Rohdaten mit übertragen werden sollen oder nicht und ob der Server die Daten im JSON Format oder binär übertragen soll.

```
{"enableRawOutput":true,"format":"Json"}
```

Neuere Versionen des ThinkGear Servers erlauben eine ereignisgesteuerte Aufnahme der Daten (z.B. durch Tastendruck). Hierbei kann dem Kommando `startRecording` eine Konfiguration mit übergeben werden.

```
{
"startRecording":
{
"rawEeg":true,
"poorSignalLevel":true,
"eSense":true,
"eegPower":true,
"blinkStrength":true
},
"applicationName":"SkyScraper"
}
```

Analog dazu kann die Aufname der Daten mit dem Kommando `stopRecording` wieder beendet werden. Während die Aufnahme aktiv ist, sendet der ThinkGear Server ein JSON-Array als Antwort mit den angeforderten Werten.

4.4 Protokoll-Parameter

Nachfolgend eine Übersicht einiger Protokoll-Parameter

- **poorSignalLevel**: gibt die Qualität des Gehirnwellensignals an. Dies ist ein Integer im Bereich von 0 bis 200, wobei 0 für ein sehr gutes Signal und 200 für einen Verbindungsabbruch steht.
- **eSense**: Container für die eSense Werte attention und meditation im Wertebereich von 0 bis 100
- **eegPower**: Container für die einzelnen Frequenzbereiche (delta, theta, tiefes Alpha, hohes Alpha, tiefes Beta, hohes Beta, tiefes Gamma, hohes Gamma
- **rawEeg**: Rohdaten des Sensors entweder als Integer oder Float
- **rawEegMulti**: Bei Headsets mit mehreren Kanälen beinhaltet dieser Container die einzelnen Werte der Kanäle.
- **blinkStrength**: Integerwert zwischen 0 bis 255, welcher die Stärke eines erkannten Augenzwinkerns repräsentiert

4.5 SkyScraper

Die Open-Source Software *SkyScraper* wurde von Jornack Hupkens[1] entwickelt. Sie basiert auf Software von Eric Blue[2] und kombiniert die Funktionalitäten der Software *Mindstream* und *brain_grapher*. Die Java-Software bietet die Möglichkeit, Daten eines ThinkGear-kompatiblen BCIs abzuspeichern und gleichzeitig in einer grafischen Benutzeroberfläche anzuzeigen. Die aufgezeichneten Daten können anschließend in ein CSV (Comma-separated values) oder in ein Microsoft-Excel Format konvertiert werden.
SkyScraper arbeitete leider nur mit den aufbereiteten EEG-Daten. Im Rahmen dieser Arbeit wurde eine Abspaltung[3] der Software erstellt, welche folgende Änderungen beinhaltet:

1. Auslesen der rohen EEG-Signale
2. Export der rohen EEG-Signale in CSV Dateien

[1] https://github.com/Jornack abgerufen am 11.09.2014
[2] http://eric-blue.com/ abgerufen am 11.09.2014
[3] https://github.com/xenobyte/SkyScraper abgerufen am 11.09.2014

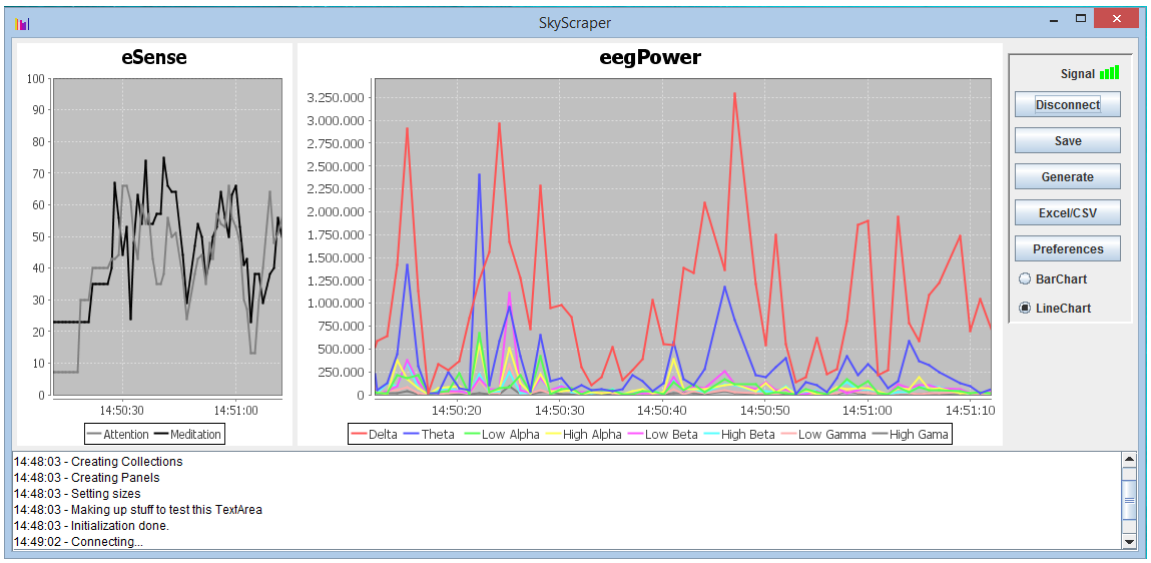

Abbildung 4.3: Screenshot der Software SkyScraper

3. Optimierungen für Java 8

4. Diverse Fehlerkorrekturen

Neurosky vertreibt mit den *Research Tools* eine vergleichbare Software zu einem Preis von rund 500 US-Dollar.

5 EEG-Signale zur Authentifikation

5.1 Vorüberlegungen

In den letzten Jahren wurde die Idee Gehirnwellen zur Benutzer-Authentifikation heranzuziehen immer beliebter. Diverse wissenschaftliche Studien [CNWJ13] [ABTV11] [MM07] haben untersucht, ob sich aus EEG-Signalen eindeutige charakteristische Merkmale über Benutzer extrahieren lassen. Gehirnwellen als biometrische Authentifikationsmethode bieten einige Vorteile. Die Methode wäre nahezu immun gegen Wörterbuch-Attacken, und auch ein heimliches Hinsehen während der Passworteingabe, sogenanntes *shoulder-surfing*, wäre ausgeschlossen. Ein weiterer nicht zu verachtender Vorteil im Vergleich zu anderen biometrischen Authentifikationsmethoden ist die Tatsache, dass man seine Gehirnwellen (im Vergleich zu Fingerabdrücken) nicht überall hinterlässt.

Das Neurosky Mindwave Mobile bietet im Vergleich zu anderen Mehrkanal-BCIs den Vorteil, dass die Elektrode nicht mit Natriumchlorid angefeuchtet werden muss, bevor das BCI einsatzbereit ist. Außerdem bietet die Position der Ableitungselektrode (*Fp1* im 10-20 System) den Vorteil, dass eine Abnahme direkt auf der Kopfhaut stattfinden kann und das Signal nicht durch Haare gemindert wird.
Die Anforderung der Universalität als biometrisches Merkmal (siehe Kapitel 2.4) ist bei EEG-Signalen gegeben, da jeder lebendige Mensch Gehirnwellen erzeugt. Die Eindeutigkeit des Merkmals ist zu prüfen und steht daher noch aus. Die Beständigkeit des Merkmals liegt nur bedingt vor. Erkrankungen wie zum Beispiel Aufmerksamkeitsdefizit-/Hyperaktivitätsstörung (ADHS), Epilepsie, Schlaganfälle oder Gehirntumore haben Auswirkungen auf die Elektroenzephalografie. Außerdem liegt es in der Natur der Elektroenzephalografie, dass bei gleicher Tätigkeit nicht die gleichen Wellen produziert werden. Das Merkmal müsste also über viele Messungen gemittelt werden. Die Anforderung der quantitativen Erfassbarkeit hingegen wird uneingeschränkt erfüllt und ist mittels Elektroenzephalografie ohne weiteres durchführbar. Die Anforderung der Performanz setzt ein der Aufgabe entsprechenden Elektroenzephalografen voraus. Hans Berger beschrieb in seiner Arbeit [Ber91] eine hohe Akzeptanz seiner Patienten

zur Elektroenzephalografie. Sofern der Benutzer nicht aufwändig präpariert werden muss, sollte die Anforderung der Akzeptanz erfüllt sein. Die Anforderung der Fälschungssicherheit ist gegeben, da sich Gehirnwellen nicht ohne erheblichen Aufwand duplizieren lassen, allerdings auch nicht von dem Benutzer selbst. In der Theorie erfüllen Gehirnwellen also mit Einschränkungen die Anforderungen an ein biometrisches Merkmal. Der renomierte Berliner Gehirnforscher John-Dylan Haynes hält eine Authentifikation über Gehirnwellen für denkbar. [HP]

5.2 Vorangegangene Studien

Betrachtet man die bereits durchgeführten Studien zu diesem Thema, so fällt eine Studie der University of California in Berkeley besonders heraus. Die Forschungsergebnisse wurden auf der *17th International Conference on Financial Cryptography and Data Security* in Okinawa (Japan) präsentiert und in einem Paper [CNWJ13] veröffentlicht. Den Forschern gelang es mit einem Brain-Computer-Interface der Firma Neurosky eine Erfolgsquote von 99% bei der Benutzeridentifikation zu erzielen. Verglichen mit anderen Studien [ABTV11] [MM07] erscheint die Mustererkennung der University of California in Berkeley am vielversprechendsten und wurde daher in dieser Arbeit als Referenzstudie herangezogen.

5.3 Experimente

Wie auch in der Referenzstudie [CNWJ13] wurden im Rahmen dieser Arbeit 15 Probanden (Studenten vor dem ersten akademischen Grad oder Akademiker) mit einem Neurosky Mindwave Mobile präpariert. Jeder Proband wurde in zwei 30-50-minütigen Sitzungen, die an unterschiedlichen Tagen stattgefunden haben, aufgefordert fünfmal hintereinander die unten aufgeführten Experimente durchzuführen. Während der Experimente, wurden die EEG-Signale vom Brain-Computer-Interface ermittelt und via Bluetooth an einen Computer übertragen. Mit der Software SkyScraper wurden die Daten aufgezeichnet und die BCI-Signale überwacht.

1. **Atem-Aufgabe**: Der Proband schließt seine Augen und konzentriert sich 10 Sekunden lang auf seine Atmung.

2. **Simulierte Fingerbewerbung**: Der Proband stellt sich 10 Sekunden lang vor, er würde seinen rechten Zeigefinger synchron zu seinem Atem bewegen, ohne dass der Finger dabei wirklich bewegt wird.

3. **Sport-Aufgabe**: Der Proband wählt eine Bewegung einer von ihm gewählten Sportart und stellt sich 10 Sekunden lang vor, er würde diese Bewegung ausführen.
4. **Lied-Zitieraufgabe**: Der Proband stellt sich 10 Sekunden lang vor, er würde ein Lied singen, ohne dabei einen Laut von sich zu geben.
5. **Augen-und-Audioton-Aufgabe**: Der Proband schließt seine Augen und hört 5 Sekunden lang einen Audioton. Anschließend öffnet er die Augen und starrt für weitere 10 Sekunden auf einen Punkt, welcher auf einem Blatt Papier vor ihm liegt.
6. **Objekt-Zählaufgabe**: Dem Proband wird eine Tabelle mit 5x6 Kästchen, bestehend aus den Farben Rot, Grün, Blau und Gelb gezeigt. Für insgesamt 30 Sekunden wird dem Probanden alle 5 Sekunden eine neue Tabelle vorgelegt. Seine Aufgabe besteht darin, die Kästchen mit der von ihm gewählten Farbe zu zählen.
7. **Passthought-Aufgabe**: Der Proband wird gebeten sich ein Passthought zu überlegen. Ein Passthought ist wie ein Passwort, nur dass im Vergleich zu einer bestimmten Kombination an Zahlen und Buchstaben hier ein bestimmter Gedanke gewählt wird. Die Aufzeichnung erfolgt 10 Sekunden lang.

Mit 15 Probanden und zwei Sitzungen mit jeweils fünf Durchgängen der sieben Experimente wurden so insgesamt 1050 Datensätze gesammelt.

5.4 Fragebogen

Nach jeder Sitzung wurde den Probanden, wie auch in der Referenzstudie, ein Fragebogen vorgelegt, in dem diese eine der sieben Aufgaben auswählen sollten, mit der sie am ehesten ihre tägliche Authentifikation durchführen würden. Nach der zweiten Sitzung wurden die Probanden aufgefordert, die Aufgaben mit den binären Möglichkeiten

- einfach oder schwierig
- langweilig oder unterhaltsam

zu bewerten.

Aufgabe	war schwierig	war langweilig	tägliche Aufgabe
Atem	0/15	5/15	7/30
Fingerbewerbung	3/15	9/15	0/30
Sport	8/15	8/15	0/30
Lied	3/15	8/15	5/30
Audio	3/15	2/15	5/30
Farbobjekte	1/15	4/15	4/30
Passthought	3/15	4/15	9/30

Tabelle 5.1: Auswertung des Fragebogens

5.5 Auswertung

Bei der Auswertung des Fragebogens zeigten sich keine nennenswerte Abweichungen bezüglich der Akzeptanz der Aufgaben bei den Probanden. Die Ergebnisse werden in der nachfolgenden Tabelle aufgeführt.

5.5.1 Reproduzierbarkeit

Im Gegensatz zur Referenzstudie [CNWJ13, S.14, Tabelle 6] konnten sich viele meiner Probanden in der zweiten Sitzung nicht mehr an ihre Auswahl bei der Sport-, Lied-, Passthought-Aufgabe sowie der Objekt Zählaufgabe aus der ersten Sitzung erinnern.

5.6 Auswertungsalgorithmen

Im Entstehungsprozess dieser Bachelorarbeit stellte sich heraus, dass sich die Datenverarbeitungsalgorithmen der Referenzstudie nicht komplett nachimplementieren ließen, da einige Details zu wage formuliert oder schlichtweg nicht erläutert wurden. Anfragen an die Autoren der Studie nach den Quellcodes der Auswertungssoftware blieben unbeantwortet. Ebenso blieben Anfragen des technischen Journalisten Richard Adhikari[1] an die Autoren bzgl. eines Kommentars über die Ergebnisse unbeantwortet.
Nachfolgend werden also die nachvollziehbaren Arbeitsschritte der Studie erläutert.

5.6.1 Datenverarbeitung

Die von der Studie aufgezeichneten Datensätze wurden für die Datenanalyse zuerst aufbereitet, indem jeweils die mittleren fünf Sekunden aus den gesamten 10 Sekunden extrahiert wurden.

[1] http://www.technewsworld.com/story/77762.html abgerufen am 11.09.2014

Eine Ausnahme bildet hier die Objekt-Zählaufgabe, hier wurden 5 Sekunden extrahiert, also die Dauer für die Betrachtung eines spezifischen Bildes. Anschließend wurden aus dem rohen EEG-Signal nur die α-Wellen (8 - 12 Hz) sowie die β-Wellen (12 - 30 Hz) extrahiert und separat gespeichert. Üblich sind hier FIR Bandpass Filter auf den jeweiligen Frequenzbereich [Kot12].

Anschließend wurde mittels eines Kompressionsalgorithmus aus dem zweidimensionalen Signal ein eindimensionales Signal erzeugt. Dabei reduziert der Kompressionsalgorithmus das Signal in der Zeitdimension. Für jede einzelne Frequenzkomponente wurde ein Median über die dazugehörige Frequenzkomponente der gesamten Zeit ermittelt. Wie dies im Detail funktioniert und wie die Frequenzbereiche hier genau aufgeteilt sind, lassen die Autoren offen. Das Ergebnis des Kompressionsalgorithmus ist ein eindimensionaler Spaltenvektor mit einem Eintrag für jede gemessene Frequenz. In diesem Spaltenvektor werden fortan die Messdaten gespeichert und vom Authentifikationssystem bearbeitet.

5.6.2 Datenanalyse

Nachdem die Datensätze gesammelt und verarbeitet wurden, müssen die Signale der einzelnen Probanden voneinander unterschieden werden. Dabei ermitteln die Forscher der Referenzstudie die Ähnlichkeit zweier Signale u und v des Vektors mittels Kosinus-Ähnlichkeit.

$$similarity(u, v) = \frac{\sum_{i=1}^{n} u_i \cdot v_i}{\sqrt{\sum_{i=1}^{n} (u_i)^2} \cdot \sqrt{\sum_{i=1}^{n} (v_i)^2}} = \frac{u \cdot v}{\|u\| \, \|v\|} \tag{5.1}$$

Die Funktion liefert einen Wert zwischen 0 und 1, wobei eine Ähnlichkeit von 1 eine perfekte Übereinstimmung repräsentiert.
Die Forscher definieren zwei Werte: die sogenannte *self-similarity*, welche die Ähnlichkeit des Signals bei ein und demselben Probanden beschreibt sowie die *cross-similarity*, die die Ähnlichkeit der Signale unterschiedlicher Probanden definiert. Die Forscher nehmen an, dass die *self-similarity* immer größer sein sollte als die *cross-similarity*. Dies gelte für alle Probanden in allen Aufgaben.

Für eine gegebene Aufgabe t und einen gegebenen Probanden s definiert sich die *self-similarity* von s in t über den Mittelwert einer Ähnlichkeit aller nur möglichen Datensätze des Probanden s.
Ebenso definiert sich die *cross-similarity* von s in t über die Ähnlichkeit für jedes nur mögliche Paar, wovon ein Datensatz zu dem Probanden s gehört und der andere Datensatz nicht.

Anschließend ermittelten die Forscher für jeden Probanden die *self-* und *cross-similarity* für jede Aufgabe und errechneten daraus einen Mittelwert. Diese Werte sind in der Tabelle 1 des Papers [CNWJ13, S.9] aufgeführt, ebenso deren relative Differenz in Prozent. Es fällt auf, dass die *self-similarity* größer ist als die *cross-similarity*. Dies ist eine wichtige Grundannahme für das Authentifikationssystem. Weiter fällt auf, dass eine Differenz in der prozentualen Abweichung unter den 15 Probanden existiert. Die Forscher nutzen dies nach eigener Aussage, um das Protokoll zu verbessern. Tabelle 2 [CNWJ13, S.9] zeigt eine alternative Darstellung der Ergebnisse. Für eine definierte Aufgabe errechneten die Forscher für jeden Probanden die *self-* und *cross-similarity* und ermittelten dann den Mittelwert über alle Probanden. Die Ergebnisse weisen mehr Ähnlichkeiten der Aufgaben untereinander auf als unter den Probanden. Außerdem ist in jedem Fall die *self-similarity* wieder größer als die *cross-similarity*.

5.6.3 Authentifikation

Um die Performanz ihres Authentifikationsprotokoll zu ermitteln, definieren die Forscher die *Half Total Error Rate* (kurz HTER) wie folgt:

$$HTER = \frac{FAR + FRR}{2} \tag{5.2}$$

In Testverfahren selektierten die Forscher fünf Datensätze zufällig, von jeder Aufgabe und jedem Probanden, und trainierten damit das Authentifikationsprotokoll. Die verbleibenden Datensätze wurden genutzt, um das Protokoll zu testen.

In ihrem *Common Task Common Threshold protocol* korrespondieren alle Datensätze mit einer fest definierten Aufgabe. Die Forscher wählten einen allgemeinen Grenzwert T für alle Probanden. Der eigentliche Authentifikationsmechanismus arbeitet dabei wie folgt: Als Eingabe lieferte man dem Protokoll eine Identität und einen Datensatz von EEG-Signalen. Daraus ermittelten die Forscher die *self-similarity* als gemittelte Ähnlichkeit zwischen den abgespeicherten fünf Datensätzen des Probanden. Danach wurden zufällig fünf Datensätze ausgewählt, die nicht zu dem Probanden gehörten, mit denen dann die *cross-similarity* als Mittelwert errechnet wurde. War der prozentuale Unterschied zwischen *self-similarity* und *cross-similarity* größer oder gleich T ist, wurde der Proband akzeptiert. Andernfalls wurde der Benutzer abgewiesen. Tabelle 3 [CNWJ13, S.11] zeigt die Ergebnisse des *Common Task Common Threshold* Protokolls. Die beste Performanz lieferte hier die *Augen-und-Audioton-Aufgabe* mit einer *HTER* von 32%. Die *FAR* war bei jeder Aufgabe niedriger als die *FRR*.

Die Forscher verbesserten daraufhin ihr Protokoll mit angepassten Grenzwerten in ihrem *Customized Threshold* Protokoll. Es arbeitet ähnlich wie das vorher beschriebene *Common Task Common Threshold* Prokotoll, mit dem Unterschied, dass sie anstelle eines allgemeinen Grenzwertes T nun einen speziell angepassten Grenzwert T_i für den Probanden i verwenden. Die genaue Bereichnung dieser angepassten Grenzwerte geht aus der Studie nicht hervor. Die Ergebnisse werden in Tabelle 4 dargestellt [CNWJ13, S.11]. In fast allen Fällen gelang es den Forschern mit den angepassten Grenzwerten eine deutlich höhere Performanz zu erzielen.

Als weitere Steigerung entwickelten die Forscher das *Customized Task Customized Threshold* Protokoll, bei dem sie für jeden Probanden die optimale Aufgabe ermitteln, um so den prozentualen Unterschied zwischen *self-similarity* und *cross-similarity* zu maximieren. Das Ergebnis protokollierten die Forscher in der letzten Zeile von Tabelle 4 [CNWJ13, S.11]. Mit dieser Modifikation erreichten sie eine *HTER* von 1,1%. Dies bestärkte die Forscher in ihrer Annahme, dass es keine bestimme Aufgabe gäbe, welche sich für die Authentification am besten eigne.

5.7 Benutzeridentifikation

Um nun einen Benutzer anhand eines eingegebenen EEG-Signals zu identifizieren, bedienten sich die Forscher künstlicher Intelligenz und einiger Klassifizierungsmethoden. Sie wählten eine Signatur als Testdatensatz aus, bei der sie sich auf Alpha- und Beta-Wellen beschränkten sowie einen Mittelwert über den mittleren Abschnitt der Zeit bildeten. Mittels eines angepassten Nächste-Nachbarn-Klassifikationsverfahrens ließen die Forscher eine Signatur untersuchen und notierten, ob der Algorithmus richtig oder falsch lag. Abbildung 3 [CNWJ13, S.13] zeigt die Erfolgsquote für K = 5.
Mit dieser Methode erreichten die Forscher eine Erfolgsquote von 22%.

5.8 Diskussion

Wie bereits beschrieben stellte sich im Entstehungsprozess dieser Arbeit heraus, dass sich die Referenzstudie nicht komplett reimplementieren ließ. So wird der Kompressionsalgorithmus z.B. nur wage beschrieben oder die angepassten Grenzwerte werden gar nicht erläutert. Ein Vergleich der gesammelten Messwerte war somit nicht möglich. Der Benutzeridentifikation mit Hilfe des Nächste-Nachbarn-Klassifikationsverfahrens wurde angesichts der geringen Erfolgsquote keine weitere Beachtung geschenkt.

5.8.1 Die eingesetzte Hardware

Das Neurosky Mindwave Mobile ist primär für den Unterhaltungsmarkt ausgelegt und im Vergleich zu klinischen Elektroenzephalografen oder anderen Brain-Computer-Interfaces eher minderwertig. Es war während der Sitzungen mit Probanden nahezu unmöglich ein Signal mit konstanter Qualität aufzuzeichnen. Häufig musste die Position der Elektrode variiert werden. Anders als in den Vorüberlegungen angenommen stellte sich heraus, dass das Neurosky Mindwave Mobile sehr wohl zwischen den Sitzungen gewartet werden muss, da die Elektrode durch z.B. Körperfett oder Hautcremes verschmutzt und so die Signalqualität vermindert wird. Die Ableitungselektrode sowie der Ohrclip für die Referenzspannung wurden vor und nach jeder Sitzung mit Mecetroniumetilsulfat gereinigt.

Auch der Bluetooth-Pairing-Prozess über eine feste PIN beim Neurosky Mindwave Mobile ist für sicherheitsrelevante Anwendungen eher ungeeignet. Ein Angreifer könnte unter Umständen die übertragenen Signale abhören [SW05].

5.8.2 Platzierung der Elektrode

Laut Beschreibung liest das Neurosky Mindwave Mobile die EEG-Signale von dem Messpunkt *Fp1* ab. Da sich aber Schädelform und -größe von Mensch zu Mensch unterscheiden, wäre hier trotzdem eine Abmessung des Kopfes notwendig. Aus der Referenzstudie geht nicht hervor, ob eine solche Abmessung nach dem 10-20 System bei jedem Probanden stattgefunden hat. Dies bleibt aber zu bezweifeln, da die Position der Ableitungselektrode in meinen Experimenten teilweise im Zentimeterbereich verändert werden musste, um eine bessere Signalqualität zu erzielen.

Der Abnahmepunkt *Fp1* ist ohnehin für die einzelnen Aufgaben der Referenzstudie nicht unbedenklich, da hier viele Muskelartefakte durch Gesichts- oder Augenmuskulatur auftreten. Ganz im Gegensatz zum Unterhaltungsbereich, wo häufig eine sog. *blink detection* Anwendung findet, um Augenzwinkern zu erkennen ist die Position der Ableitungselektrode für diese Experimente eher ungünstig. Speziell für die α-Wellen wäre hier eine Ableitungselektrode an den okzipitalen Hirnregionen besser geeignet.

5.8.3 Die eingesetzte Analysetechnik

Die Forscher der Referenzstudie nutzten ausschließlich die Amplitudenkorrelation als Basis ihrer Analysetechnik. Dies ist im Vergleich zu allgemeinen üblichen Verfahren wie Zeit-

Frequenz-Analysen mit anschließendem Vergleich von Aktivitätsclustern im 2D-Raum eher unkonventionell [ZH11]. Um auch die Ähnlichkeit zweier Signale bei unterschiedlichen Zeitverschiebungen zu ermitteln, wäre die Kreuzkorrelation anstelle der Kosinus-Ähnlichkeit ein geeigneteres Mittel gewesen.

5.8.4 Aussagekraft der Ergebnisse

Im Abstract [CNWJ13, S.1] werben die Forscher mit einer erzielten Genauigkeit von 99%. Dies bezieht sich aber nur auf den Vergleich der statischen Datensätze mit dem von den Forschern entworfenen Protokoll. Bei der eigentlichen Benutzeridentifikation liegen die Forscher mit einer Erfolgsquote von 22% zwar dreifach über der Quote, die man mit zufälligem Raten erzielen würde. Für wirklich praktische Anwendung ist dieses Ergebnis allerdings unbrauchbar. Selbst die Genauigkeit von 99% ist für EEG-Signale zwar außergewöhnlich, im Vergleich zu etablierten biometrischen Merkmalen wie Fingerabdruck- oder Retinascannern aber nicht erwähnenswert. Diese Erfolgsquote stützt sich allerdings auf zwei Annahmen:

1. Es existiert kein Proband (oder Benutzer), den das System nicht kennt.
2. Das System geht nur von gutwilligen Versuchspersonen aus.

Angenommen, es existiere eine Menge von Menschen A von denen das System nur 1% kennt: Authentifiziert man nun eine Person mit der Passthought Aufgabe B ($HTER = 0.011$), so liegt die Wahrscheinlichkeit, dass die erfolgreich authentifizierte Person tatsächlich dem System bekannt ist nach dem Satz von Bayes [BP63] bei 50%.

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)} = \frac{0.99 \cdot 0.01}{(0.99 \cdot 0.01) + (0.01 \cdot 0.99)} = 0.5 \tag{5.3}$$

Dieses Ergebnis ist mit den Ergebnissen anderer Studien [ABTV11] [MM07] vergleichbar.

5.8.5 Eigene Messungen

Die in dieser Arbeit erfassten Messdaten der Probanden wurden zur Analyse folgenden Berechnungen unterzogen. Für jeden Probanden wurden aus den Rohdaten aller 35 Datensätze einer Sitzung jeweils die α-Wellen und β-Wellen extrahiert. Dazu wurden die mittleren 5 Sekunden der Rohdaten ausgewählt und darauf ein FIR Bandpassfilter für den jeweiligen Frequenzbereich angewendet. Anschließend wurde der Median über α und β des Datensatzes gebildet und abgespeichert. Die gespeicherten Medianwerte aller Datensätze wurden dann auf Ähnlichkeit

untersucht. Für die Berechnung der *self-similarity* wurden jeweils die Datensätze der ersten und zweiten Sitzung eines Probanden miteinander kreuzkorreliert. Die *cross-similarity* wurde durch Kreuzkorrelation der Daten einer Sitzung eines Probanden mit den entsprechenden Daten eines anderen Probanden errechnet. Im Gegensatz zur Referenzstudie sind sich die Signale eines jeweiligen Probanden selbst nicht konstant ähnlicher als die Signale mit anderen Probanden. Bei den nachfolgenden Diagrammen stehen Ausschläge in Y-Achse für eine Zeitverschiebung des Signals. Hier ein Auszug der Ergebnisse.

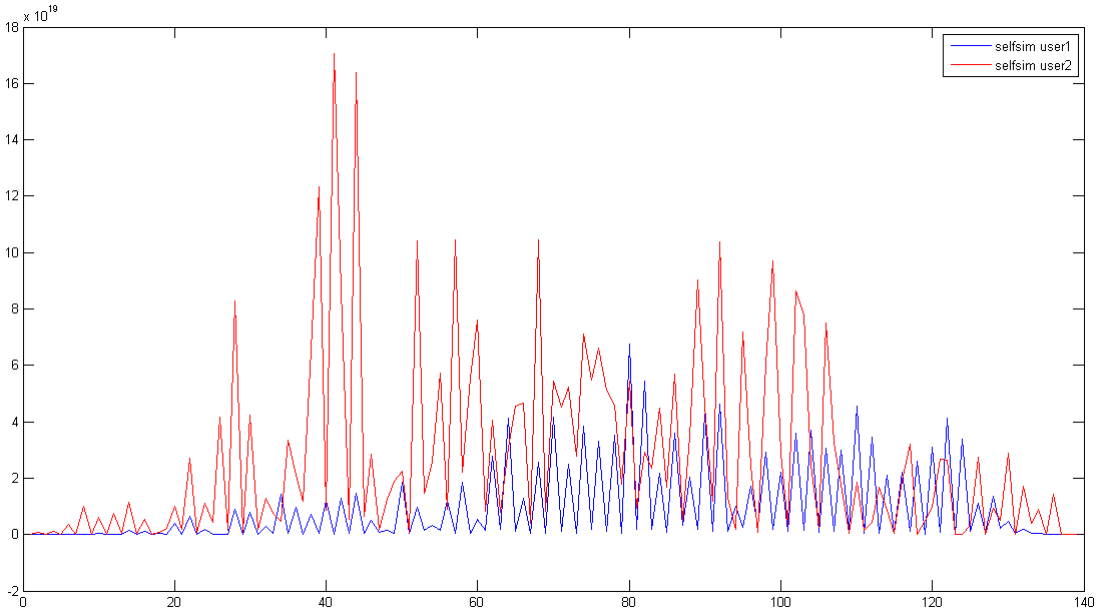

Abbildung 5.1: *self-similarity* von zwei Probanden

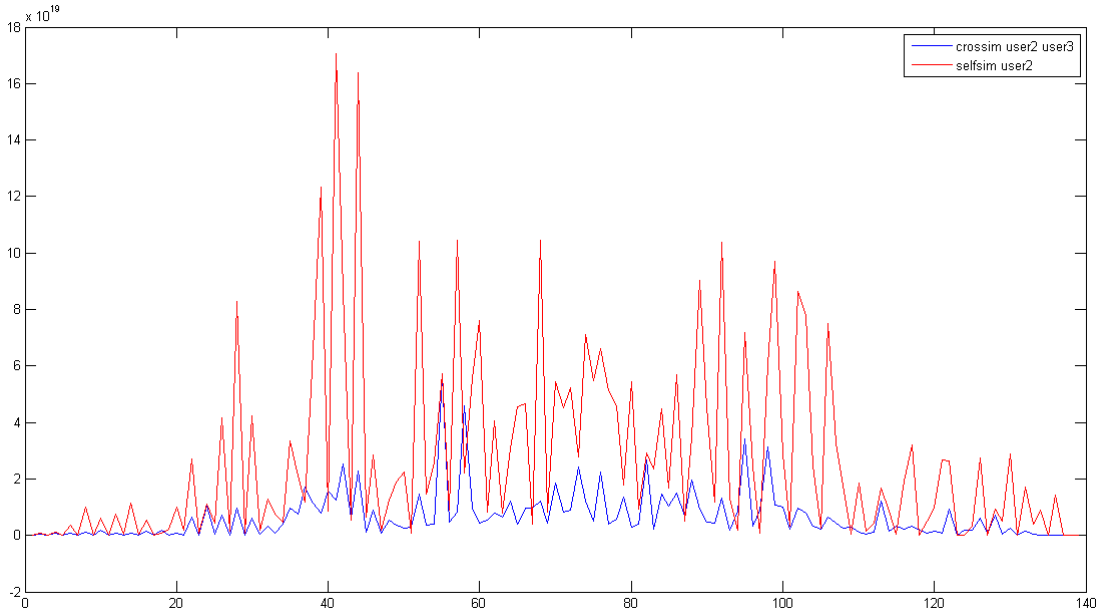

Abbildung 5.2: Vergleich von *cross-similarity* und *self-similarity* zweier Probanden

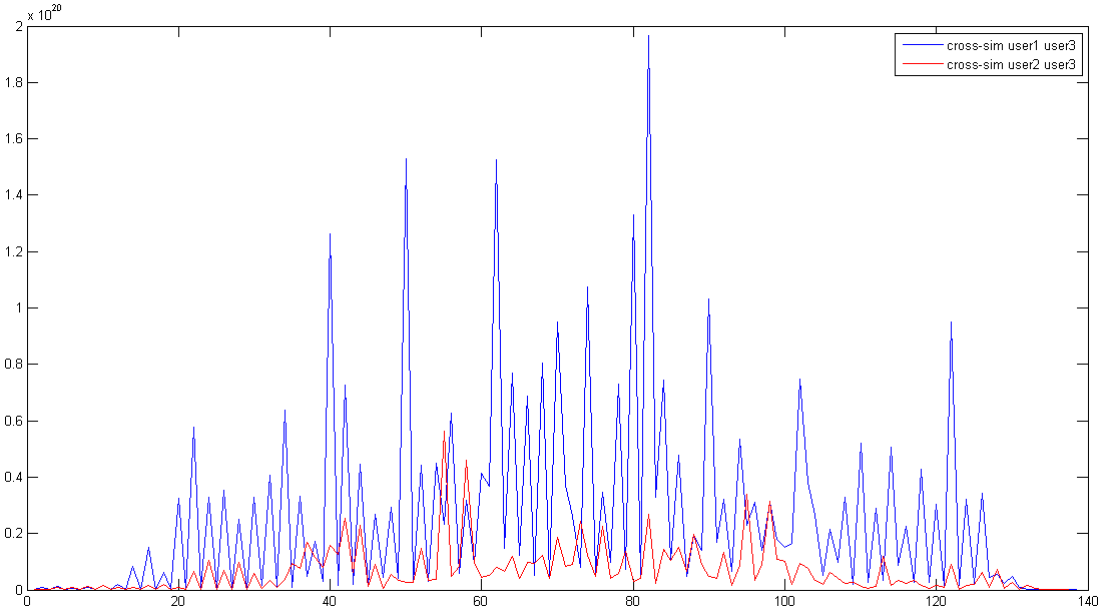

Abbildung 5.3: Vergleich zweier *cross-similarity* Werte

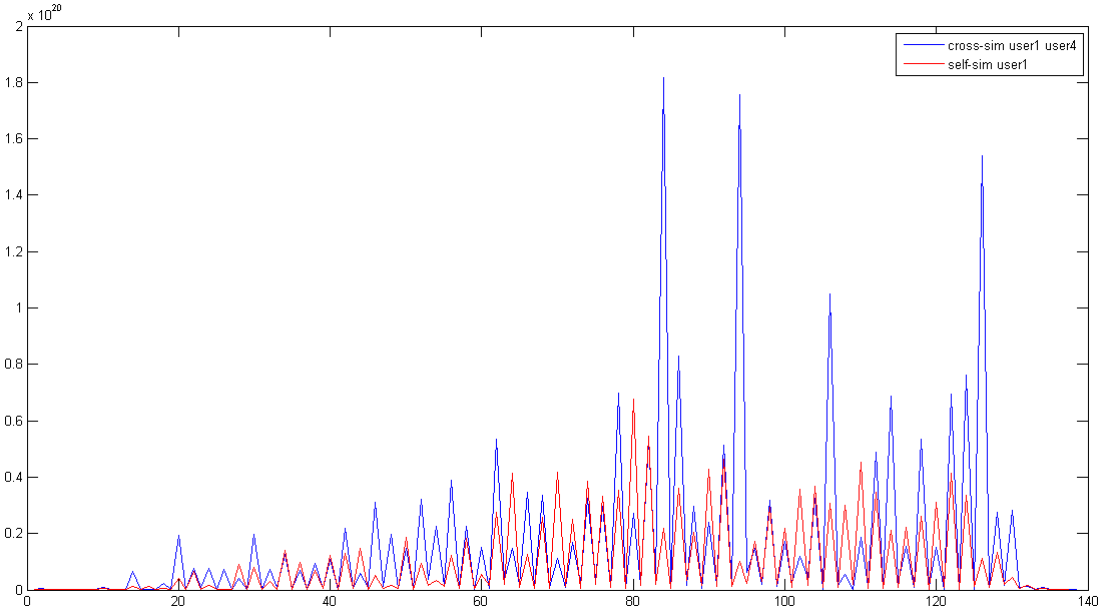

Abbildung 5.4: Weiterer Vergleich von *cross-similarity* und *self-similarity*

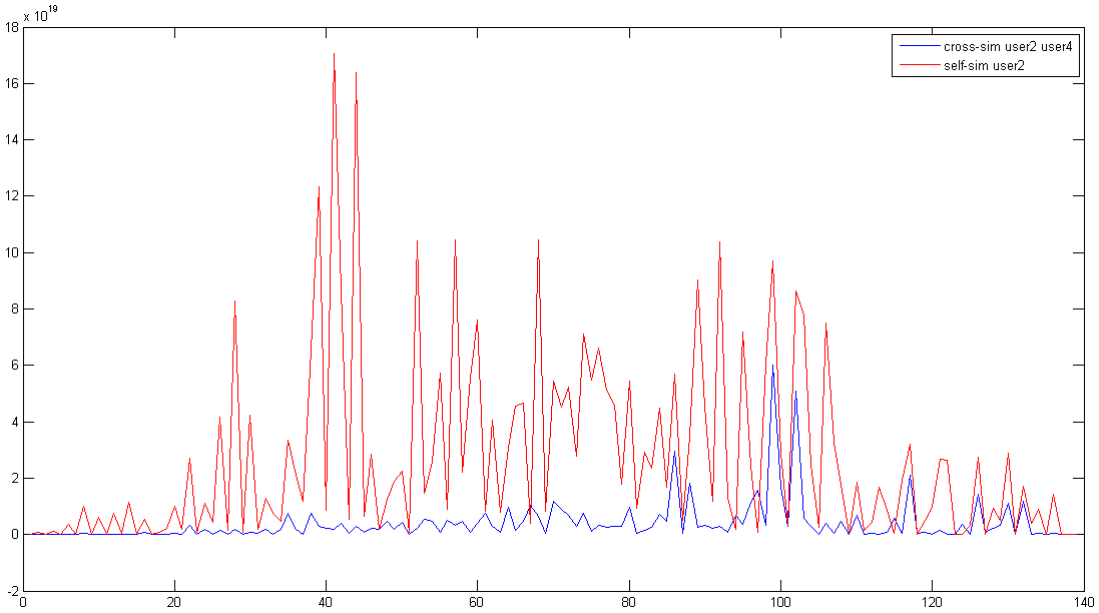

Abbildung 5.5: Vergleich von *cross-similarity* und *self-similarity* mit anderen Probanden

6 Zusammenfassung und Ausblick

Abschließend werden die Ergebnisse dieser Arbeit zusammengefasst. Zudem werden einige Ansätze für mögliche, auf diesen Ergebnissen aufbauende Arbeiten erläutert.

6.1 Fazit

Im Rahmen dieser Arbeit wurde die Eignung von Elektroenzephalografiedaten eines Brain-Computer-Interfaces zur computergestützten Authentifizierung anhand einer Referenzstudie überprüft. Hierzu wurde eine Open-Source Software so angepasst, dass mit dem Neurosky Mindwave Mobile Rohdaten aufgezeichnet werden können. Mit dieser Software wurden in Experimenten EEG-Signale von Probanden aufgezeichnet. Auch wenn einige der Anforderungen an ein biometrisches Merkmal von Gehirnwellen erfüllt werden, kann diese Methode aktuell als ungeeignet betrachtet werden. Wie sich in Experimenten herausstellte, ist die höhere Benutzerfreundlichkeit eines Ein-Kanal BCIs im Vergleich zu Mehr-Kanal BCIs nur teilweise gegeben. Die Signalqualität ist bei dem Neurosky Mindwave Mobile sehr wechselhaft und die Ableitungselektrode muss regelmäßig gereinigt werden. Die Ableitungselektrode sehr präzise positioniert werden, was sich negativ auf die Benutzerfreundlichkeit auswirkt. Weiterhin ist der Bluetooth-Pairing-Prozess des BCIs nicht für sicherheitsrelevante Szenarien ausgelegt. Die Position der Ableitungselektrode auf dem Messpunkt $Fp1$ ist bei einer reinen Betrachtung der α- und β-Wellen ist ungünstig, da hier viele Störsignale der Gesichts- und Augenmuskulatur aufgenommen werden und die Signalamplitude der α-Wellen über den okzipitalen Hirnregionen am größten ist.

Die Ergebnisse der Referenzstudie sind bei genauerer Analyse nicht nachvollziehbar und unterscheiden sich je nach Blickweise nicht wesentlich von anderen Studien.
Ein sicherer Beleg für eine eindeutige Charakteristik von Elektroenzephalografiedaten verschiedener Probanden konnte nicht nachgewiesen. Die von den Forschern angenommene Charakteristik der aufgezeichneten Signale könnte aus der wahrscheinlich willkürlichen Positionierung der Ableitungselektrode resultieren.

6.2 Ausblick

Im Verlauf dieser Arbeit ergab sich eine Reihe von Ideen, welche aufbauend auf diese Arbeit umgesetzt werden könnten.

6.2.1 Optimierungen an SkyScraper

Die Software SkyScraper könnte mit einigen Erweiterungen verbessert werden.

Anpassung der grafischen Benutzeroberfläche

Die grafische Darstellung der EEG-Signale ist eher unüblich und teilweise unübersichtlich. Wünschenswert wäre hier eine separate Darstellung für die eSense-Signale sowie jeweils für die aufbereiteten und rohen EEG-Signale im positiven und negativen Bereich ähnlich der folgenden Abbildung:

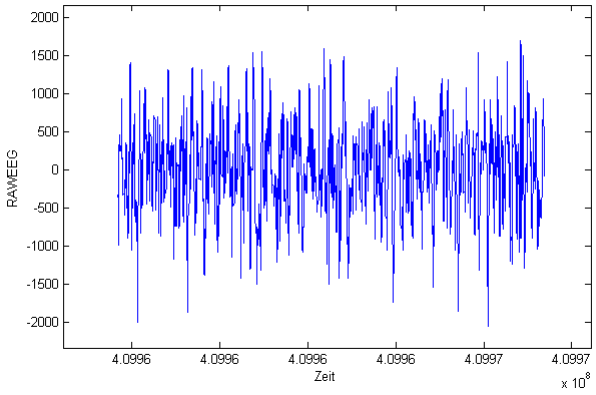

Abbildung 6.1: Plot von rohen EEG-Daten

Für die Zeit-Frequenz-Analysen wäre eine Darstellung als Spektrogramm wünschenswert ohne Vorher die Daten in MATLAB verarbeiten zu müssen.

Datenimport und -export

In Sachen Benutzerfreundlichkeit wäre es nützlich wenn sich mehrere Datensätze auf einmal als CSV-Datei exportieren lassen. Bei vielen Datensätzen ist die derzeitige Lösung sehr zeitaufwändig. Weiterhin wäre es wünschenswert, sich aus importierten EEG-Daten ein ent-

sprechendes Diagramm generieren zu können. Diese Funktionalität ist teilweise vorhanden, funktioniert allerdings nicht fehlerfrei.

JUnit-Testfälle

Die die Software existieren derzeit keinerlei Testfälle. Um zu verifizieren, dass mit nachfolgenden Erweiterungen keine schwerwiegenden Fehler in die Software Einzug erhalten, wären JUnit-Tests eine mögliche Option.

6.2.2 Weitere Untersuchungen der gesammelten Probandendaten

Die in dieser Bachelorarbeit aufgezeichneten EEG-Signale können für weitere Experimente verwendet werden. Ein Beispiel wäre, die hier aufgeführten Experimente mit einem anderen BCI durchzuführen und die Ergebnisse hinterher zu vergleichen.

Fouriertransformation als Analysetechnik

Da die Phasensynchronisation im Gehirn eine maßgebliche Rolle spielt, könnte wahrscheinlich mittels Fouriertransformation und anschließender Kosinus-Ähnlichkeits-Berechnung noch eine Menge an zusätzlichen Details ermittelt werden.

6.2.3 Reverse Engineering der eSense Werte

Die Berechnung der eSense-Werte von Neurosky ist nicht öffentlich dokumentiert. Es sollte jedoch möglich sein, die aufgezeichneten und aufbereiteten EEG-Signale der einzelnen Frequenzbereiche zu speichern und die dabei auftretende Änderung der entsprechenden eSense-Signale zu analysieren. Unter Umständen lassen sich noch weitere eSense-Werte errechnen.

6.2.4 Vergleich unterschiedlicher Messpunkte

Eine interessante Fragestellung wäre weiterhin, ob sich EEG-Signale innerhalb des Gehirns mehr unterscheiden als Signale aus unterschiedlichen Hirnen. Weiterhin könnte man untersuchen, ob es in den Signallaufzeiten der einzelnen Hirnbereiche charakteristische Unterschiede gibt.

Literaturverzeichnis

[ABTV11] Ashby, Corey ; Bhatia, Amit ; Tenore, F ; Vogelstein, J: Low-cost electroencephalogram (EEG) based authentication. In: *Neural Engineering (NER), 2011 5th International IEEE/EMBS Conference on* IEEE, 2011, S. 442–445

[Ber91] Berger, Hans: *Das Elektrenkephalogramm des Menschen*. Frankfurt am Main : pmi-Verl, 1991. – ISBN 978–3891191842

[Bir99] Biran, A: *Matlab 5 für Ingenieure . Systematische und praktische Einführung*. Addison-Wesley, 1999. – ISBN 382731416X

[BP63] Bayes, Mr. ; Price, Mr: An Essay towards solving a Problem in the Doctrine of Chances. By the late Rev. Mr. Bayes, FRS communicated by Mr. Price, in a letter to John Canton, AMFRS. In: *Philosophical Transactions (1683-1775)* (1763), S. 370–418

[CNWJ13] Chuang, John ; Nguyen, Hamilton ; Wang, Charles ; Johnson, Benjamin: I think, therefore i am: Usability and security of authentication using brainwaves. In: *Financial Cryptography and Data Security*. Springer, 2013, S. 1–16

[DM04] Delorme, Arnaud ; Makeig, Scott: EEGLAB: An Open Source Toolbox for Analysis of Single-Trial EEG Dynamics Including Independent Component Analysis. In: *Journal of Neuroscience Methods* 134 (2004), Nr. 1, S. 9–21

[Eck13] Eckert, Claudia: *IT-Sicherheit*. Oldenbourg Wissensch.Vlg, 2013. – ISBN 3486721380

[Har08] Hartenstein, Hannes: *Netzwerk-und IT-Sicherheitsmanagement: eine Einführung*. KIT Scientific Publishing, 2008. – ISBN 3866442092

[HMNS96] Haller, Neil ; Metz, Craig ; Nesser, Phil ; Straw, Mike: A one-time password system / RFC 1938, May. 1996. – Forschungsbericht

[HP] Haynes, John-Dylan ; Pritlove, Tim: *Chaosradio Express 195 - Das Gehirn*. http://meta.metaebene.me/media/cre/cre195-das-gehirn.transcript.txt. – Abgerufen am 13.04.2014

[KL14] Katz, Jonathan ; Lindell, Yehuda: *Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series)*. Chapman and Hall/CRC, 2014. – ISBN 1466570261

[Kot12] Kothe, Christian: *Introduction To Modern Brain-Computer Interface Design*. http://sccn.ucsd.edu/wiki/Introduction_To_Modern_Brain-Computer_Interface_Design. Version: 2012. – Abgerufen am 27.08.2014

[Lug01] Luger, George F.: *Künstliche Intelligenz - Strategien zur Lösung komplexer Probleme (4. Aufl.)*. Pearson Studium, 2001. – 1–892 S. – ISBN 978–3–8273–7002–0

[Mey06] Meyer, Martin: *Signalverarbeitung. Analoge und digitale Signale, Systeme und Filter*. Vieweg Verlag, 2006. – ISBN 3834802433

[MM07] Marcel, Sebastien ; Millán, José del R: Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. In: *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 29 (2007), Nr. 4, S. 743–752

[Neu12] Neurosky: *MindWave Mobile: User Guide*, Februar 2012. http://download.neurosky.com/support_page_files/MindWaveMobile/docs/mindwave_mobile_user_guide.pdf. – Abgerufen am 27.08.2014

[Neu14a] Neurosky: *ThinkGear Connector Development Guide*, Juni 2014. http://developer.neurosky.com/docs/doku.php?id=thinkgear_connector_development_guide. – Abgerufen am 27.08.2014

[Neu14b] Neurosky: *ThinkGear Socket Protocol*, Juni 2014. http://developer.neurosky.com/docs/doku.php?id=thinkgear_socket_protocol. – Abgerufen am 27.08.2014

[Psc90] Pschyrembel, Willibald: *Pschyrembel Klinisches Wörterbuch : mit klinischen Syndromen und Nomina anatomica*. Berlin u.a : De Gruyter, 1990. – ISBN 978–3110108811

[RLG+10] Renard, Yann ; Lotte, Fabien ; Gibert, Guillaume ; Congedo, Marco ; Maby, Emmanuel ; Delannoy, Vincent ; Bertrand, Olivier ; Lécuyer, Anatole: OpenViBE:

An Open-Source Software Platform to Design, Test, and Use Brain-Computer Interfaces in Real and Virtual Environments. In: *Presence* 19 (2010), Nr. 1, S. 35–53

[SE06] Sterman, M B. ; Egner, Tobias: Foundation and practice of neurofeedback for the treatment of epilepsy. In: *Applied psychophysiology and biofeedback* 31 (2006), Nr. 1, S. 21–35

[SW05] Shaked, Yaniv ; Wool, Avishai: Cracking the bluetooth pin. In: *Proceedings of the 3rd international conference on Mobile systems, applications, and services* ACM, 2005, S. 39–50

[Wel11] Wellach, Ingmar: *Praxisbuch EEG: Einführung in die Befundung, Beurteilung und Differenzialdiagnose*. Georg Thieme Verlag, 2011. – ISBN 978–3131539212

[Wol12] Wolpaw, Jonathan R.: Brain-computer interfaces: progress, problems, and possibilities. In: Luo, Gang (Hrsg.) ; Liu, Jiming (Hrsg.) ; Yang, Christopher C. (Hrsg.): *IHI*, ACM, 2012. – ISBN 978–1–4503–0781–9, S. 3–4

[ZH11] Zschocke, Stephan ; Hansen, Hans-Christian: *Klinische Elektroenzephalographie*. Springer Berlin Heidelberg New York Tokio, 2011. – ISBN 978–3642199424

Tabellenverzeichnis

Abbildungsverzeichnis

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 15. September 2014 Timo Briddigkeit