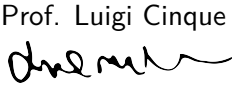
SAPIENZA
UNIVERSITÀ DI ROMA

EEG-Based Authentication: Unveiled Impostor Attack Analysis

Facoltà di Ingegneria dell'Informazione, Informatica e Statistica
Applied Computer Science and Artificial Intelligence

Riccardo De Sanctis
ID number 1937859

Advisor
Prof. Luigi Cinque



Co-Advisors
Prof. Daniele Pannone
Prof. Danilo Avola

Academic Year 2022/2023

EEG-Based Authentication: Unveiled Impostor Attack Analysis
Sapienza University of Rome

This thesis has been typeset by LaTeX and the Sapthesis class.

Author's email: desanctis.1937859@studenti.uniroma1.it

Contents

Chapter 1

Introduction

Safety of important assets has always been the primary goal of security. Identity authentication is not only the most crucial precaution but also the most critical task to resolve in order to guarantee protection. Authentication has become essential in numerous realms of everyday life, from public and national security to e-commerce and banking.
In recent years, rapid technological advancements, while simplifying data access for a wide range of users, have simultaneously giving rise to new threats and risks. New systems for the protection of valuable resources have been brought to the forefront of attention to counter increasingly growing challenges.
Biometric features based authentication methods, given their portability, have gained much popularity. Electroencephalography-based authentication has become one of the most appealing methods, gathering significant interest due to the successful application of deep learning models and solidifying its potential of deployment. Compared to other types of authentication systems, electroencephalography-based authentication can efficiently leverage multi-factor authentication required for secure system access, whilst accommodating additional security access conditions and ease of use.
Despite its vast opportunities, numerous challenges that hinder its practical deployment must still be addressed.

1.1 Scope and Purpose

Traditional biometric traits, relying on facial characteristics, fingerprints and voice characteristics, lack confidentiality and secrecy, making them susceptible to forgery by malicious agents. Due to the inherent individuality of electroencephalography signals, characterized by their resistance to remote theft, forgery and resilience to coercion, electroencephalography-based authentication has garnered significant attention as a promising solution to existing challenges associated with classical biometric factors.
The unique pattern of neural pathways, which constitutes the distinctive brain activity of an individual, can serve as a highly effective biometric authentication feature[2]. Imitating the brain activity of someone else is impossible due to the uniqueness and unfathomability of neural pathways [23]. Brain electrical activity

is ineffective under coercion from aggressors, since it is greatly influenced by stress [4]. Furthermore, in contrast with traditional biometric features, EEG ensures that the subject is alive. Signals recorded through electroencephalography, hereafter referred to as EEG, adhere to quality measures by exhibiting valuable traits such as universality, portability and performance. They are universal and highly portable since every human being produces EEG signals through their brain, ready to be collected. Performance is facilitated by the one-dimensionality of the signal, enabling easy capture and processing within a short computational time. Other desirable qualities, such as collectability (which is facilitated by the use of a small number of electrodes)[9][20], distinctiveness between subjects and permanence (which is the capability of recognizing the of same subject over over long time frames)[25], let EEG be a suitable biometric feature for authentication. The collection of brainwaves, however, might encounter challenges related to acceptance, as individuals may harbor concerns or feel threatened by narratives associated with 'mind reading' or 'mind control'.

EEG-based authentication methods are categorized as either spontaneous or evoked based on the presence or absence of stimuli that provoked the waves. The task selected to be performed by the users during the collection of brain signals contributes to deterrence of forgery by restricting the set of potentially exploitable user data to those produced exclusively within that specific situation and stimulation.
The framework for assessing the user's declared identity used in this work is grounded in a stimulus-response pattern. Stimuli are presented following a rapid serial visual presentation (RSVP) paradigm, which leverages the innate user knowledge factor and ensures ease of use. During the RSVP process, images are rapidly displayed at the same spatial location, usually a monitor screen, with multiple images presented per second. The stream of images within an RSVP paradigm consist of frequent non-target images and infrequent target images. The role of the target images is to elicit a unique response to that particular stimulus, measured as an event-related potentials (ERP). ERPs represent small signal amplitude variations in the ongoing EEG activity associated with the onset of a stimulus. Despite the rapid presentation of images, the brain is capable of assimilating the information contained therein and generating an unconscious response, free from potential dishonest intervention or alteration caused by rational thinking.
Images apt to be target stimuli are the ones of which content is well known to the user. In contrast, non-target stimuli consist of random and unfamiliar images. Notably, images depicting family members, friends, special places or objects possess the capability to evoke a distinctive ERP, making them particularly suitable as target stimuli. Non-target images may be chosen from the same domain as the target images or from any other random category, provided their content remains neutral and unbiased. Each user possesses a distinctive set of target images and will have a unique individual response to it [24][26], rendering the RSVP paradigm a fitting model for EEG-based authentication. The authentication system analyzes each user's reaction to the displayed image, and based on their EEG response, either grants or denies system access.

The robustness of the authentication system constitutes a critical security assumption

for ensuring any concrete deployment. In the realm of EEG-based authentication models, substantial progress has been made towards accurate detection of legitimate users and rejection of impostors. However most of them are only applicable within lab-controlled environments and case studies; their resistance to potential criminal attacks, data breaches, malicious exploits and fraudulent misuse has not been thoroughly investigated.
Illegitimate agents might gain access to images intended as target stimuli for a specific user, attempting to authenticate in by mimicking the user's response to the leaked stream of images. Additionally, attackers could directly steal the EEG-data stored in the system, gaining control and revealing personal and confidential information.

Two primary categories of attacks against the authentication system can be identified:

- Veiled attack: In this scenario, attackers possess limited knowledge of the target's basic information (e.g. name, age, gender). However, crucial information required for passing the security such as key, password, PINs or target images, is veiled or undisclosed.
- Unveiled attack: In this category, attackers have full knowledge of the information necessary to authenticate as the user.

This works aims to propose a model that is robust to unveiled attacks, ensuring data security and integrity, while also maintaining the ability to scale and generalize to new users.

1.2 Literature Review

Since the proposal of the first EEG-based authentication system by Poulos et al.[1] in 1999, numerous studies have explored authentication models relying on different tasks to stimulate EEG signal. These tasks include resting with closed or open eyes[1] [2][20], motor imagery[3][4][9], imagined speech[5], word generation[4], visual stimulus presentation [6][7][8], among others. A comprehensive review of the state-of-the-art techniques used for EEG signal preprocessing and feature extraction was conducted by Saeidi et al.[10], 128 articles were studied.
Shallow and deep models for EEG analysis were proposed; Bidgoly et al.[31] and Pawan et al.[32] deeply investigated them. To apply shallow methods, feature extraction is necessary. Common feature extraction methods such as Autoregressive Model, fast Fourier Transform, Common Spatial Pattern, and Wavelet transform are discussed in their work. Similarity-based methods, relying on distances such as euclidean, cosine or cross correlation, are among the simplest methods reported for EEG-based authentication systems. Shallow models, including Support Vector Machines[30], Hidden Markow Models and Artificial Neural Networks, are widely utilized. Their work reported that the majority of employed deep models are based on Convolutions Neural Networks, often combined with Long Short-Term Memory or Gated Recurrent Units.
Different scenarios of impostor attacks were investigated for EEG-based Authentication. Wu et al. [11][21] examined the robustness of EEG-based authentication in two distinct cases: in the first, impostors were unaware of the target stimuli, while

in the second, they were informed about the target stimuli and adopted the same strategy as the legitimate user. The RSVP paradigm is used in their study, the target stimuli comprise the user's own face images, whereas face images of familiar and stranger individuals are utilized as non-target stimuli. This approach may make it easier for impostors to discern the supposed target stimuli, as the faces of the person attempting to access the system are displayed. By allowing impostors to concentrate solely on the user image seen just before the test trial, their study did not consider the scenario where impostors thoroughly learn and assimilate over time the target images of the legitimate user, successfully evoking responses at the right time and completely mimicking the behavior of the legitimate user.
In recent years, the unforgeability of EEG data has been questioned due to the progress made by Adversarial Generative Networks (GANs), which can effectively replicate brainwave signals to the extent of spoofing EEG-based authentication systems. To mitigate this vulnerability, Piplani et al. [12] demonstrated that training the classifier with GAN-generated data would be a valid countermeasure. Essentially, user EEG data stolen by imposters and used to train a GAN, could deceive a model trained without GAN-generated data. However, training a model with artificially-generated data may face challenges in terms of comprehensiveness and scalability, especially with the addition of new users. Furthermore, the disclosure of personal identification information intrinsic to stolen brainwave data still poses a risk to privacy.
The systems proposed still fail to address an important challenge. They are designed to operate with a defined set of users known at training time, necessitating the model to be re-trained from scratch each time a new user needs to be registered, which can be resource intensive and time consuming. This lack of universality renders them not applicable in practice. Others models which employ a multi-class classification approach trained of a predefined set of users, face same challenges in generalization and scalability to accommodate new users.

1.3 Problem Statement

Approaches to EEG-based authentication have traditionally prioritized the accuracy of detecting legitimate users and rejecting impostors, often overlooking other critical aspects and conditions essential for obtaining a deployable working model[22].

The potential scenario where malicious agents acquire knowledge about the target stimuli intended to elicit an ERP response from the legitimate user, thus granting impostors the ability to access the system, must be further investigated.
Unauthorized access to the system and the theft of confidential personal data pose significant privacy concerns and may potentially be exploited to train generative models to deceive the system. This is a condition that must be preemptively prevented and avoided. Impostors may spy on users during authentication phase to discover their stimuli target set or directly gain access to the images stored into the system, and subsequently reproduce an attack. This poses a significant security risk as it not only compromises the confidentiality of the authentication process but also enables malicious actors to mimic genuine users more effectively.

The primary focus of this work lies in addressing these challenges and vulnerabilities, keeping in regards the universality and scalability requirements, and enhancing reliability of EEG-based authentication systems. A model tailored for each user would necessitate an impractical amount of user-specific data, rendering user enrollment burdensome and impeding generalization to other users. Consequently, re-training would be required for each new user added to the system.

Channels reduction, which is a concrete challenge against an effective deployable model, is not directly addressed in this work. Other studies have shown good results [9][20] with this technique; therefore, its integration is the subject of future work. Authentication phase time duration, another important quality for effective system usage, is not directly investigated in this work. Other studies obtained authentication completion within a time ranging from few seconds to one minute [8][11][20].

1.4 Proposed Solution

The problems introduced previously are addressed by this work through a novel approach. The proposed model aims at effectively differentiate between legitimate users and impostors, even if the latter have acquired knowledge of the user target images. The model extracts unique features from the EEG signals, generating individual fingerprints. During login phase, the stored user fingerprint is compared to the one extracted from the recorder EEG signals. If the similarities are adequate, system access is granted; otherwise, a possible impostor is detected.
By storing solely the fingerprint of the users and not the raw data, the model ensures robustness against data breaches and theft. The model is specifically designed for authentication, minimizing the risk of erroneously classifying external users as legitimate ones. Furthermore, the use of common feature extraction facilitates the easy accommodation of new users into the system.
To obtain a feature extractor several pathways can be followed, this work takes a deep learning approach. Within this context, a feature extractor is typically a sub-part of a larger deep neural network. The feature extractor proposed is based on a Autoencoder network whose layers consist of convolutional neural networks (CNN) layers. Autoencoders excel in performing dimensionality reduction, feature extraction and anomaly detection. CNN are notably effective in spatial and temporal feature extraction. The encoder part of the autoencoder serves as the feature extractor, whereas the decoder part is used at training and can be discarded subsequently. A different approach based on classification was proposed by Bidgoly et al.[9], the CNN is combined with two fully connected layers, which serves as the classifier and are discarded after training.

Other general security measures such as encryption of stored data, monitoring of suspicious user activities, implementation of secure communication protocols and physical protection must be followed along with the system proposed to enhance the robustness of the authentication system.

Chapter 2

Background

This chapter aims to lay the foundations for the rest of the work by introducing key topics related to *Authentication*, *Brain-Computer Interaction* and *Artificial Neural Networks*.

2.1 Authentication

An authentication system M can be formally defined as a tuple:

$$M = (A, S, f, l)$$

- A denotes the set of authentication information presented to the system during login. A single authentication input given by a user is represented as $a \in A$. In EEG-based authentication, A is the set of EEG sample records.
- S is the set of stored information produced during the registration phase by the system. The information of the claimed identity is represented as $s \in S$.
- $f : A \to S$ is the function that generates S from A. In this study, it is the feature extractor that generates the vector of stored feature given the recordings of user's brain signal. For any $a \in A$, it produces $s \in S$.
- $l : (A \times S) \to \{true, false\}$ is the authentication function that verifies the legitimacy of the claimed identity. Given a pair $(a \in A, s \in S)$ it compares their similarity and either grants or rejects access to the system.

Authentication is the processes of verifying the identity claimed by an entity based on the provided information. The user initiates the process by specifying the identity to be authenticated, access control to system assets is granted after presenting the required authentication factors that ensure the truthfulness of the claimed identity. The factors necessary for achieving secure and robust authentication encompass three distinct categories:

- Knowledge: Information known exclusively by the legitimate entity (e.g. password, PIN, answer to a security question).

- Ownership: Possession of items exclusive to the legit entity (e.g. a smart card or security token).
- Inherence: Biometric features, which are traits or attributes closely associated with the identity or actions of the legitimate entity. These comprehend both physiological (e.g. fingerprint, iris) and behavioral features (e.g. gait, typing pattern).

EEG-based authentication leverages the electric signals generated by the brain as a unique identifier for the user. Brain activity, stemming from the intricate network of neurons in the brain, can be elicited by visual or emotional stimuli, thus incorporating both the physiological and the behavioral components of the biometric features.

The weakest level of protection is offered by single-factor authentication, where only a single component from one of the three categories of factors is used to authenticate an individual's identity. Multi-factor authentication achieves a higher level of protection by leveraging the effectiveness of multiple components combined together.
In EEG-based authentication, multiple factors can be seamlessly integrated into the authentication process. This involve combining the collection of brain signals with the presentation of stimuli designed to exclusively trigger the desired entity, associating a target stimuli with a specific response and thereby exploiting the knowledge factor category. Furthermore, the identity selection and authentication process can be initiated upon the presentation of an ownership category factor, such as an identity card or security token.

EEG biometric authentication ultimately reduces to resolving a binary classification problem. Designing a model capable of correctly distinguish between legitimate users and impostors requires that brain waves collected from the users seeking access to the system are generated consistently across all users. When registering new users into the system, EEG waves are collected while the user is at rest or performing a specific task, such as watching the RSVP stream of images. After signals have been recorded, they undergo processing, and features are extracted. During inference when new signals are provided, the classifier, trained on the extracted features, can perform either user identification or user authentication. In the former, the system detects the user's identity by matching the most similar features stored across all users to the presented ones. In the latter, the identity to be authenticated-in is first selected, then the system directly compares the stored features for that identity to the ones provided by the system logger. The similarity between the twos is assessed, and if they are sufficiently comparable, access is granted. To maintain system consistency, the task the user perform during login must align with that undertaken during registration.
Clearly, utilizing a model designed for identification to perform authentication is inappropriate, as it would not reject users not registered into the system but instead attempt to match them to an existing user, which is not the expected behaviour. Furthermore, it would be not possible to include new users into the system without retraining the whole model.

2.2 Brain Computer Interaction

To acquire data from the brain and process it using a computer, specialized equipment is required. A brain-computer interface (BCI) is a machinery that establishes a connection between the central nervous system and an external digital device. Depending on the flow of information, BCI are categorized as mono-directional and bi-directional. The level of invasiveness in BCI implementations varies based on the proximity of electrodes to the brain tissue. Non-invasive BCIs include techniques such as Electroencephalography, Magnetoencephalography (MEG), and Magnetic Resonance Imaging (MRI). Electrocorticography (ECoG) represents a partially invasive BCI, where electrodes are placed directly on the exposed brain surface. Microelectrode arrays (MEAs) are examples of implanted invasive BCIs.
Two categories of electrodes can be applied over the scalp, wet and dry. Wet electrodes are generally made of silver/silver chloride material (Ag / AgCl), they use an electrolytic gel material as a conductor between the skin and the electrode. Dry electrodes consist of a single metal that acts as a conductor between the skin and the electrode, their material is usually stainless steel. Dry electrode facilitate portability of EEG recording, avoiding the set-up phase and washing phase needed for gel positioning needed by the wet ones, they are more user-friendly and more affordable. However, they require to be properly positioned to avoid noise in the signal recorded. Comparison between wet and dry electrodes showed that they obtain comparable results, sufficient for clinical applications[27][28]. In this study, a mono-directional EEG brain interface with 128 dry electrodes is utilized to collect samples of brain waves for brain-computer interaction.

Figure 2.1. 128 Electrodes Biosemi EEG cask

2.2.1 International 10-20 System

The 10-20 system is the international standard adopted to describe the positioning and application of electrodes across the entire surface of the scalp. Electrodes are

evenly distributed over the skull according to the reference system, where the 10 and 20 refer to the 10% or 20% distance between adjacent electrodes relative to the total front–back and right–left length of the skull.

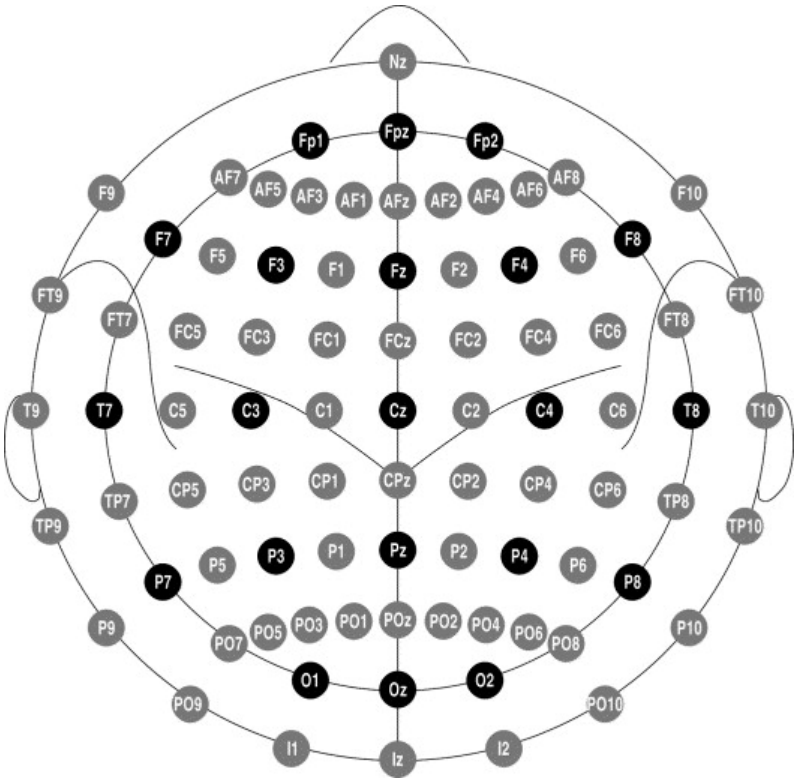


Figure 2.2. Illustration of the standard for positioning the electrodes over the scalp surface in the 10-20 System. Black circles denote positions based on the original 10–20 system, while gray circles represent additional positions introduced in the 10–10 extension.

The initial 10-20 electrode system was proposed by H.H.Jasper in 1958 [13], it allocated 21 electrodes over the scalp. In 1985, an extension to the original 10–20 system was proposed by Chatrian et al., increasing the number of electrodes from 21 to 74 [14]. This extension involved increasing the number of electrodes along the contours over the scalp, achieved by reducing the distance of the medial-lateral contours to 10% and introducing new contours in between the existing ones. The standard 10-20 systems includes these positions. To distinguish it from the original 10-20 system, it is referred to as the Extended 10-20 system, also known as the 10% system or 10-10 system. The Extended 10–20 system of electrode placement has gained widespread acceptance and was endorsed as the standard of the American Electroencephalographic Society [15][16] and the International Federation of Societies for Electroencephalography and Clinical Neurophysiology [17][18]. In 2001, Oostenveld R. and Praamstra P. [19] proposed a logical extension of the 10-10 system, integrating the standard locations of both the original 10-20 system and the 10-10 system, thereby facilitating the utilization of up to 345 electrode locations. Given that the system employs proportional distances of 5% of the total length along contours between skull landmarks, as opposed to the 20% and 10% distances

used respectively in the 10–20 and 10–10 systems, it is referred to as the 5% system or the 10–5 system. Additionally, they proposed a subset of 128 electrodes derived from the 10-5 system as the standard configuration for modern Brain-Computer Interface apparatus. This selection aligns with the common operational setup of 128 electrodes, as the one employed in the present study.

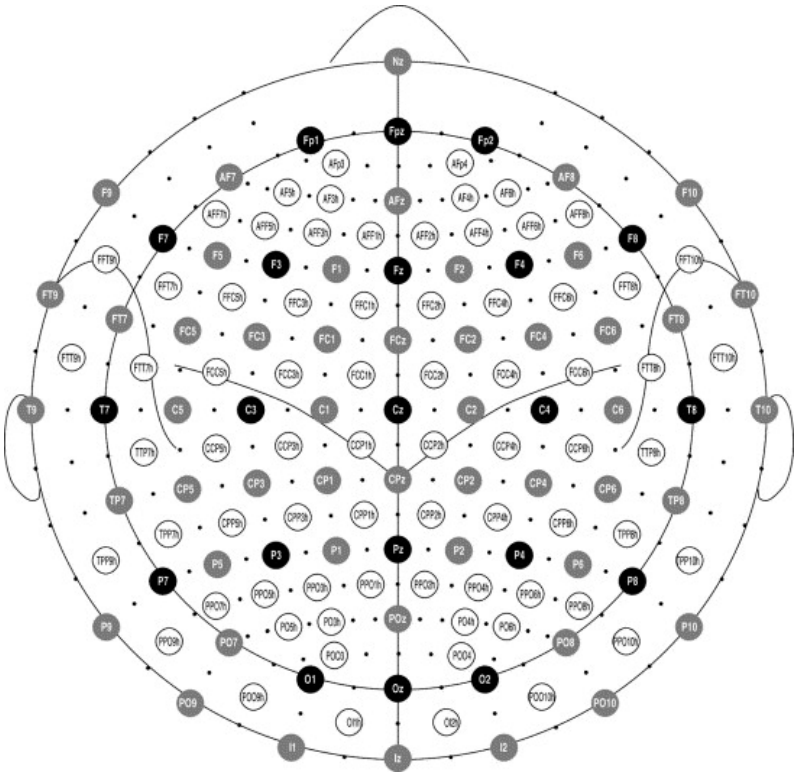
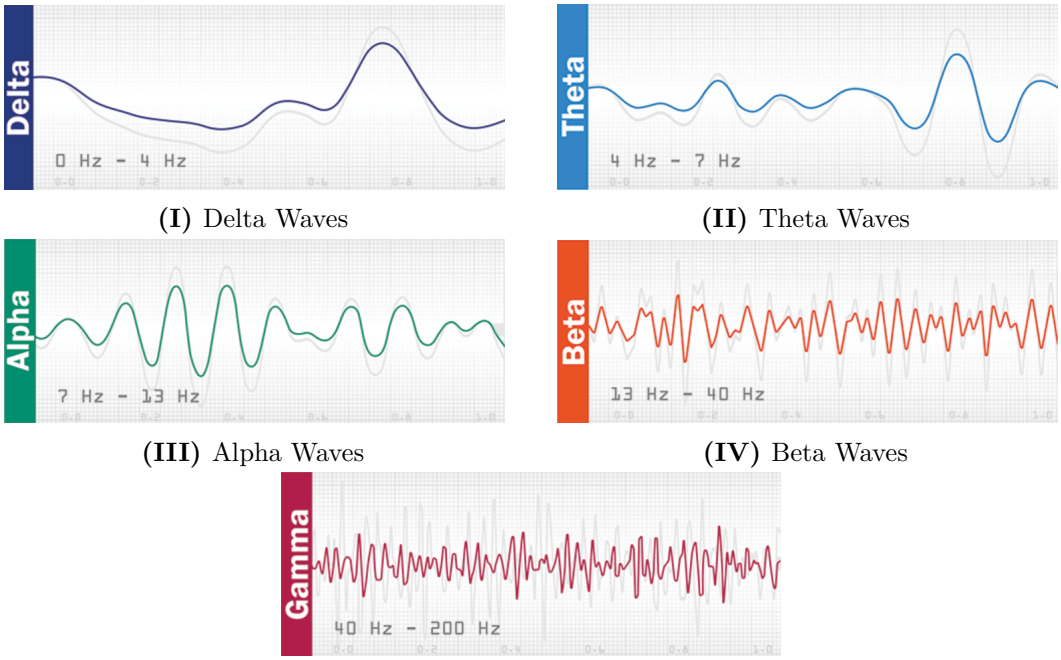


Figure 2.3. Illustration of the standard for positioning the electrodes over the scalp surface in the 10-5 system. Dots indicate positions additional to the 10–10 system, with a subset of useful positions designed for a 128-channel EEG system are highlighted by white circles.

2.2.2 EEG Waves

The EEG activity is the outcome of ionic current flows generated by the synchronized synaptic activation of the brain's neurons. This activity manifests as rhythmic voltage fluctuations, with amplitudes ranging from 5μV to 100μV and frequencies from 0.5Hz to 40Hz. Based on their frequency, brain waves are classified into the following frequency bands:

- δ (delta): frequency band lower than 4Hz. Delta waves are the slowest and have the highest amplitude. They are usually observed in babies and during sleeping.
- θ (theta): frequency band ranges from 4Hz to 8Hz with amplitude normally less than 100μV. Theta band is observed in children, during relaxation, meditation and memory recalling.



(I) Delta Waves

(II) Theta Waves

(III) Alpha Waves

(IV) Beta Waves

(V) Gamma Waves

Figure 2.4. Frequencies bands of EEG Waves. The displayed figures illustrate general frequency bands of EEG waves. It is important to note that the frequencies values shown are indicative and not accurate representations.

- α (alpha): frequency band ranges from 8Hz to 12Hz with amplitude normally less than 50μV. Alpha waves are divided into low alpha waves(8-10Hz) and high alpha waves (10-12Hz). The alpha frequency band is usually the dominant one, it appears during relaxed awareness or when eyes are closed. Focused attention or relaxation with opening eyes reduces the amplitude of the Alpha band.

- β (beta): frequency band ranges from 12Hz to 30Hz, amplitude is normally less than 30μV. Beta waves are divided into low beta waves (12-20Hz) and high alpha waves (20-30Hz). Beta waves are associated with thinking, active concentration, alert, focused attention and body movements.

- γ (gamma): frequency band greater than 30Hz, amplitude is the lowest. Gamma waves are divided into low gamma (30-40Hz) and high gamma (above 40Hz). Gamma waves are observed during higher cognitive functions, multiple sensory processing and problem solving.

- μ (mu): frequency band ranges from 8Hz to 13Hz, overlapping with other frequencies. It reflects the synchronous firing of motor neurons in rest state.

2.3 Artificial Neural Network

Artificial Neural Networks (NN) are computational models inspired by the biological Neural Networks structure and functioning. A formal definition provided by E.Fiesler[29], that applies to both natural and artificial Neural Network, is presented in summary:

$$\mathcal{N} = (T, C, S(0), \Phi)$$

- T is the topology which consists of the framework and interconnection structure.
- C is the set of constraints associated with the neural network. Constraints include limitations on parameters, connectivity, or other properties relevant to the network's behavior.
- *S(0)* is the set of initialization states, indicating the initial states or condition of the neural network. It refer to the starting point of the network, considering initial weights, initial activation and initial local threshold.
- Φ is the set of transition functions, describing how the neural network evolves from one state to another over time. Transition functions describe the behaviour of neurons output and the learning rules, how parameters are updated.

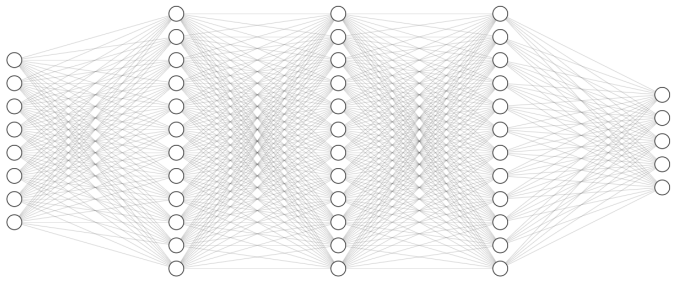


Figure 2.5. Fully Connected Feed Forward Neural Network (FCNN): Illustration of an artificial neural network with three hidden layers, featuring eight neurons at the input layer and five neurons at the output layer.

A neural network can been seen as a parameterized function that taken a D-dimensional input, produces a D'-dimensional output, $\mathcal{N}_\theta : \mathbb{R}^D \to \mathbb{R}^{D'}$, parameterized by θ.

2.3.1 Convolutional Neural Network

Convolution is a mathematical operation which combines two functions to describe the overlap between them. Convolution creates a new function by sliding one of the input function over the other one, multiplying the function values at each point where they overlap, and adding up the products. The resulting function is representative

of the interaction between the two original functions. Formally, convolution is an integral that expresses the amount of overlap of one function $f(t)$ as it is shifted over function $g(t)$:

$$(f * g)(t) =^{def} \int_{-\infty}^{\infty} f(\tau) \cdot g(t - \tau)\, d\tau = \int_{-\infty}^{\infty} f(t - \tau) \cdot g(\tau)\, d\tau$$

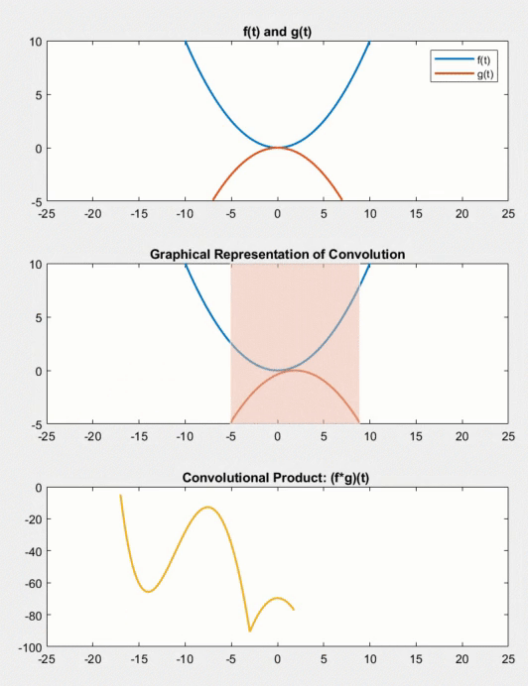


Figure 2.6. Continuous Convolution

As can be observed, the convolution operation is commutative. Convolution can be applied also in the discrete case, such as those encountered in Machine Learning problems. Let f, g be defined on the set $\mathbb{Z}$ of integers. The discrete convolution of f and g is given by:

$$(f * g)[n] =^{def} \sum_{m=-\infty}^{\infty} f[m] \cdot g[n - m] = \sum_{m=-\infty}^{\infty} f[m - n] \cdot g[n]$$

Convolutional neural networks are based on the convolution operator. They were inspired by the visual cortex of animals where individual cortical neurons respond to stimuli only in a restricted region of the visual field, known as the receptive field. The receptive fields of different neurons partially overlap such that they cover the entire visual field. This behaviour is replicated in CNN by using a convolution filter (or kernel) that slides over the whole input features. The kernels possess shared weights for the whole layer. This consistently reduces the number of parameters, allowing the network to have more layers and go deeper. CNNs particularly excels in domains such as image analysis, natural language processing and signal processing, among others.

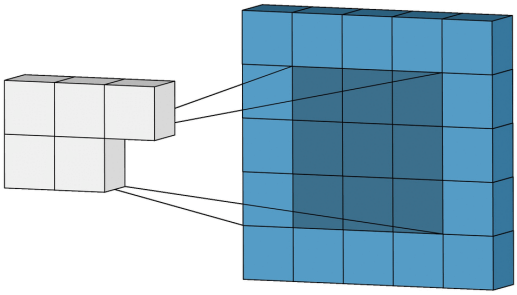


Figure 2.7. 2-dimensional Discrete Convolution

CNN architecture consists of an input layer, hidden layers that perform convolutions and an output layer. The process involves the dot product between the input layer's matrix and the convolution kernel, followed by an activation function. The convolution kernel slides along the input matrix of the layer, generating a feature map (or activation map) through the convolution operation. This feature map then contributes to the input of the next layer. Subsequent layers, such as pooling layers, fully connected layers, and normalization layers, could then be employed. The output resulting from a kernel slide exhibits lower dimensionality than the input, therefore padding is employed. This technique guarantees dimensionality consistency by introducing values, typically zeroes, to the boundaries of the data.

Sampling

Different down-sampling and up-sampling techniques are employed within CNN layers. Max Pooling is a down-sampling technique frequently employed in convolutional neural networks (CNNs) to diminish the spatial dimensions of an input volume. This non-linear down-sampling method aims to make the representation smaller and more manageable, while concurrently reducing the number of parameters and computational load in the network. Max pooling operates independently on each depth slice of the input, resizing it spatially. There are three primary advantages to Max Pooling:

- Feature Invariance: Max pooling helps the model to become invariant to the location and orientation of features.
- Dimensionality Reduction: By down-sampling the input, max pooling significantly reduces the number of parameters and computations in the network, thus speeding up the learning process and reducing the risk of overfitting.
- Noise Suppression: Max pooling helps to suppress noise in the input data. By taking the maximum value within the window, it emphasizes the presence of strong features and diminishes the weaker ones.

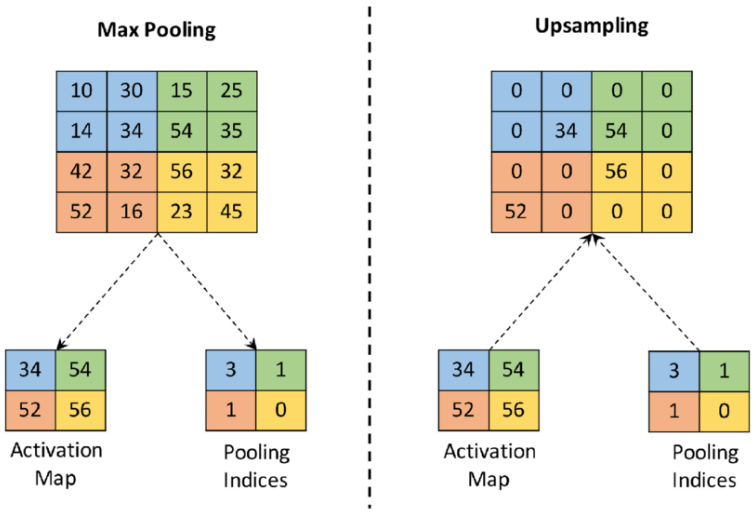


Figure 2.8. Illustration of Max Pooling and Upsampling techniques.

Max pooling is applied to the convolutional layers of a CNN. This process entails sliding a window (commonly referred to as a filter or kernel) across the input data, similarly to the convolution step. However, instead of conducting a matrix multiplication, max pooling selects the maximum value within the window. The inverse operation of Max Pooling is the upsampling interpolation. An alternative to Max Pooling is Average Pooling, where the average of the values whitin the window is selected.

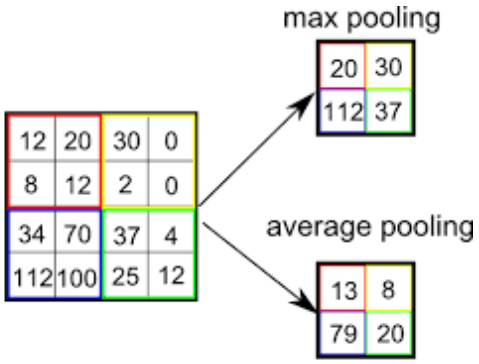


Figure 2.9. Max Pooling and Average Pooling

2.3.2 Autoencoder

Autoencoders are artificial neural networks used in unsupervised learning. They encode input data into a lower-dimensional representation using an encoder and subsequently decode it, attempting to reconstruct it as accurately as possible to the original input through a decoder. The decoder mirrors the structure and behavior of the encoder. Autoencoders are particularly well-suited for tasks such as dimensionality reduction, feature learning, data compression, denoising and anomaly

detection.

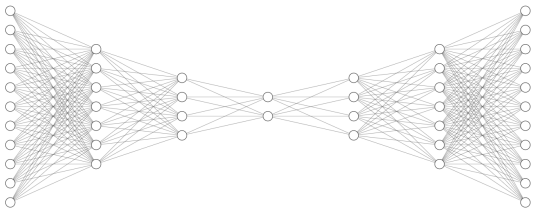


Figure 2.10. Autoencoder Architecture: Fully Connected Neural Network style

The autoencoder is formally defined by two sets $\mathcal{X}$ and $\mathcal{Z}$, and two parameterized family of functions E_ϕ and D_ϕ:

- $\mathcal{X}$ is the set of decoded messages, typically represented as an euclidean space $\mathcal{X} = \mathbb{R}^m$ for some m.
- $\mathcal{Z}$ is the set of encoded messages, usually an euclidean space $\mathcal{Z} = \mathbb{R}^n$ for some n.
- $E_\phi : \mathcal{X} \to \mathcal{Z}$ is the family of encoding functions, parameterized by ϕ.
- $D_\phi : \mathcal{Z} \to \mathcal{X}$ is the family of decoding functions, also parameterized by ϕ.

For any decoded message input, $x \in \mathcal{X}$, it is possible to obtain an encoded message $z = E_\phi(x)$, often referred to as the code, the latent variable, latent representation, or latent vector. Conversely, for any encoded message $z \in \mathcal{Z}$, it is possible to obtain a decoded message $x' = D_\phi(z)$. The goal of the autoencoder is to learn an effective encoding z from x and subsequently reconstruct x' to be as similar as possible to x.

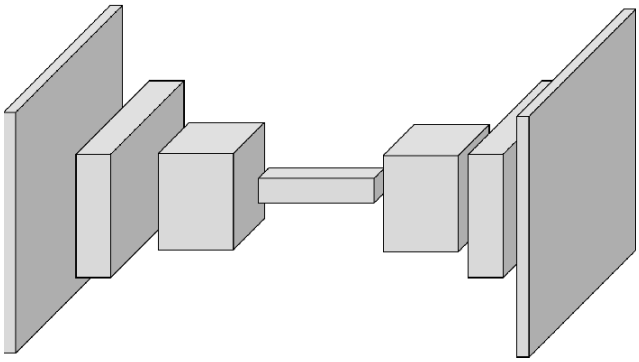


Figure 2.11. Autoencoder Architecture: Convolutional Neural Network style

Chapter 3

Method

This chapter illustrates the system implementation and the results obtained.

3.1 Dataset

To study a model coherent with the proposed task, an appropriate set of data is indispensable. A dataset capable of conciliating user knowledge stimulated by visual stimuli of familiar faces and impostors gaining notion of user target stimuli was required. The FFR-EEG dataset, created and utilized in *A robust neural familiar face recognition response in a dynamic (periodic) stream of unfamiliar faces*[33] by Yan X. and Rossion B. to study and measure human general face familiarity recognition across variable facial identities, is suitable for this work. Twenty-six participants observed a rapid serial visual presentation of natural images, showcasing different unfamiliar faces at a constant rate of 6 Hz (i.e., 6 faces per second). Periodically, variable images of various famous face identities were introduced every 7th image (i.e., 0.86 Hz). Two different versions of the experiment were conducted several months apart.

The set of target stimuli and of non-target stimuli were the same for all participants. This experimental arrangement reproduce the scenario in which impostors acquire knowledge of the victim's target images. A model capable of distinguishing users under these conditions, without relying on the knowledge factor, would be suitable for rejecting unveiled attack by impostors.

3.1.1 Participants

A total of twenty-seven Caucasian individuals participated in the experiment. Sixteen completed the first version, eleven completed the second version and one participant took part in both versions. Data of one subject participating to the first version was excluded due to excessive much muscular noise artifacts. There was no age difference among participants. The final sample consisted of ten males and six-teen females, with a mean age of 22 $\pm$ 2.13 year. Participants were unaware of study's objective and performed an orthogonal task. All participants, self-reported as right-handed, had normal or corrected-to-normal vision and no history of neurological

or psychiatric disorders. Written consent was obtained from all participants prior to the experiment. The study was approved by The Biomedical Ethical Committee of University of Louvain.

3.1.2 Stimuli

In the first version of the experiment, stimuli comprised 240 color images featuring famous male celebrity faces. There were 12 different face identities, each represented by 20 distinct natural images. The selection of these six celebrities was based on pilot questionnaires conducted among participants from other experiments. Additionally, six random foreign celebrities were included as unfamiliar faces. The faces in the stimuli sets exhibited variations in head orientation, lighting, and expression, among other factors. Visual properties of the images from the two stimulus sets were carefully considered and matched for age, hair color, and overall facial appearance. This matching process aimed to prevent potential distinctions in image characteristics between the two sets. The images were sized at 200 $\times$ 250 pixels, providing a visual angle of approximately 8.5° in width and 9.1° in height when viewed from a distance of 80 cm. In total, 23 out of 26 participants reported knowing all six familiar identities well. Two participants were unable to recall one familiar identity face, while another participant recognized the face of a familiar identity but was not familiar with their name and profession.The analysis conducted by Yan and Rossion revealed that these three participants exhibited significant and equivalent familiar face recognition responses compared to the rest of the participants.
In the first version of the experiment, the number of facial identities is strictly matched between familiar and unfamiliar faces, with each identity being presented across 20 variable images. However, due to the larger number of unfamiliar face presentations, each unfamiliar face identity was, on average, shown six times more than each familiar face identity in the experiment. Therefore, to ensure that this difference in presentation frequency does not account for the familiar face recognition response, a second version of the experiment was conducted. In this second version, there were a total of 36 unfamiliar face identities to strictly balance the face identity repetitions of familiar and unfamiliar faces, although the number of identities was not matched. During each stimulation sequence of 70 seconds, each face identity was presented 10 times, with 10 different natural images. All other parameters of the stimuli were identical for the two versions.

3.1.3 Testing Procedure

In each stimulation sequence, unfamiliar faces were presented at a fixed rate of 6 Hz over 74 seconds, including a 2-second stimuli fade-in and a 2-second fade-out. The faces were selected randomly by the stimulation program, ensuring that the exact same image did not appear consecutively. Within a sequence, familiar face images of different face identities were inserted every 7^{th} image. All face stimuli were presented through sinewave modulation of contrast, ensuring a smooth transition between images. At every stimulation cycle, the image size randomly varied between 80% and 120% in order to even further minimize pixel overlap (e.g., eyes falling in the same location) between consecutive stimuli. Face stimuli were presented

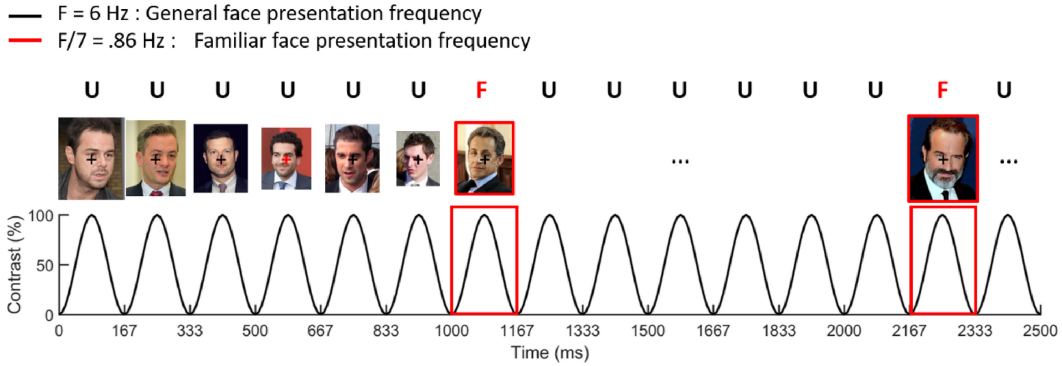


Figure 3.1. Experiment Face Presentation Frequency Setup: Unfamiliar faces presented at 6 Hz, with periodic insertion of familiar faces every 7th image at 0.86 Hz.

at upright or inverted orientation in each sequence, six times each. The order of the face orientation conditions was randomized across participants. Participants performed an orthogonal task by responding to the color change of a central fixation cross (from black to red, appearing non-periodically and lasting 200 ms). The entire recording took about 20 minutes, with approximately seven minutes per orientation for visual stimulation and including breaks.

3.1.4 Acquisition Procedure

The experiment took place in a quiet, low-lit room. Stimulation sequences were presented on an LED monitor with a 1600 × 900 window resolution and a 120 Hz refresh rate, centrally on the screen. High-density 128-channel EEG was acquired using the ActiveTwo Biosemi system at a 512 Hz sampling rate. The magnitude of the offset of all electrodes, referenced to the common mode sense, was maintained below 30 μV. Vertical and horizontal electrooculogram (EOG) were recorded using four additional flat-type active electrodes: two above and below the participant's right orbit and two lateral to the external canthi of the two eyes.

3.1.5 Preprocessing Analysis

EEG data was analyzed with the open source software Letswave 5, running in MATLAB R2013a (MathWorks, USA). Initially, EEG data underwent band-pass filtering between 0.05 and 100 Hz with a 4th order zero-phase Butterworth filter. Subsequently, the data was down-sampled to 256 Hz for ease of processing. The data sequence was then segmented relative to the starting trigger of each trial, with an additional 2 sec before and after each sequence. Eyeblink artifacts, occurring more than 0.2 times per second on average, were corrected by applying independent component analysis to the data from eight participants across two experiments. Channels containing artifacts were interpolated using the values from their three neighboring channels. On average, 2.5 ± 1.9 channels were interpolated per participant, with a maximum of 6 channels. Subsequently, the cleaned-up data was referenced to the average of all 128 electrodes.

Figure 3.2. Biosemi ActiveTwo AD-box system

3.1.6 Frequency Domain Analysis

The preprocessed data were epoch-aligned to have an integer number of cycles corresponding to familiar face presentations. The initial and final 2 seconds of each presentation sequence were discarded to eliminate artifacts from eye movements and muscle activity associated with abrupt stimulus onset and offset. The resulting epochs were 68.84 seconds in length, precisely capturing 59 face presentation cycles. Subsequently, a Fast Fourier Transform was applied to extract amplitude spectra with a frequency resolution of .0145 Hz.

Baseline EEG activity was estimated with the neighbouring 20 bins surrounding the frequency bins of interest, 10 bins by each side, excluding immediately adjacent bins to address remaining spectral leakage. Local maximum and minimum amplitude bins were excluded to prevent the signal projection into the noise EEG spectrum. Two methods were employed for baseline correction of the EEG responses:

1. Division by EEG noise to visualize the EEG spectrum in signal-to-noise ratio, enhancing visibility of small responses.

2. Subtraction of the EEG noise (baseline subtraction) to quantify responses in μV across summed harmonics

For the two presentation frequencies (6 Hz and .86 Hz), responses were observed at multiple harmonics. The selection of harmonics was based on the grand-averaged response patterns across all participants, channels and face orientation conditions.

3.1.7 Time Domain Analysis

The spatio-temporal dynamics of the FFR response was investigated as follows: referenced EEG signal were low-pass filtered with a 30 Hz cut-off (4th order Butterworth filter) and then cropped into an integer number of cycles of the familiar face presentation frequency (ranging from 2 to 70.84 seconds, encompassing 59 face presentation cycles). Afterward, the general face presentation frequency and its first

five harmonics (up to 30 Hz) were removed using a narrow-band notch filter (width = 0.05). The EEG waveforms were then segmented into smaller epochs, each containing seven stimulation cycles (i.e., 1167 ms), comprising six unfamiliar face presentations and one familiar face presentation at the second position. Epochs were averaged and baseline-corrected relative to the first unfamiliar face stimulus presentation. This analysis was conducted on individual participants before averaging at the group level.

3.1.8 Behavioral Analysis

For the fixation color detection task, response times were calculated relative to the onset of color change. Responses were considered correct if they occurred between 150 ms and 1000 ms following target onset.

3.1.9 Data

Epochs have been extracted per user. Data has been normalized on an epoch-wise basis through mean subtraction and unit variance scaling. The resulting training set consisted in epochs belonging to twenty different users. Data from three unseen users was used for testing model's generalization performance to new users. The remaining three users were considered impostors. The training and validation sets consist of data from normal users, whereas the testing set includes data from new users and impostors. Each epoch comprises a vector of 132 electrode channel recordings, encompassing 17,625 timestamps, which corresponds to approximately 70 seconds.

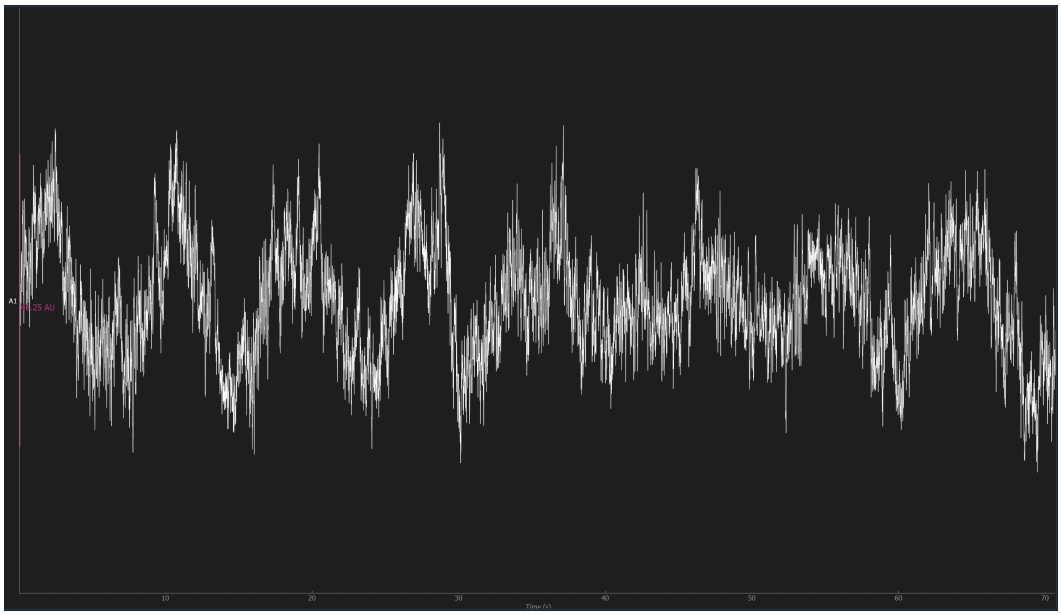


Figure 3.3. EEG wave data visualization. One epoch collected from electrode fp1 of participant 1. EEG data visualized using the MNE 1.6.0 Python library.

3.2 System overview

This study introduces a novel solution to tackle privacy concerns, universality issues, and the vulnerability to mimicking attacks posed by impostors. The proposed system employs a deep neural network based feature extractor. Specifically, a model based on convolutional layers within an autoencoder is utilized for training and subsequently obtaining the feature extractor.

The model is initially trained using preprocessed EEG data from the users. In the enrollment phase, users create a new account and undergo the RSVP process. Personal target images selected by users are inserted into the system and displayed, interleaved with non-target images already present into the system. After recording and processing EEG data, the system extracts the EEG fingerprint associated with users and stores it into the system database, along with the corresponding target images. During authentication, users select their identity and the RSVP process is initiated, retrieving the target images stored for the selected identity. Identity can be confirmed by presenting a token, ensuring the incorporation of a ownership-factor during the authentication process. The system analyze the users' response to the presented images, assessing if they provide correct responses to target images and no responses to non-target images. The model extract features from the EEG data and compares them with the fingerprint stored for the selected identity. If the distance score between the extracted features and the stored fingerprint is smaller than the threshold, access is granted, otherwise access is negated. The threshold can be adjusted according to the desired level of protection. Decreasing the threshold will guarantee an higher level of protection, rejecting an higher number of impostors. However, an higher number of genuine users will be classified as non legitimate. Increasing the threshold will result in a more lenient level of security, accepting a higher number of legitimate users along with impostors.
The distance score is computed using the Mean Square Error (MSE) Loss:

$$MSE = \frac{1}{|N|} \cdot \sum_{i \in N} (y_i - \hat{y}_i)^2$$

where N is the dataset, and |N| is its cardinality. y_i is the ground truth for instance the i^{th} instance and $\hat{y}_i$ is the model's prediction.

In the scenario were impostors execute an unveiled attack, the knowledge-factor cannot be exploited. The response to the stimuli are manipulated to resemble the legitimate ones, with the only distinctive element among users being their inherent and intrinsic responses, which originate from biological differences.

3.2.1 Feature Extractor

The autoencoder model employed is logically divided into two parts: the encoder and the decoder. Upon completion of training, the encoder functions as a feature extractor. To ensure effective feature extraction, the autoencoder is trained to reconstruct the input, promoting the development of robust features.

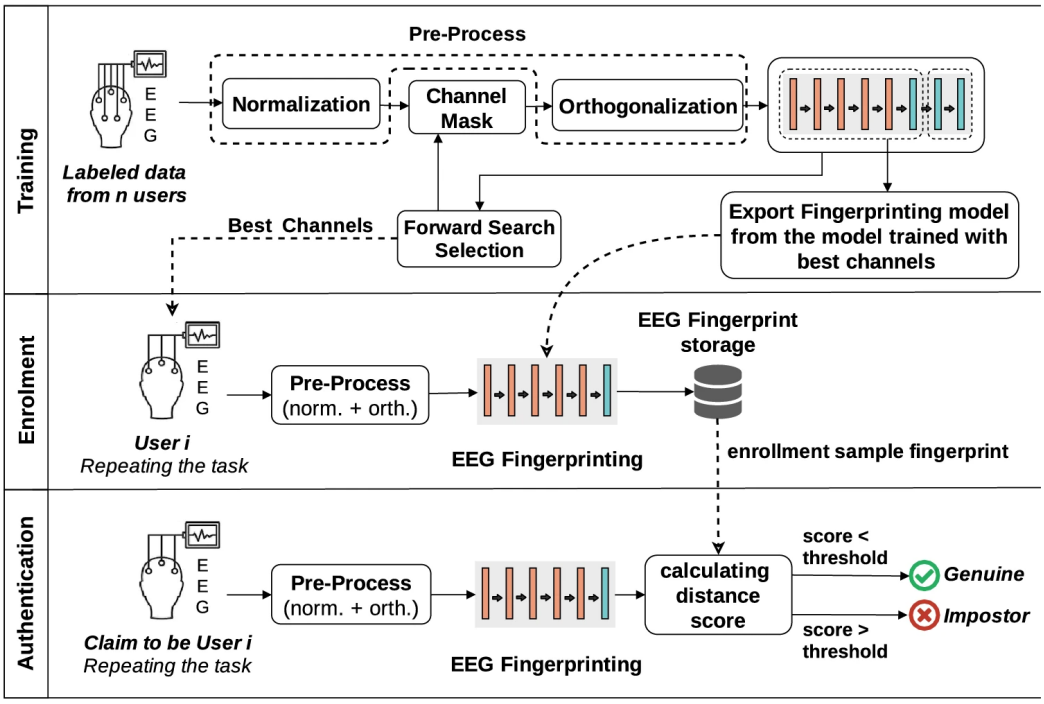


Figure 3.4. Schema of the EEG-based Authentication model proposed by Bidgoly et al.[9]. The authentication model proposed in this study shares the same logical architecture and structure, differing only in the channels reduction processing.

The model is implemented using the Pytorch machine learning framework. The encoder architecture, depicted in Figure 3.5, consists of ten layers, including five 1d-convolution layers and five max-pooling layers. The decoder architecture, depicted in Figure 3.6, mirrors the encoder structure, replacing max-pooling layers with upsampling layers. An additional last convolutional layer is included in the decoder architecture to ensure dimensionality matching. The kernel size is set at 7, max-pool size is 2 and padding is setting accordingly to maintain dimensionality consistency. In the encoder and decoder, CNN layers are interleaved with max pooling and upsampling linear interpolation layers, respectively. To mitigate overfitting during training, dropout is implemented with a probability of 25%. The number of filters applied at each layer varies, aligning with the dimensionality complexity of the data.

3.3 Results

The model's performance was assessed across the various users authentication trials. Impostor attacks were conducted on both users encountered during training and new users. The attack simulation involved deploying all impostor epochs data against each user, leading to a higher number of total authentication trial instances for impostors compared to legitimate users. To tackle the class imbalance, the accuracy metric has been adjusted to offer a more meaningful evaluation of the

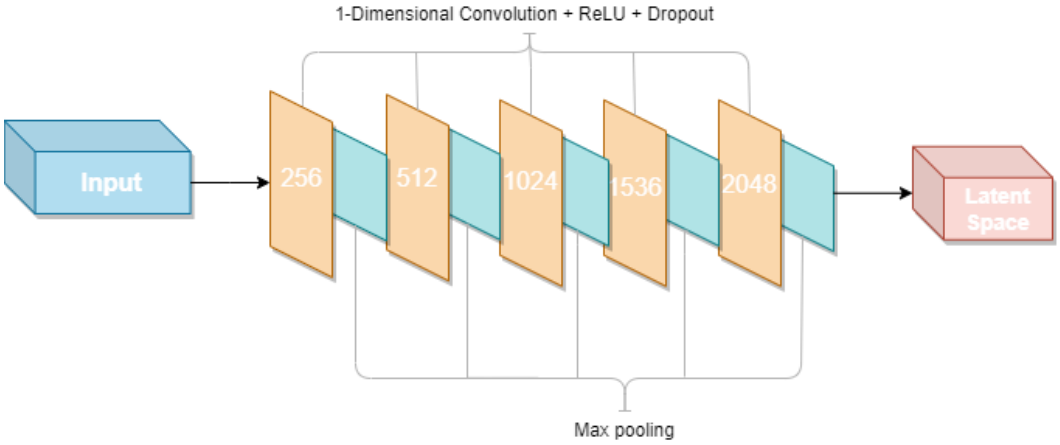


Figure 3.5. Illustration of the encoder's architecture. The number on the layers represent the number of filters applied at that convolutional layer.

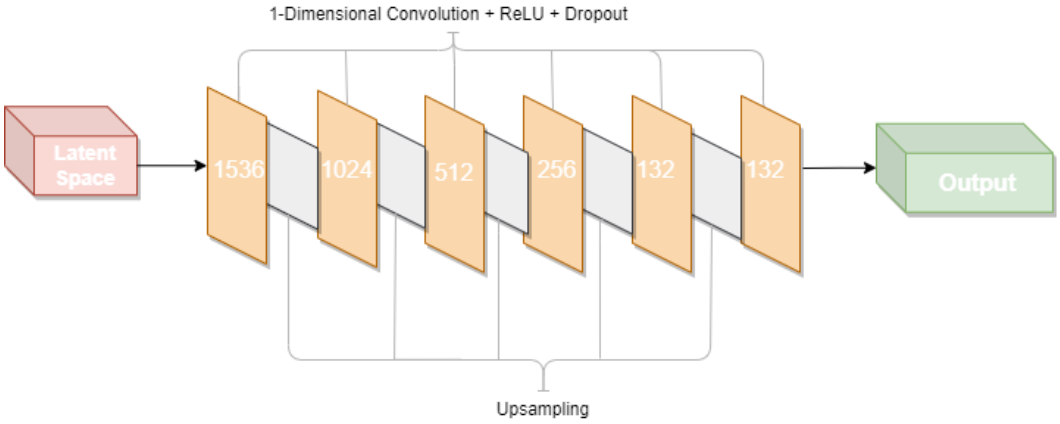


Figure 3.6. Illustration of the decoder's architecture. The number on the layers represent the number of filters applied at that convolutional layer.

model's performance.

$$Balanced\ Accuracy = \frac{1}{2} \cdot \left(\frac{TP}{TP + FN} + \frac{TN}{TN + FP} \right)$$

- TP is the total number of true positive instances. Legitimate users that are classified correctly.
- TN is the total number of true negative instances Impostors that are classified correctly.
- FP is the total number of false positive instances. Impostors that are classified as legitimate users.
- FN is the total number of false negative instances. Legitimate users that are classified as impostors.

Figure 3.7. Training and validation loss trends.

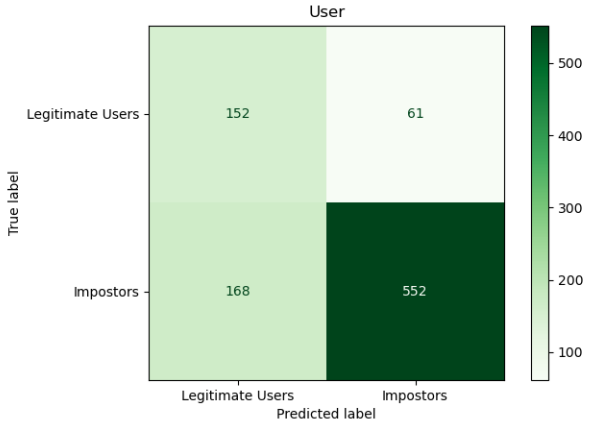


Figure 3.8. Confusion matrix showing impostors attacks conducted against users encountered during training time.

Applying a corrected accuracy metric with unbalanced data prevents favoring a model that simply classifies all instances into the same class, thereby avoiding a lack of meaningful learning. In this scenario, classifying all instances as impostors artificially inflate performance metrics, but the model would not achieve the goal or provide meaningful insights.

Figure 3.8 illustrates the confusion matrix of the model, providing a comparison of classification scores for new authentication attempts by users observed during training and those of impostors attempting to authenticate as them. Legitimate user detection accuracy is 71.36%, impostors rejection accuracy is 76.67%. The resulting balanced accuracy is 74.01%.

Figure 3.9 depicts the confusion matrix of the model when new users are registered into the system after it has been deployed and impostors try to authenticate

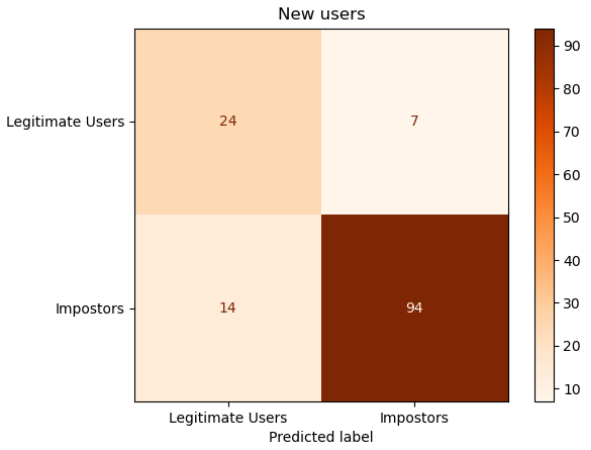


Figure 3.9. Confusion matrix illustrating impostors attack conducted against new users.

as the new users. The model successfully detects new users 77.42% of the time and rejects impostors 87.04% of the time. The balanced accuracy of the model over new users is 82.23%, 8% higher than with the users seen at training time. The reason for this increase in performance could be due to the inherent unique characteristics of the EEG signal. Nevertheless, the model is able to generalize and work properly with new users, satisfying the universality and scalability requirements.

Figure 3.10 shows the total confusion matrix of the model, considering attacks against all users. It is the union of the two precedent confusion matrices. Total detection accuracy over all legitimate users is 72.13% and the rejection accuracy is 78.02%. The balanced accuracy of the model is 75.08%.

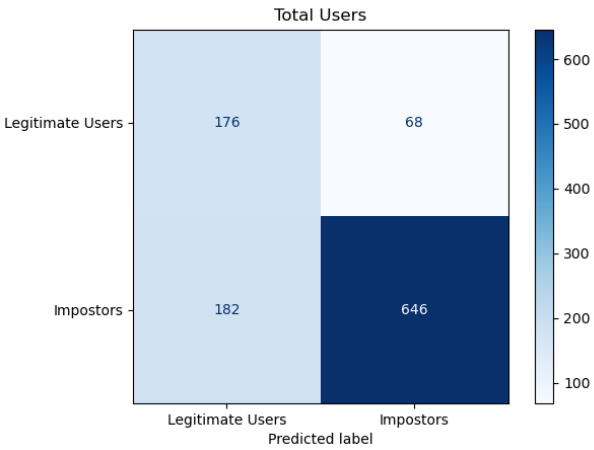


Figure 3.10. Confusion matrix representing impostors attacks conducted against all users.

The model can be fine-tuned depending on the specific needs and conditions, aligning with the desired system requirements. Adjusting the similarity threshold offers the flexibility to make the model more stringent or lenient in rejecting impos-

tors. However, this flexibility comes with a security trade-off between potentially rejecting legitimate users and accepting impostors.

To offer a comprehensive overview of the model's capabilities, another accuracy metric, the F_1 score, is employed to measure performance. The F_1 score metric provides valuable insights, particularly focusing on the model's behavior with impostors. The F_1 score is defined as follows:

$$F_1\ Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

where Precision is defined as:

$$Precision = \frac{TP}{TP + FP}$$

And Recall, or Sensitivity, is defined as:

$$Recall\ (Sensitivity) = \frac{TP}{TP + FN}$$

Model's F_1 score for impostor class is 84%, with a Recall of 78% and Precision of 90%.
This metrics is valuable in situations where accepting impostors is associated with a higher cost than rejecting legitimate users, as may be the case here. The F1 score provides a balanced assessment, considering both Precision and Recall, which is particularly useful when there is an imbalance in the costs or consequences of false positives and false negatives.

Chapter 4

Conclusion

This study examined the security robustness of EEG-based systems against impostor unveiled attacks. The proposed model demonstrates the ability to distinguish between legitimate users and impostors who have acquired knowledge or control over the user access target stimuli, attempting to replicate legitimate user behaviour. The model does not rely on exploiting the knowledge factor but is instead based on the inherent differences in signals produced by users. The model extracts distinctive features from the EEG signal and stores them as users fingerprints, which are subsequently utilized during the authentication phase to verify user identity. This approach ensures protection of users' privacy, scalability, efficiency, universality and flexibility. Users privacy is guarantee by avoiding the storage of EEG waves in raw form, thereby preventing undesired disclosure of confidential data. Storing fingerprints instead of raw data enhances computational and memory efficiency. Furthermore, fingerprints enable the model to easily generalize and accommodate new users, thereby satisfying the universality and scalability requirements. The model exhibit flexibility allowing adjustments to specific security requirements trough modification of the similarity threshold between the stored fingerprints and the presented ones. The authentication phase time in EEG-based systems can similarly be adjusted according to the specifications and security standards required.

4.1 Applications

The proposed system showcases potential for real-world application, leveraging the strengths of the employed model, the multi-factor authentication facilitated by the rapid serial visual presentation paradigm (which exploits the knowledge factor) and the inherent EEG advantages over traditional biometric features. The system can flexibly complement other traditional authentication system if a higher level of security is required. However, authentication phase time and preparation could potentially impede easy usage in environments that necessitate a light and fast authentication system. Despite the high portability of the EEG biometric feature, its adoption is limited, with only a few existing commercial and industrial applications. This limits could potentially hinder the development of trust and familiarity with these systems.

4.2 Future Developments

Potential future developments for the system include:

- Exploring different stimuli for the rapid serial visual presentation (RSVP) data recording, evaluating the performance of different type of target stimuli and acquiring more data to enhance the model capabilities.
- Integrate the standard EEG-based authentication system functionalities to construct a complete model.
- Implement real-time monitoring capabilities to detect and respond promptly to any suspicious or anomalous activities even after authentication phase has concluded, thereby increasing the system's overall security robustness.
- Develop a multi-class classification based model by replacing the autoencoder with a combination of CNN layers and feed forward fully connected layers.
- Integrating and combining different neural networks model architectures.

Bibliography

[1] M. Poulos, M. Rangoussi, V. Chrissikopoulos and A. Evangelou, "Person identification based on parametric processing of the EEG," ICECS'99. Proceedings of ICECS '99. 6th IEEE International Conference on Electronics, Circuits and Systems (Cat. No.99EX357), Paphos, Cyprus, 1999, pp. 283-286 vol.1, doi: 10.1109/ICECS.1999.812278.

[2] R. B. Paranjape, J. Mahovsky, L. Benedicenti and Z. Koles', "The electroencephalogram as a biometric," Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No.01TH8555), Toronto, ON, Canada, 2001, pp. 1363-1366 vol.2, doi: 10.1109/CCECE.2001.933649.

[3] Shiliang Sun, "Multitask learning for EEG-based biometrics," 2008 19th International Conference on Pattern Recognition, Tampa, FL, USA, 2008, pp. 1-4, doi: 10.1109/ICPR.2008.4761865.

[4] S. Marcel and J. D. R. Millan, "Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 743-752, April 2007, doi: 10.1109/TPAMI.2007.1012.

[5] K. Brigham and B. V. K. V. Kumar, "Subject identification from electroencephalogram (EEG) signals during imagined speech," 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 2010, pp. 1-8, doi: 10.1109/BTAS.2010.5634515.

[6] R. Palaniappan and P. Raveendran, "Individual identification technique using visual evoked potential signals", *Electron. Lett.*, vol. 38, no. 25, pp. 1634-1635, Dec. 2002. doi: 10.1049/el:20021104.

[7] Seul-Ki Yeom, Heung-Il Suk, Seong-Whan Lee, Person authentication from neural activity of face-specific visual self-representation, Pattern Recognition, Volume 46, Issue 4, 2013, Pages 1159-1169, ISSN 0031-3203. doi: 10.1016/j.patcog.2012.10.023.

[8] Y. Chen et al., "A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2635-2647, Dec. 2016, doi: 10.1109/TIFS.2016.2577551.

[9] Bidgoly, A.J., Bidgoly, H.J. & Arezoumand, Z. Towards a universal and privacy preserving EEG-based authentication system. *Sci Rep* 12, 2531 (2022). doi: 10.1038/s41598-022-06527-7.

[10] Saeidi M, Karwowski W, Farahani FV, Fiok K, Taiar R, Hancock PA, Al-Juaid A. Neural Decoding of EEG Signals with Machine Learning: A Systematic Review. Brain Sci. 2021 Nov 18;11(11):1525. doi: 10.3390/brainsci11111525. PMID: 34827524; PMCID: PMC8615531.

[11] Wu Q, Yan B, Zeng Y, Zhang C, Tong L. Anti-deception: reliable EEG-based biometrics with real-time capability from the neural response of face rapid serial visual presentation. Biomed Eng Online. 2018 May 3;17(1):55. doi: 10.1186/s12938-018-0483-7. PMID: 29724232; PMCID: PMC5934893.

[12] T. Piplani, N. Merill and J. Chuang, "Faking it, Making it: Fooling and Improving Brain-Based Authentication with Generative Adversarial Networks," *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Redondo Beach, CA, USA, 2018, pp. 1-7, doi: 10.1109/BTAS.2018.8698606.

[13] Jasper, H.H. (1958) The Ten-Twenty Electrode System of the International Federation. Electroencephalography and Clinical Neurophysiology, 10, 371-375.

[14] G.E. Chatrian, E. Lettich, P.L. Nelson Ten percent electrode system for topographic studies of spontaneous and evoked EEG activity Am J EEG Technol, 25 (1985), pp. 83-92.doi: 10.1080/00029238.1985.11080163.

[15] Guideline thirteen: guidelines for standard electrode position nomenclature. American Electroencephalographic Society. J Clin Neurophysiol. 1994 Jan;11(1):111-3. PMID: 8195414. doi: 10.1097/00004691-199401000-00014.

[16] Klem GH, Lüders HO, Jasper HH, Elger C. The ten-twenty electrode system of the International Federation. The International Federation of Clinical Neurophysiology. Electroencephalogr Clin Neurophysiol Suppl. 1999;52:3-6. PMID: 10590970.

[17] Nuwer MR, Comi G, Emerson R, Fuglsang-Frederiksen A, Guérit JM, Hinrichs H, Ikeda A, Luccas FJ, Rappelsburger P. IFCN standards for digital recording of clinical EEG. International Federation of Clinical Neurophysiology. Electroencephalogr Clin Neurophysiol. 1998 Mar;106(3):259-61. doi: 10.1016/s0013-4694(97)00106-5. PMID: 9743285.

[18] Nuwer MR, Comi G, Emerson R, Fuglsang-Frederiksen A, Guérit JM, Hinrichs H, Ikeda A, Luccas FJ, Rappelsberger P. IFCN standards for digital recording of clinical EEG. The International Federation of Clinical Neurophysiology. Electroencephalogr Clin Neurophysiol Suppl. 1999;52:11-4. PMID: 10590972.

[19] Oostenveld R, Praamstra P. The five percent electrode system for high-resolution EEG and ERP measurements. Clin Neurophysiol. 2001 Apr;112(4):713-9. doi: 10.1016/s1388-2457(00)00527-7. PMID: 11275545.

[20] Stergiadis, C.; Kostaridou, V.-D.; Veloudis, S.; Kazis, D.; Klados, M.A. A Personalized User Authentication System Based on EEG Signals. *Sensors* **2022**, *22*, 6929. doi: 10.3390/s22186929.

[21] Wu Q, Zeng Y, Zhang C, Tong L, Yan B. An EEG-Based Person Authentication System with Open-Set Capability Combining Eye Blinking Signals. Sensors (Basel). 2018 Jan 24;18(2):335. doi: 10.3390/s18020335. PMID: 29364848; PMCID: PMC5855894.

[22] Seul-Ki Yeom, Heung-Il Suk, Seong-Whan Lee, Person authentication from neural activity of face-specific visual self-representation, Pattern Recognition, Volume 46, Issue 4, 2013, Pages 1159-1169, ISSN 0031-3203, doi: 10.1016/j.patcog.2012.10.023.

[23] D. Bassett, M. Gazzaniga, Understanding complexity in the human brainTrends in Cognitive Sciences, 15 (5) (2011), pp. 200-209. doi: 10.1016/j.tics.2011.03.006 . PMID: 21497128

[24] James W. Tanaka, Tim Curran, Albert L. Porterfield, Daniel Collins; Activation of Preexisting and Acquired Face Representations: The N250 Event-related Potential as an Index of Face Familiarity. *J Cogn Neurosci* 2006; 18 (9): 1488–1497. doi: 10.1162/jocn.2006.18.9.1488. PMID: 16989550.

[25] Zhang Y, Li M, Shen H, Hu D. On the Specificity and Permanence of Electroencephalography Functional Connectivity. Brain Sci. 2021 Sep 24;11(10):1266. doi: 10.3390/brainsci11101266. PMID: 34679331; PMCID: PMC8722434.

[26] W. G. Lennox, E. L. Gibbs and F. A. Gibbs, "The brain-wave pattern an hereditary trait: Evidence from 74 normal pairs of twins", *J. Heredity*, vol. 36, no. 8, pp. 233-243, 1945. doi: 10.1093/oxfordjournals.jhered.a105509.

[27] Hinrichs, H., Scholz, M., Baum, A.K. *et al.* Comparison between a wireless dry electrode EEG system with a conventional wired wet electrode EEG system for clinical applications. *Sci Rep* 10, 5218 (2020). doi: 10.1038/s41598-020-62154-0.

[28] M. Samara, C. Farmaki, N. Zacharioudakis, M. Pediaditis, M. Krana and V. Sakkalis, "Comparison between dry and wet EEG electrodes in an SSVEP-based BCI for robot navigation," 2022 IEEE 22nd International Conference on Bioinformatics and Bioengineering (BIBE), Taichung, Taiwan, 2022, pp. 333-338, doi: 10.1109/BIBE55377.2022.00075.

[29] E Fiesler, Neural network classification and formalization, Computer Standards & Interfaces, Volume 16, Issue 3, 1994, Pages 231-239, ISSN 0920-5489, doi: https://doi.org/10.1016/0920-5489(94)90014-0.

[30] S. Keshishzadeh, A. Fallah and S. Rashidi, "Improved EEG based human authentication system on large dataset," 2016 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, Iran, 2016, pp. 1165-1169, doi: 10.1109/IranianCEE.2016.7585697.

[31] Amir Jalaly Bidgoly, Hamed Jalaly Bidgoly, Zeynab Arezoumand, A survey on methods and challenges in EEG based authentication, Computers & Security, Volume 93, 2020, 101788, ISSN 0167-4048, doi: 10.1016/j.cose.2020.101788.

[32] Pawan, Rohtash Dhiman, Machine learning techniques for electroencephalogram based brain-computer interface: A systematic literature review, Measurement: Sensors, Volume 28, 2023, 100823, ISSN 2665-9174, doi: 10.1016/j.measen.2023.100823.

[33] Xiaoqian Yan, Bruno Rossion, A robust neural familiar face recognition response in a dynamic (periodic) stream of unfamiliar faces, Cortex, Volume 132, 2020, Pages 281-295, ISSN 0010-9452, doi: 10.1016/j.cortex.2020.08.016.