mathematics

MDPI

Article

Cryptographic Algorithm Designed by Extracting Brainwave Patterns

Marius-Alin Dragu [1], Irina-Emilia Nicolae [2] and Mădălin-Corneliu Frunzete [2,*]

[1] Department of Bioengineering and Biotechnology Engineering, Faculty of Medical Engineering, National University of Science and Technology Politehnica, 060042 Bucharest, Romania; marius_alin.dragu@upb.ro
[2] Department of Applied Electronics and Information Engineering, Faculty of Electronics, Telecommunications and Information Technology, National University of Science and Technology Politehnica, 060042 Bucharest, Romania
* Correspondence: madalin.frunzete@upb.ro

Abstract: A new authentication method based on EEG signal is proposed here. Biometric features such as fingerprint scanning, facial recognition, iris scanning, voice recognition, and even brainwave patterns can be used for authentication methods. Brainwave patterns, also known as brain biometrics, can be captured using technologies like electroencephalography (EEG) to authenticate a user based on their unique brain activity. This method is still in the research phase and is not yet commonly used for authentication purposes. Extracting EEG features for authentication typically involves signal processing techniques to analyze the brainwave patterns. Here, a method based on statistics for extracting EEG features is designed to extract meaningful information and patterns from the brainwave data for various applications, including authentication, brain–computer interface systems, and neurofeedback training.

Keywords: user authentication; EEG signals; visual evoked potentials (VEPs); local neighbor descriptive pattern (LNDP); personalized electrode selection algorithm; machine learning

MSC: 94A60; 68P25

Citation: Dragu, M.-A.; Nicolae, I.-E.; Frunzete, M.-C. Cryptographic Algorithm Designed by Extracting Brainwave Patterns. *Mathematics* **2024**, *12*, 1971. https://doi.org/10.3390/math12131971

Academic Editor: Jonathan Blackledge

Received: 15 May 2024
Revised: 14 June 2024
Accepted: 19 June 2024
Published: 25 June 2024

1. Introduction

Over the past decade, the world has witnessed a paradigm shift in the widespread use of brain–computer interfaces (BCI) in both user authentication (UA) and user identification (UI) applications, the two having substantial similarities but different purposes. Thus, while authentication systems confirm or deny a user's identity, identification systems are used to find a person in a group [1,2]. In such a technology-driven society, traditional identifiers (ID cards or classic passwords) are being replaced by biometric identifiers (e.g., face, fingerprint, voice, or iris recognition). Biometric recognition refers to the automatic recognition of individuals based on physiological and/or behavioral traits [3].

Biometric systems have been used in various low-cost devices in recent years; for example, fingerprint/face recognition has been integrated into smartphones and computers [4,5]. Unlike traditional systems, biometrics are advantageous as the encryption key [6] is harder to compromise or duplicate [7]. However, a biometric system is vulnerable to a variety of attacks designed to undermine the integrity of the authentication process [8,9].

Similarly, personal identification through biometric systems has recently attracted the attention of the security research community. Thus, one of the main tools for security systems is the use of personal identification systems. The main spoofing methods used to attack the security of biometric systems and allow unauthorized persons to access other people's data include printing photos or printing 3D masks (for systems based on face recognition), playing a recorded signal in front of a speech recognition system, or presenting an eyeball to an iris scanner [10].

In view of these attacks, the design of new systems involves the identification of *unique* (distinct and unique to everyone), *permanent* (remains relatively constant for a long period of time), *universal* (all people possess those biometric traits and could use the system), and *collectable* (can be easily quantified through some type of collection process) traits [11]. These requirements form a representative pattern of whether a given biometric-based authentication system is reliable and useful [12]. In this context, such biometric systems can be developed using an authentication method based on cognitive traits, dependent on the autonomic nervous system, involving the acquisition of signals such as EEG (electroencephalogram) [13,14]. EEG signals can be described as distinctive, more difficult to be artificially generated, and reflect an internal and personal process that cannot be perceived by others [15]. Also, these are triggered by external stimuli, offering user-specific brainwave patterns. Different fields, such as healthcare and patient identification (enhancing the security of electronic health records), financial services (to secure online banking and financial transactions, adding an extra layer of protection), data centers and server rooms (securing critical data centers and server rooms where sensitive information is stored), electronic voting and ATM machine or private sectors, and different companies and government offices (in order to authenticate employees) can benefit from the results obtained in this new active research topic area represented by the study of EEG-based authentication and identification systems [16,17].

The paper is organized as follows. Section 2 presents the related research work on brainwave patterns-based biometric systems. Section 3, Materials and Methods, focuses on materials and methods, providing the concept of authentication and identification proposed system and detailing the algorithms and mathematical concepts related to channel selection, password generation (authentication stage) and user identification. A series of statistical techniques are introduced for the selection of representative channels and the investigation of medical data dynamics in relation to ensuring the uniqueness of users within the proposed system. Further, a brief overview of the analyzed database is presented in Section 4, Experimental design, including the brain signal acquisition protocol and the EEG montage. The main results related to system performance are addressed and discussed in Section 5, Results, underlying the security of proposed EEG-based biometric system. In Section 6, evaluation of proposed system results in terms of security analysis.

2. Literature Review

Over time, brainwave data have proven to be a suitable framework for designing biometric authentication systems. Researchers have proposed various methods to encrypt EEG signals, illustrating the tremendous potential of advanced algorithms and machine learning in behavioral pattern generation and recognition based on prior training. Beyrouthy et al. [18] describe it as a fusion approach that combines electroencephalography with Artificial Intelligence (AI) and the Internet of Things (IOT).

The majority of EEG biometric research uses EEG signals captured while the subject is in a resting state [19]. In this way, for the first time, Poulos et al. [20] successfully introduced EEG in the context of user authentication, without explicitly evaluating the security aspects from a biometric perspective. Under resting state eye-closed conditions, they obtained the EEG data from 4 users and 75 imposters. They obtained an accuracy score ranging from 72% to 78% when auto-regressive parameters and a Learning Vector Quantization network were used. Later, Chuang et al. [21] and Curran et al. [22] suggested a new algorithm for the authentication stage that checks whether the degree of similarity related to a user is higher than that with other users. This approach tends to ignore cases where someone is not registered in the system and may attempt to be authenticated instead of an authenticated user.

Stergiadis et al. [23] developed an EEG-based authentication method using the Auto-WEKA software package, which contains libraries and predefined functions in Java Script for implementing machine learning algorithms (ML). The authors proposed as a pattern descriptor vector with 15 spectral density characteristics of power. The reported average

results indicate an accuracy of 95%, a true positive rate (sensitivity) of 93%, and a true negative rate (specificity) of 93%. The dataset contains signals from 15 subjects during resting state, with eyes open, for a duration of 30 s, in which the participants were asked to keep their eyes open and focus on an "x"-shaped symbol appearing in the center of the screen.

Introducing external-stimuli-based protocols or mental activity protocols for brain signal acquisition is a common way to enhance identity authentication systems [24]. For example, the work of Sooriyaarachchi et al. [25] provides an overview of system authentication for smart devices that use brain waves recorded in the presence of an auditory stimulus (music). The data from 20 subjects were collected from users while they listened to two types of music: a famous song in English, and the person's favorite song. Random Forest classifiers based on 20 features extracted from EEG separated into sub-bands were designed for the user identification and verification stages. The reported results for these experiments were approximately 85% when involving a single channel in the authentication stage, and 95% when considering two electrodes.

Moreover, Damaševicius et al. [6] created a paradigm shift in this direction, merging the native cryptographic algorithms with EEG in a biometric system. The proposed algorithm was tested on a database consisting of 42 subjects, obtaining an average accuracy of 85%. The authors reported that for some subjects, the accuracy was quite low (45%), explaining this result as a mismatch between the subject and the BCI system, which is a phenomenon known as the *BCI illiteracy effect*. According to the literature, about 15–20% of people cannot control a brain–computer interface system with high accuracy [26].

Das et al. [27] proposed an unsupervised algorithm based on autoencoders to learn sparse feature representations to realize the person identification task. This was conducted in an open-source database containing motor imagery EEG signals from 109 subjects. The Autoencoder-CNN model yielded the highest recognition rate of 87% for task-based identification and 99% for resting state recognition. In addition, in their study, Seyfizadeh et al. [28], using the same dataset, designed a deep learning framework, specifically a neural network (ResNet) for the identification of distinct individuals based on their brainwaves. Considering both the time and frequency domain characteristics of the EEG signals, this model effectively reveals the intricate details present in the data, thereby improving the overall performance. The proposed approach produced an outstanding classification accuracy of 99% and an equal error rate of 0.41%.

Yap et al. [29] investigated the potential of developing an EEG biometric system using a self-collected database of eight participants and an SVM classifier. The subjects were asked to perform two tasks: resting state with eyes closed, and visual stimulation. The reported accuracy is 87–99% for the visual stimulation protocol and 83–96% for the resting state. Sabeti et al. [30] demonstrated that in terms of inter-subject variability, ERP (evoked related potential)-EEG data are a tremendous biomarker in person identification and verification systems compared with resting state EEG. To perform the person verification task, they used three methods, with the average accuracy for the ERP (P300) component as follows: 96% (k-nearest neighbor-kNN), 95% (SVM), and 97% (Random Forest). Moreover, the EER was estimated to be 0.02% (kNN) and 0.015% (SVM, Random Forest).

The EEG-based biometric procedure consists of an enrolment (authentication) and verification stage. In the enrolment process, one or more biometric traits of the individual person are compared to the configured biometric profile [31]. Therefore, the verification stage requires a one-to-one match to decide the results as a valid user or imposter. Currently, classification/deep learning methods are used to perform user verification [8]. In this way, the analyzed literature suggests the following limitations:

- **Database**: Most of the works that perform brain fingerprint extraction, and, in equal measure, the design of EEG-based authentication systems, use databases, designed for other purposes such as emotion recognition or character determination [32–34].
- **The protocol used in the EEG signals acquisition**: A remarkable number of papers discuss the opportunity to design an authentication system, using resting state EEG signals. The resting state is used for the identification of the user and is applied on a

larger scale as a source of reference. When designing a system for authentication, it is necessary to account that this approach does not allow for password reset or recovery. On a large scale, there are two such protocols used for acquisition, namely Rest Eyes Open (REO) and Rest Eyes Closed (REC) [12,35]. The main disadvantages of this protocol are the sensitivity of external stimuli, which can disturb users' attention, or the modification of signals generated, and artifacts generated by controlled or uncontrolled movements, such as blinking, as well as significantly affecting the accuracy of the system [3,36–38].

- **Channel selection**: The extraction of the representative channels is not based on a personalized algorithm [23,39].
- **Classification**: The most popular authentication mechanism relies on classification algorithms (number of classes = number of users) in order to gain access to the system. Such an approach, Single-Factor Authentication (SFA) [40], does not take into consideration the situations in which unknown persons outside of the database are trying to connect [1,33].

To overcome the aforementioned limitations, we propose a Two-factor authentication (2FA) system, namely authentication based on the generated password from EEG signals and identification using a one-vs-all classification algorithm, with each user having a trained LNDP descriptor- based model. Thus, the proposed system provides an additional level of protection against attacks, namely an identification stage confirming or rejecting the identity of the user whose password was previously accepted. Additionally, the identification phase restricts access to the system for users whose profiles have not been configured.

In this work, we also explored our database, consisting of 25 subjects, created for the purpose of designing an authentication system. In our experiment, the acquisition protocol is based on external visual stimuli, recording brain activity in response to the presentation of various images to each subject.

Protocols based on external stimuli involve the acquisition, preprocessing, and processing of EEG signals obtained following the presentation of a stimulus. Compared to resting EEG acquisition, resetting user credentials can be accomplished by changing the stimulus source. Additionally, this protocol may require frequent password resets due to changes in brain activity over time. Visual evoking potentials (VEP)/steady state visual evoked potential (SSVEP), rapid serial visual presentation (RSVP), and sound-based protocols are examples of paradigms used in external stimulus-based protocols.

Visual evoked potential (VEP) is the most used category of ERP, according to statistical data reported in [22]. Resetting the user's credentials, in terms of repeating the enrollment step, is carried out with a different stimulus, as the brain's response to a given stimulus changes over time. In such scenarios, a password reset can only be carried out by replacing the incentives. Protocols based on external stimuli require repeated measurements of brain activity to achieve classification algorithms of a high accuracy of.

Therefore, the presence of visual stimuli elicits unique and distinct brain responses between subjects, enabling the reset of user credentials by applying different images. Considering that protocols based on external stimuli require repeated measurements of brain activity to achieve high algorithm accuracy, each subject was presented with 25 categories of images (hobbies/personal images), with each category containing 32 images.

3. Materials and Methods

3.1. System Overview

The proposed system, created according to the personality and uniqueness of users, is shown in Figure 1, and is divided into two phases: authentication and identification. To make a personalized selection of representative channels, a statistical algorithm was developed. In the authentication stage, for each subject, the password match validator is computed (validating the generated and system-stored password when the profile of user is configured with the password when a participant tries to connect). In the identification stage, in order to enhance system security, a LNDP (Local Neighbor Descriptive Pattern)

descriptor-based machine learning model is trained, which is a measure that aims to design an additional layer of user identify verification.

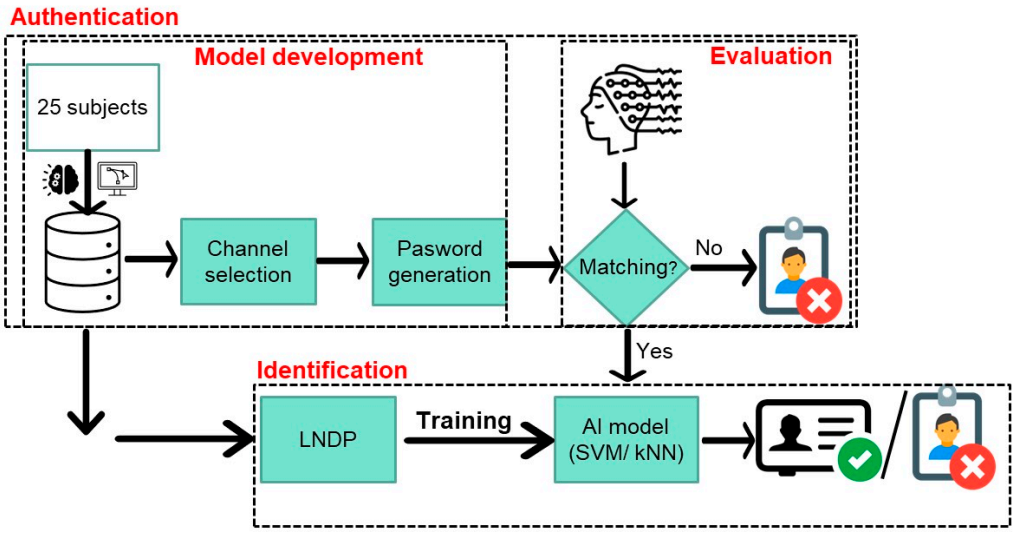

Figure 1. General structure of EEG-based authentication and identification system.

3.2. Preprocessing

In the preprocessing stage, we filtered the raw data with a Notch filter having a center frequency of 50 Hz to remove the power line interference, and subsequently, we applied Independent Component Analysis, to reject the artifacts embedded in the data (e.g., eye blinks or eye movements). Data were cleaned and analyzed offline, using MATLAB (R2022b).

3.3. Channel Selection

Knowing that the presence of a large number of channel recordings increases the computational complexity of processing signals and the risk of overfitting, a channel selection based on maximum variance [41] is performed in this area. In order to make a custom selection, we implemented a statistical algorithm. First of all, for each subject, for the EEG signal corresponding to each image (I_n) which is displayed, we calculated the variance as follows:

$$Var_{I_n}(c) = \frac{1}{k}\sum_{i=1}^{k}(x(i) - \mu(c))^2 \quad (1)$$

where x, μ, and k are the EEG data, mean, and number of samples of the data acquired on channel c, respectively.

The channel with maximum variance is selected from each recording I_n as follows:

$$C_n = \underset{c}{argmax}\ Var_{I_n}(c) \quad (2)$$

Subsequently, for each channel, we computed the probability of being selected as follows:

$$h(i) = \frac{1}{T}\sum_{n=1}^{T}\delta(C_n - i), \quad (3)$$

where i = the number of channels (1, 2, 3, . . ., 33) and T = total number of recordings.

In the end, we selected the first N channels, so that the cumulative probability is greater than the threshold (0.7). Figure 2 depicts the stages of this algorithm.

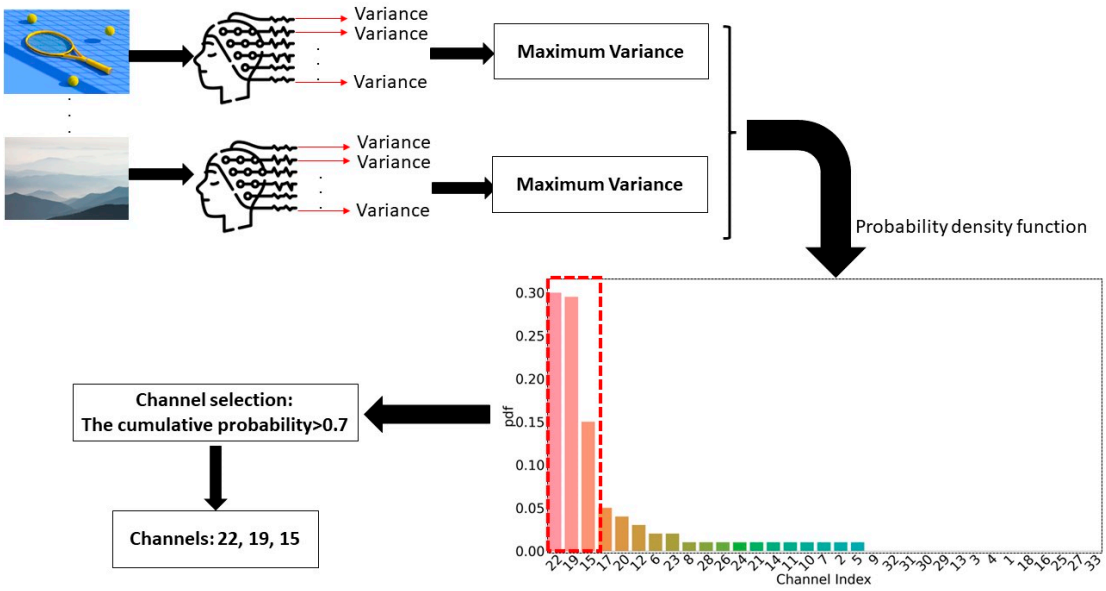

Figure 2. The flowchart of channel selection algorithm.

3.4. Password Generation

Different features were extracted and analyzed to generate a password based on EEG signal. The features (Table 1) which proved the uniqueness between inter-subjects were used as input in our algorithm. Given that the EEG signal is non-stationary, it is very important to be analyzed in both the temporal and frequency domains. The train set consists of 80% of the total samples of each participant, as these models only need positive samples. The uniqueness notion is described hereunder.

Table 1. The list of EEG features analyzed in this work.

Category		Feature	Definition
a. The extracted and analyzed features in time domain.			
Time domain (t.d)	1	Average	The arithmetic mean of EEG samples
	2	Median	The middle value when the samples are arranged in ascending order
	3	Standard Deviation	The dispersion relative to the mean
	4	Variance	A measure of dispersion around the mean
	5	Skewness	A measure of asymmetry
	6	Kurtosis	A measure of a distribution's tails
	7	Number of waves	
	8	Zero-crossing rate	The number of times that signal crosses the horizontal axis
	9	Minimum	The minimum value of EEG signal
	10	Maximum	The maximum value of EEG signal
	11	Minimum arguments	Inidices of the minimum values
	12	Maximum arguments	Inidices of the maximum values
	13	Activity	A measure of the squared standard deviation of the amplitude of the signal
	14	Peak-to-peak amplitude	The difference between the highest and the lowest values in a waveform
	15	Mean square	The arithmetic mean of squared amplitude values
	16	Mobility	The square root of the activity of the first derivative of the signal divided by the activity of the signal
	17	Complexity	The ratio between the mobility of the first derivative and the mobility of the signal
	18	Energy	The sum of squared amplitude values

Table 1. *Cont.*

Category		Feature	Definition
b. The extracted and analyzed features in frequency domain.			
Frequency domain (f.d)	19	Average	
	20	Median	
	21	Standard Deviation	The dispersion relative to the mean
	22	Variance	A measure of dispersion around the mean
	23	Skewness	A measure of asymmetry
	24	Kurtosis	A measure of a distribution's tails
	25	δ	Relative power of δ-band (0.5–4 Hz)
	26	θ	Relative power of θ-band (4–8 Hz)
	27	α	Relative power of α-band (8–12 Hz)
	28	β	Relative power of β -band (12–30 Hz)
	29	γ	Relative power of β-band (>30 Hz)
	30	σ	Relative power of σ-band (12–14Hz)
	31	β/α	
	32	θ/α	
	33	θ/β	
	34	γ/δ	The ratios between relative power bands
	35	$(\theta+\alpha)/\beta$	
	36	$(\theta+\alpha)/(\alpha+\beta)$	
	37	$(\gamma+\beta)/(\gamma+\alpha)$	
Entropies	38	Shannon Entropy	A measure of randomness in the EEG signal
Nonlinear	39	Lyapunov Exponent	A measure to determine chaotic behavior

As a next step, we computed across all subjects, for each feature, the first quartile (Q1), the upper (third) quartile (Q3), the inter-quartile range (IQR), defined as:

$$\text{IQR} = [\text{Q1}, \text{Q3}] \tag{4}$$

Targeting the identifying of features that underline the uniqueness of EEG signal, we applied Algorithm 1 and Figure 3.

Algorithm 1. Identification of uniqueness descriptors

Input: The extracted features, for all subjects
For each feature:

1. The overlap degree between interquartile ranges, corresponding to subjects i and j is calculated:
$$\theta^{k}_{overlap}(i,j) = \frac{Range\left(IQR_i \cap IQR_j\right)}{Range(IQR_i)} 100[\%] \tag{5}$$
A symmetric matrix, θ^k, of dimension (25, 25) is obtained for each feature k.
2. The rate of values $\theta^{k}_{overlap}(i,j) < 30\%$, p^k is determined.
3. A feature is validated as a descriptor of uniqueness if $p^k \geq 70\%$

Output: The selected features

The procedure used to processing EEG signal in order to generate the password for each of the participants is shown next (Algorithm 2 and Figure 4).

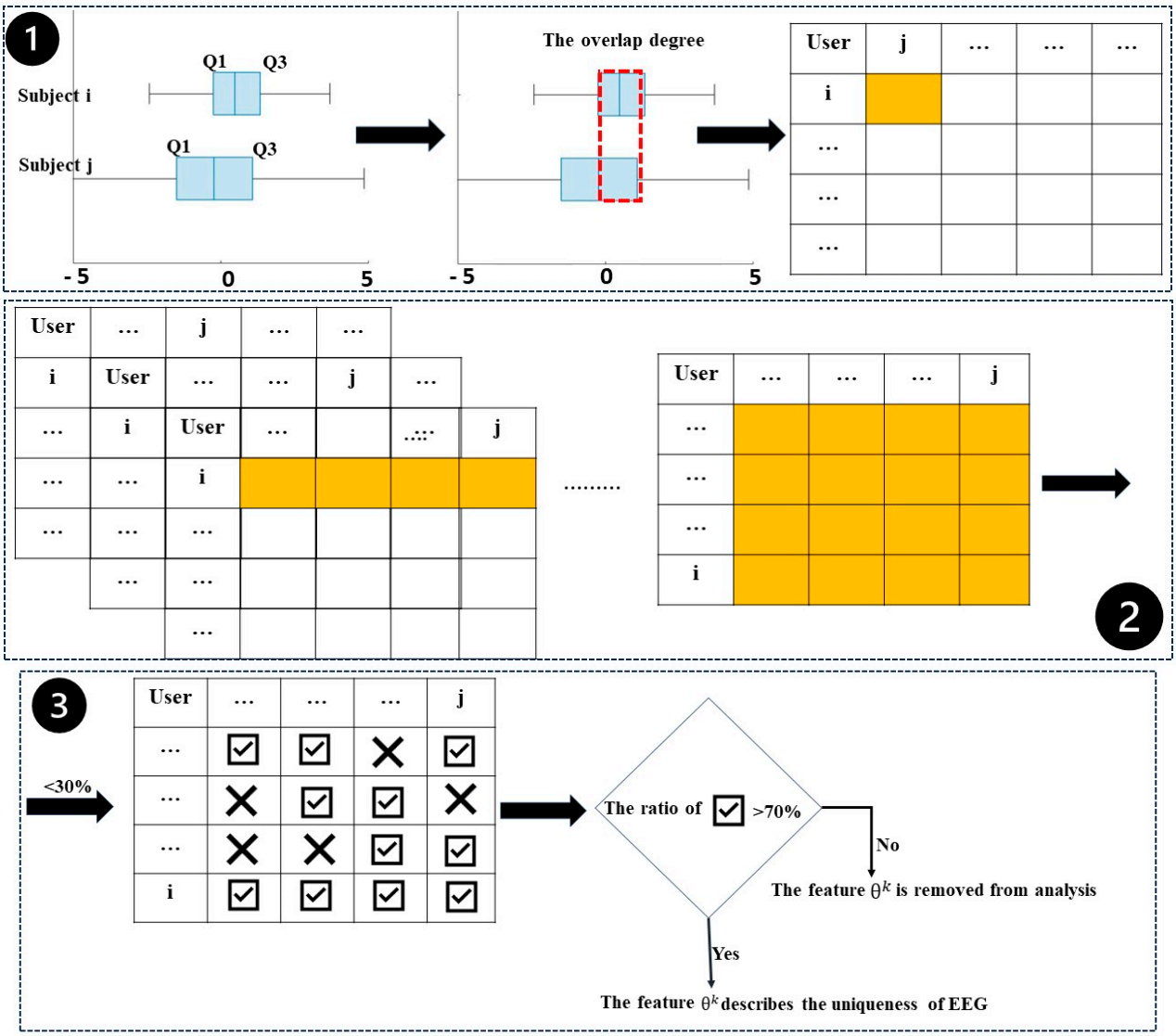

Figure 3. The flowchart of finding features used descriptors of uniqueness.

Algorithm 2. Processing EEG signals for password generation

Input: The selected features

For each feature that was selected as a descriptor:

1. The minimal value of Q1, m_Q, and maximal value of Q3, M_Q, are computed considering all analyzed EEG signals.
2. For the range $[m_Q, M_Q]$, a uniform quantizer is applied with P levels; $P = 2^p$.
3. For each subject, the probability density function for the values v_i obtained when the quantization is applied.
4. Further on, the value v_i with maximum probability, l, is determined. The binary representation of l using p bits is saved for the next steps.

Output: The value v_i with maximum probability with maximum probability for selected features (for each subject)

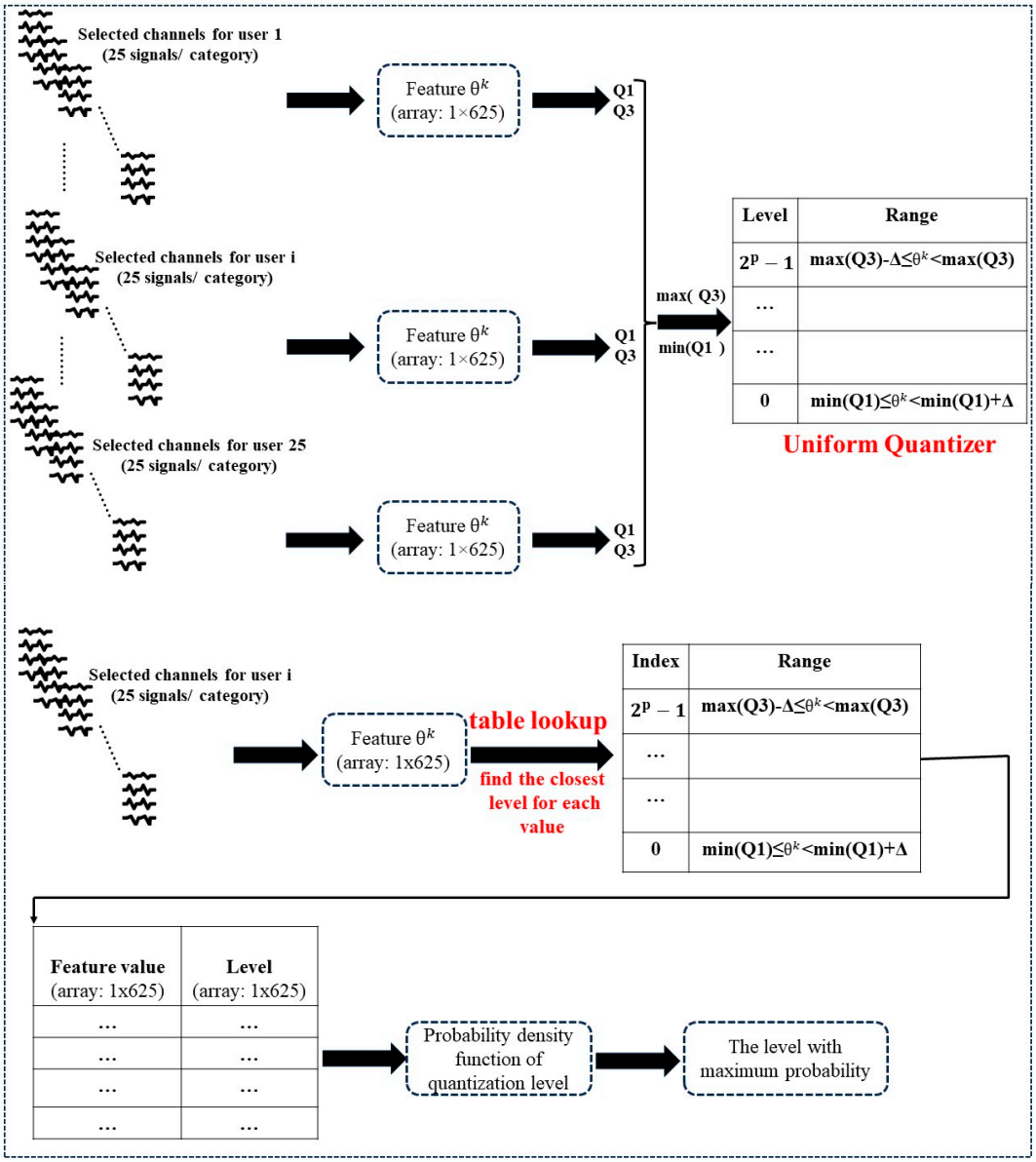

Figure 4. The flowchart of password generation algorithm.

Furthermore, for each subject we employed a distinctive model of linear/polynomial regression, to prove the uniqueness of EEG signals. For each of them, we found a specific pair of features which can be fitted by a regression model having $R^2 > 0.9$. Simultaneously, our research was concentrated on finding some regression models that can be applied to all subjects. These can contribute to developing a service, like "reCAPTCHA", which protects the biometric system against various attacks (e.g., artificial EEG signals, noise signals, errors caused by non-compliance with the protocol conditions by users) designed to undermine integrity.

Finally, the password will be represented as a vector with $(\varphi + 1) \times p$ elements (Figure 5) where φ represents the number of selected features (Θ^k) as a descriptor of uniqueness. Each element is shown as a binary digit. The first p elements are initialized to 1, corresponding to the identified model regression; otherwise, the elements having an index between $ip + 1$ and $(i + 1)p$ contain the binary representation of l, for feature Θ^i, with $i = 1, 2, 3, \ldots, \varphi - 1, \varphi$. Also, for each attempt, the identified regression equation will be verified. If the error is lower than 5%, the first p bits are equal to 1; otherwise, they are equal to 0.

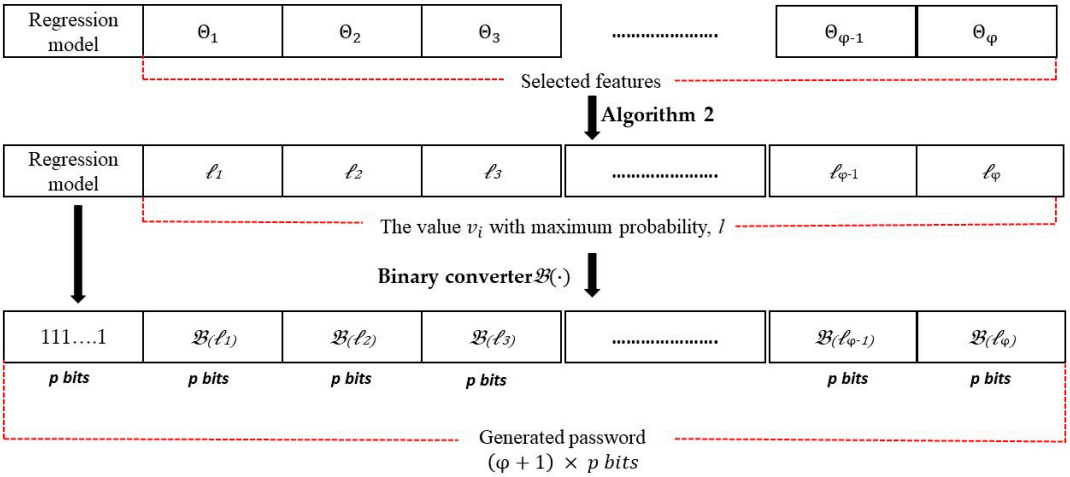

Figure 5. Password generation framework.

3.5. User Authentication

The user authentication scheme proposed here is addressed to an algorithm designed with a symmetric cryptosystem. To define the requirements for the authentication process, we performed the password matching using Hamming distance, H, defined as follows:

$$H = \frac{1}{(\varphi+1)\cdot p} \sum_{i=1}^{(\varphi+1)\cdot p} \mathcal{P}_i \oplus \mathcal{A}_i, \tag{6}$$

where $\mathcal{P}$ represents the password generated by the proposed algorithm (stored in the data base) and $\mathcal{A}$ is the generated password when a participant tries to connect φ and p with the same meaning as in previous paragraphs. Moreover, $\mathcal{P}_i$ and $\mathcal{A}_i$ represents the value for the bit placed at index i; $\oplus$ is the bitwise XOR operator.

One can easily notice that H represents a way to evaluate the number of comparisons in which the corresponding bits are different. To analyze the similarities at the bit level, Equation (6) is as follows:

$$\overline{H} = \frac{1}{(\varphi+1)\cdot p} \sum_{i=1}^{(\varphi+1)\cdot p} \overline{\mathcal{P}_i \oplus \mathcal{A}_i}, \tag{7}$$

In this way, the authentication problem is described by finding the optimal value of $\overline{H}$, $\overline{H}^*$, so that a claim of a participant to log in will be authorized if $\overline{H} \geq \overline{H}^*$. Consequently, $\overline{H}^*$ will be treated as a threshold value.

3.6. User Identification

Closely related to the concept of authentication, another important topic is previously described, discussed in the following paragraphs: identification (Figure 6). In order to increase the security of the EEG-based system, a machine learning algorithm is integrated. The great advantage of this approach is that the identity of the user, whose password has been accepted by the system in the authentication stage, is verified by the designed algorithm, reducing the error rate in this process.

In this way, the problem of user identification is approached as one of one-vs.-all classification, producing a model for each subject. According to the characteristics of EEG, we adopt two different classification methods to obtain a better result: SVM (Support Vector Machine) and kNN (k-Nearest Neighbors). These are widely used in this field [1]. The input vector for these algorithms is based on Local Neighbor Descriptive Pattern (LNDP), described in [42]. To compute 1D-LNDP, we considered 8 neighboring points. Therefore, each sample from the EEG signal, was encrypted on 8 bits, the range for the decimal value, thus obtained, being between 0 and 255, like uniform quantization on images (256 gray

levels). In this case, the 80/20 rule was applied. The proportion of positive and negative samples in each set is defined as 50%.

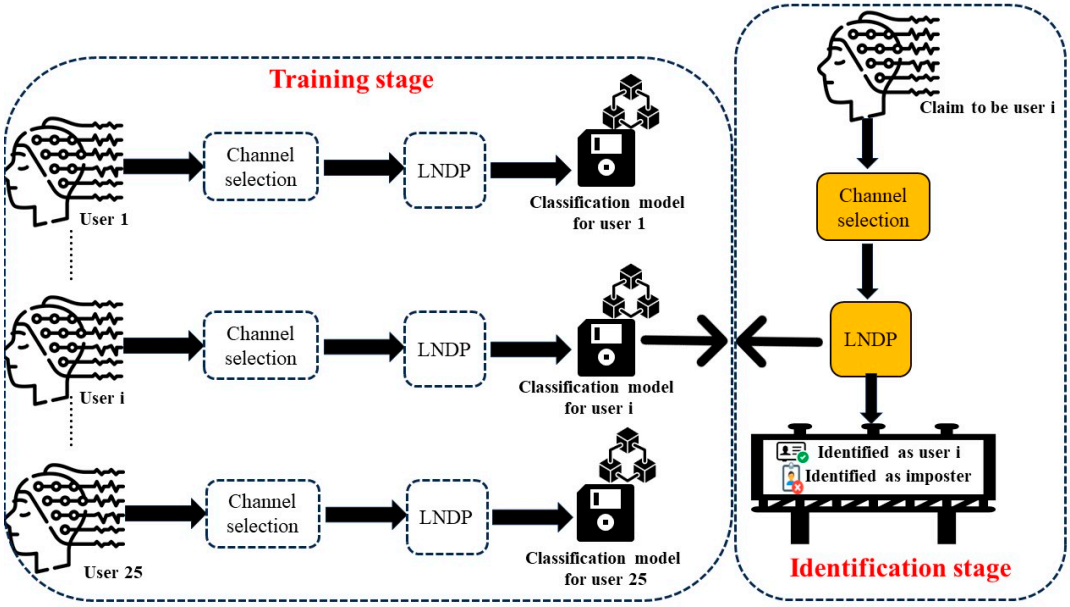

Figure 6. The identification stage pipeline.

After all signal points' transformation codes have been computed, the histogram is extracted as follows:

$$v_1 = \gamma\ (LNDP), \tag{8}$$

where $\gamma(\cdot)$ represents the histogram extraction function and v_1 the result of histogram extractions (256 bins).

Next, we computed the down-sampling local neighbor descriptive pattern, at level 2, 3, 4. the down sampling-1D method is presented in [43]. So, mathematically:

$$\begin{cases} v_2 = \vartheta(LNDP) \\ v_3 = \vartheta(v_2), \\ v_4 = \vartheta(v_3) \end{cases} \tag{9}$$

where $\vartheta(\cdot)$ represents the down-sampling LNDP function and v_2, v_3, v_4 down-sampling one-dimensional local neighbor descriptive pattern, at level 2, 3, 4.

Finally, the features that will serve as input for SVM/kNN algorithm will be as follows: v_1, v_3, v_4 and the average, median, maximum, minimum, variance, kurtosis, and skewness of v_2.

3.7. Evaluation Metrics

The general biometric system performance is given by the specific parameters, namely false acceptance rate (*FAR*), false rejection rate (*FRR*), and equal error point (*ERR*) which are defined hereunder.

False acceptance rate quantifies the number of attempts in which an imposter is identified as a valid user.

$$FAR = \frac{FA}{IA}, \tag{10}$$

where *FA* is the number of false acceptances (the situations in which a claim of an imposter as an authorized user is validated by the system) and *IA* is the total number of imposter test samples (imposter attempt).

False rejection rate represents a way to evaluate the number of attempts in which a valid user is recognized as an imposter by the system.

$$FRR = \frac{FR}{AA}, \tag{11}$$

where FR is the number of false rejections (the situations in which a claim of a valid user to be identified is rejected by the system) and AA the total number of user test samples (authorized attempt).

Equal error point is defined as a unique point so that the previously described parameters, FAR and FRR, are equal. A lower EER is associated with a high accuracy. So, mathematically, we obtain the following:

$$EER = \arg\left[FAR(\Psi) = FRR(\Psi)\right] \tag{12}$$

In addition, sensitivity, specificity and accuracy can be defined as follows:

$$Sensitivity = 1 - FRR = \frac{TA}{AA}, \tag{13}$$

where TA is the number of correct acceptances (the situations in which a claim of a valid user to be identified is accepted by the system).

$$Specificity = 1 - FAR = \frac{TR}{IA}, \tag{14}$$

where TR is the number of correct rejections (the situations in which a claim of an imposter as an authorized user is rejected by the system).

$$Accuracy = \frac{C}{T}, \tag{15}$$

where C is the number of correct decisions (valid user/imposter) and T is the total number of test samples.

The implementation of described methodology was made in MATLAB 2022b on an Intel (R) Pentium (R) Gold 7505, running at 2.00 GHz, 20 GB RAM in Windows 11.

4. Experimental Design

The database used for this study comprises EEG signals (visual evoked potentials), from 25 subjects, acquired using a 1000 Hz sampling frequency, on 33 channels, in monopolar montage, with mastoid reference. The electrodes were distributed according to the extended 10–20 system of Nebraskan's 128-channels Quick-Cap (this system is seen in Figure 7, with the used electrodes depicted as filled black circles). During data collection, the room's ambient parameters were quiet, soundproofed, with an external environment, fresh air movement, and no substantial electromagnetic interference.

In the course of the acquisition session, different images, representing general hobbies (e.g., animals, food, travel, reading), are displayed to the subjects. These were grouped into 32 categories, with each category having 32 images, and were shown in the same order to all subjects. Therefore, for each image, our pipeline acquisition, depicted in Figure 8, adheres to the following 2.5 s inter-stimulus interval (ISI): 1 s blank gray screen and 1.5 s exposure to different visual stimuli (images). For capturing the complete temporal dynamics of neural responses before and after the stimuli, the signals were divided into 3 s epochs as follows: 0.5 s (blank gray screen before displaying the image), 1.5 s (displaying the image), and 1 s (blank gray screen after displaying the image). The interval stimuli period was tailored in relation to the cognitive process involved, namely working memory, attention, and imagination, as suggested in the literature at around 2 s [44,45], and, at the same time, was intended to be comfortable for the user. An initial test was performed with users with varying stimuli lengths and the most comfortable ISI duration was, on average, 2.5 s.

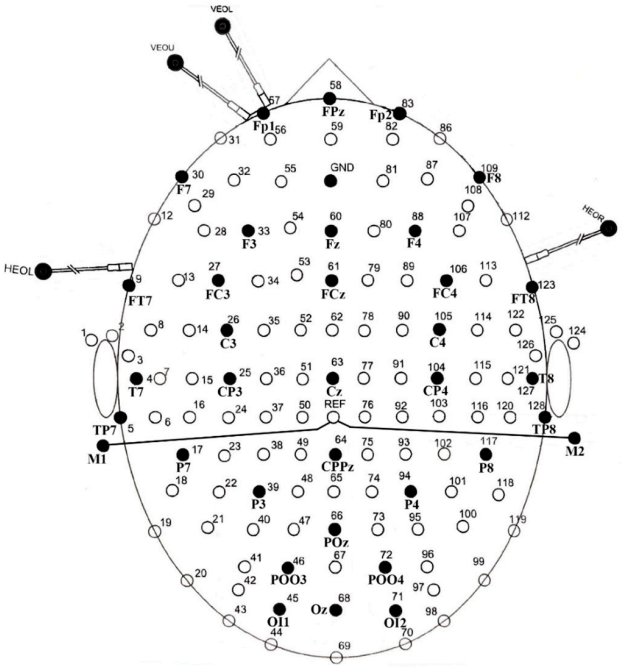

Figure 7. The 10–20 electrode placement EEG recording system (the used electrodes are represented as filled black circles).

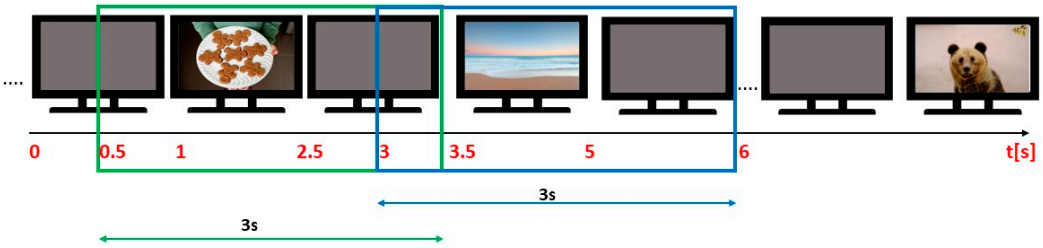

Figure 8. EEG recording pipeline.

The dataset is stored and labeled, subject files being organized, according to the following format 1 × 32 cell, and each cell (corresponding to image categories) 33 × 2999 × 32, 50, where 33 the represents number of channels, 2999 represents the number of samples, and 32 represents the number of images from a category. Moreover, each category was labelled by the user, having a three-point Likert scale (1: dislike, 2: neutral, 3: like).

5. Results

5.1. Channel Selection

The results of the channel selection are collated in Table 2. As can be observed, a diversity is identified regarding the electrodes marked as representative, as each subject presents a different set of extracted channels compared to the others.

In Figure 9, you can see the probability distribution function (pdf) of selected electrodes. The most frequently chosen channels were found to be PO_Z, F_Z, POO_4, CPP_Z, P_4, FCz, and Oz. Looking at the spatial mapping of these electrodes, we can say that this result is related to cognitive states, specifically to the signal acquisition protocol used, such as concentration, attention, vision, and sensory integration.

Table 2. The selected channels for analyzed subjects.

Subject	The Number of Selected Channels	Selected Channels
1	4	F_Z, PO_Z, FC_4, FC_3
2	2	FC_Z, C_Z
3	2	POO_4, O_Z
4	6	CPP_Z, F_Z, P_4, PO_Z, C_4, FC_Z
5	1	CPP_Z
6	4	P_4, PO_Z, CPP_Z, F_Z
7	2	P_4, PO_Z
8	5	P_4, PO_Z, CPP_Z, C_Z, F_Z
9	4	POO_4, PO_Z, CPP_Z, FC_Z
10	2	CP_3, CP_4
11	8	FP_2, F_Z, FC_Z, PO_Z, C_Z, P_3, F_4, FP_Z
12	4	PO_Z, POO_4, CPP_Z, P_4
13	6	PO_Z, P_4, POO_4, CPP_Z, O_Z, C_Z
14	4	PO_Z, F_Z, POO_4, CPP_Z
15	4	PO_Z, F_Z, CPP_Z, C_Z
16	6	PO_Z, F_Z, C_4, FC_Z, C_3, POO_4
17	5	POO_4, P_4, FC_Z, OI_2, PO_Z
18	3	F_Z, PO_Z, C_4
19	3	PO_Z, C_3, POO_4
20	4	F_Z, PO_Z, POO_3, POO_4
21	4	F_Z, PO_Z, FC_Z, POO_4
22	2	O_Z, POO_3
23	3	O_Z, PO_Z, POO_3
24	3	PO_Z, C_4, OI_1
25	3	TP_7, FP_2, F_7

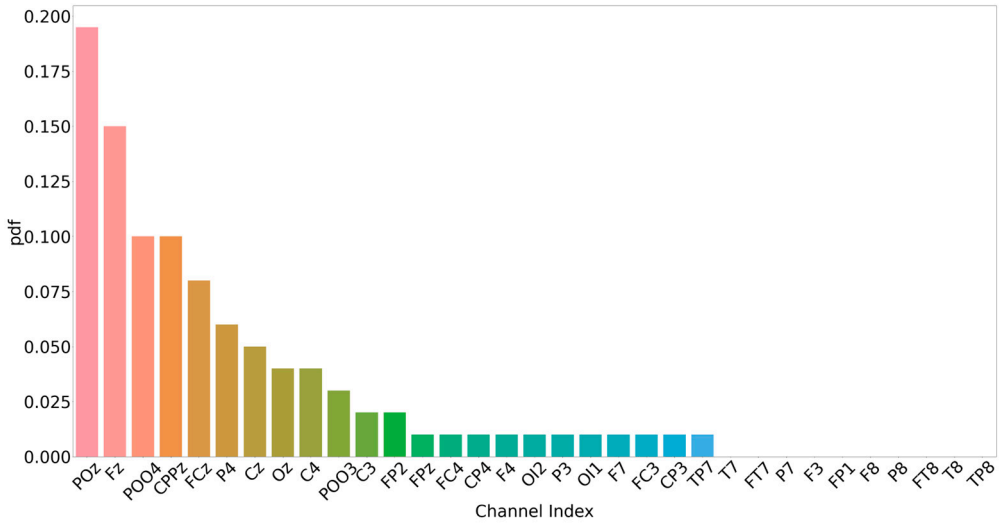

Figure 9. Selected channel distribution (considering all subjects).

5.2. Password Generation

For establishing the features which describe the uniqueness, we applied Algorithm 2 and investigated p^k values (Figure 10—the index on the x-axis is referenced to Table 1). It can be noticed that the features selected (red bars) for use in the password generation stage are as follows: variance, standard deviation, peak-to-peak distance, mean square and energy (time-domain); for the frequency domain, the selected features are as follows: average, variance, standard deviation, relative power of the β-band (12–30 Hz), and relative power of the γ-band (>30 Hz).

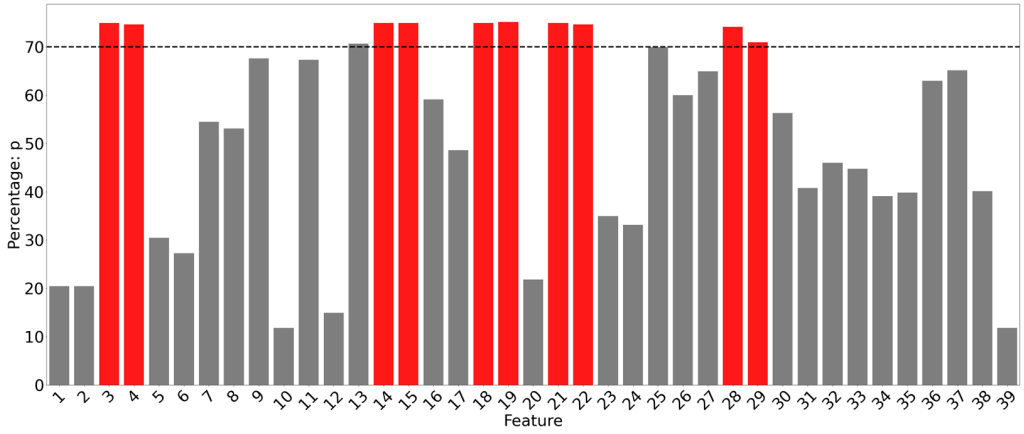

Figure 10. p^k value for each feature and selected features as descriptors of uniqueness (red bars).

Table 3 presents the pair of features, fitted by a regression model (linear/polynomial so that R^2 is maximized).

Table 3. The identified regression model for each subject.

Subject	Features	The Applied Regression Model	R^2
1	Complexity—Lyapunov Exponent	Polynomial (degree 7)	0.97
2	Relative power of β-band–Variance (f.d)	Linear	0.98
3	$(\theta + \alpha)/\beta - (\theta + \alpha)/\beta$ (relative power ratios)	Linear	0.98
4	Relative power of δ–band–Variance (f.d)	Polynomial (degree 4)	0.98
5	Mobility—Lyapunov Exponent	Linear	0.97
6	Relative power of σ-band–Relative power of β-band	Linear	0.96
7	Relative power of α-band–Standard deviation (f.d)	Polynomial (degree 2)	0.99
8	Relative power of β-band–Minimum	Linear	0.95
9	Mean (f.d)–Square mean	Polynomial (degree 2)	0.98
10	Minimum–Maximum	Polynomial (degree 2)	0.97
11	Relative power of γ-band–Variance (t.d)	Linear	0.93
12	$\theta/\beta - (\theta + \alpha)/\beta$ (relative power ratios)	Linear	0.97
13	Relative power of θ-band–Standard deviation (f.d)	Polynomial (degree 5)	0.98
14	Mean (f.d)–Peak-to-peak distance	Polynomial (degree 2)	0.98
15	Relative power of σ-band–Relative power of γ-band	Polynomial (degree 2)	0.98
16	Mean (f.d)–Energy	Polynomial (degree 2)	0.93
17	Square mean–Maximum value	Linear	0.91
18	Standard deviation (f.d)–Maximum value	Linear	0.97
19	Zero crossing rate–Mobility	Polynomial (degree 2)	0.98
20		Linear	0.92
21	Relative power of σ-band–Standard deviation (f.d)	Linear	0.97
22	Relative power of θ-band–Standard deviation (f.d)	Linear	0.97
23	Relative power of α-band–Variance (f.d)	Linear	0.96
24	Relative power of β-band–Standard deviation (t.d)	Linear	0.94
25	Relative power of θ-band–Relative power of σ-band	Linear	0.99

Regarding the regression models, that can be applied to all subjects, we identified the following pair of highly correlated features: variance (t.d)–mean square, mean square–variance (t.d), and standard deviation (t.d)–peak-to-peak distance.

Considering the database organization, for each subject, a group consisting of three passwords is generated, corresponding to the labels of visual stimuli (like/dislike/neutral). Finally, the most suitable types of images which should be displayed to the user will be chosen, so that the system has the highest performance; in terms of accuracy, this is either FAR or FRR.

Taking into account the fact that we selected $\varphi = 10$ features as descriptors of uniqueness and a quantization was realized on 16 levels ($p = 4$), each password will be represented as a vector having 11 (10 features + 1 identified correlation) $\times$ 4 = 44 bits.

In order to compute H^*, we calculated FAR and FRR for different proposed threshold values and proposed the following scenarios:

Scenario 1: Authentication can be achieved if the password is verified at the level of at least one selected channel. The FAR and FRR curves are shown in Figure 11a. The intersection point is: (32, 0.038); we can say that ERR = 0.038 for the threshold value of 32.

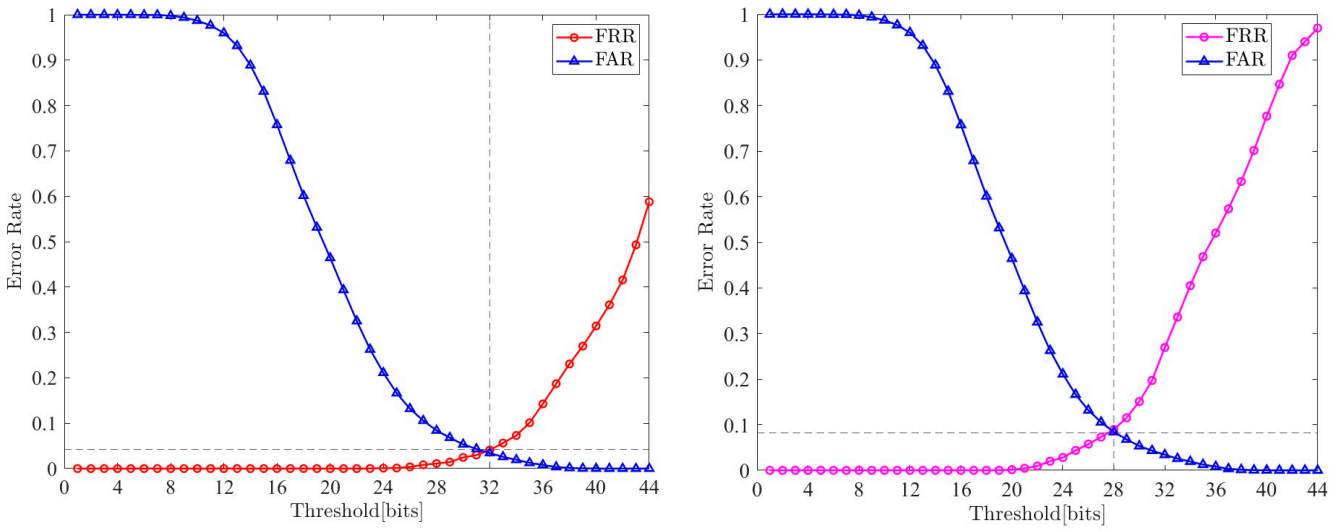

Figure 11. FAR and FRR. Authentication is performed if the password is verified at the level of at least one selected channel (**a**) and at least two selected channels (**b**).

Scenario 2: Authentication can be achieved if the password is verified at the level of at least two selected channels. The FAR and FRR curves are depicted in Figure 11b. In this case, ERR = 0.084 and the threshold value is 28.

Analyzing these results, it can be seen that in the first case, the EER is lower (0.038 vs. 0.084) and the threshold value is higher (32 vs. 28 bits). The main aim of this stage is to minimize the false rejection rate, the identification stage limiting the authentication of imposters and enhancing the overall performance. Also, in order to increase the system security, it is very important to set a threshold value as high as possible: lowering H^* will make the system more tolerant (FAR will increase) and increasing H^* will make the system more secure (FAR will decrease) [16]. By taking these facts into account, one can easily find the authentication requirements of $H^* = 32$, (meaning that up to $44 - 32 = 12$ bits of error are tolerated) as a necessary condition to be fulfilled at the level of at least one selected channel.

We can obtain a mean sensitivity (equivalent to mean true acceptance rate, TAR) of 0.89, and mean specificity (expressed by mean true rejections rate) of 0.97. Figure 12 depicts the distribution of overall sensitivity, specificity, and accuracy by violin plots.

Figure 13 shows the cumulative distribution function (cdf) for system accuracy after the authentication stage (red) and after the identification stage (blue). One can see that after the authentication stage, in 20% of subjects, the accuracy is lower than 88%, while in the final, the minimal value is 88%. Also, for 50% of the subjects, the initial accuracy is higher than 90.5%, while in the final, higher than 92.5%. Therefore, the improvement of overall accuracy by including the identification algorithm is clearly noticed. Important percentage differences, in this representation, are observed, especially in the first part of the range (corresponding to the values near the lower limit). Also, the mean overall accuracy after the first stage is 92%, while in the end, it is 93.50%.

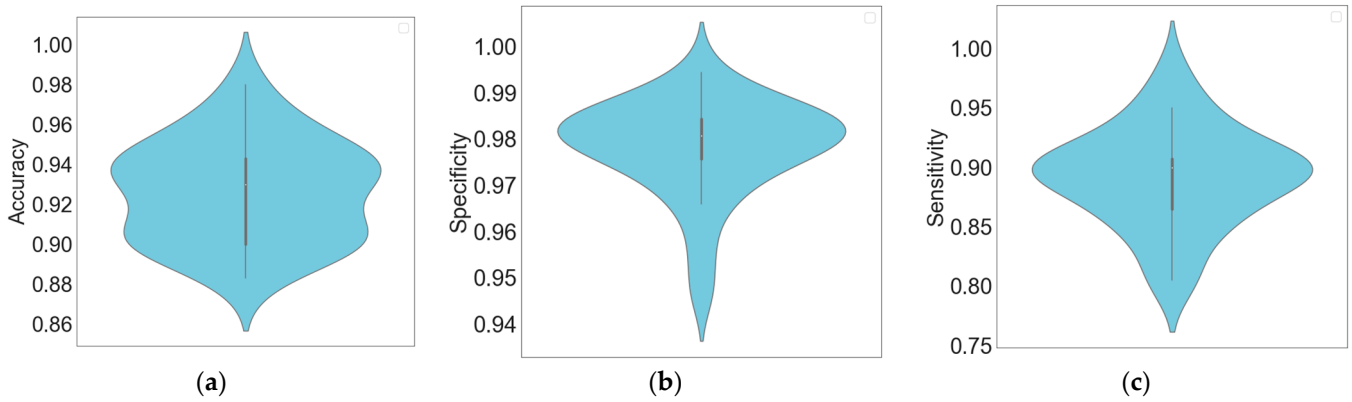

Figure 12. System performance (violin plots): accuracy (**a**), specificity (**b**), and sensitivity (**c**).

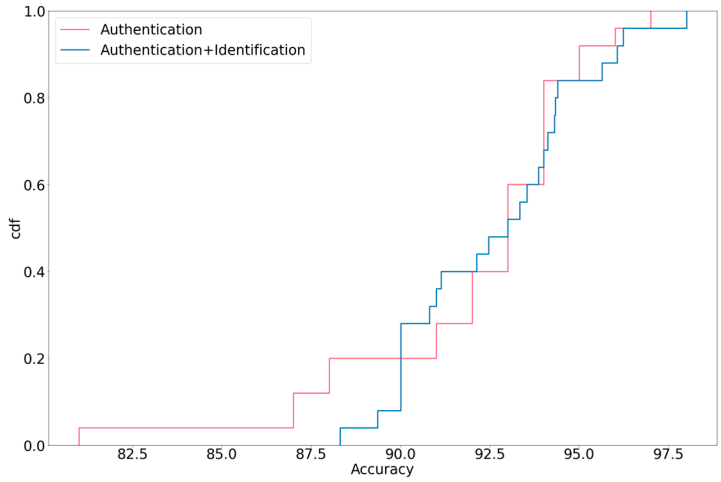

Figure 13. Cumulative distributive plot of accuracy.

Figure 14a exposes the accuracy for each of the subjects. It can be noticed that while overall accuracy was increasing following the addition of the machine learning one-vs.-all classification algorithm for user identification, for some subjects a decrease was recorded. To explain this idea, we analyze the system performance in terms of FAR and TAR.

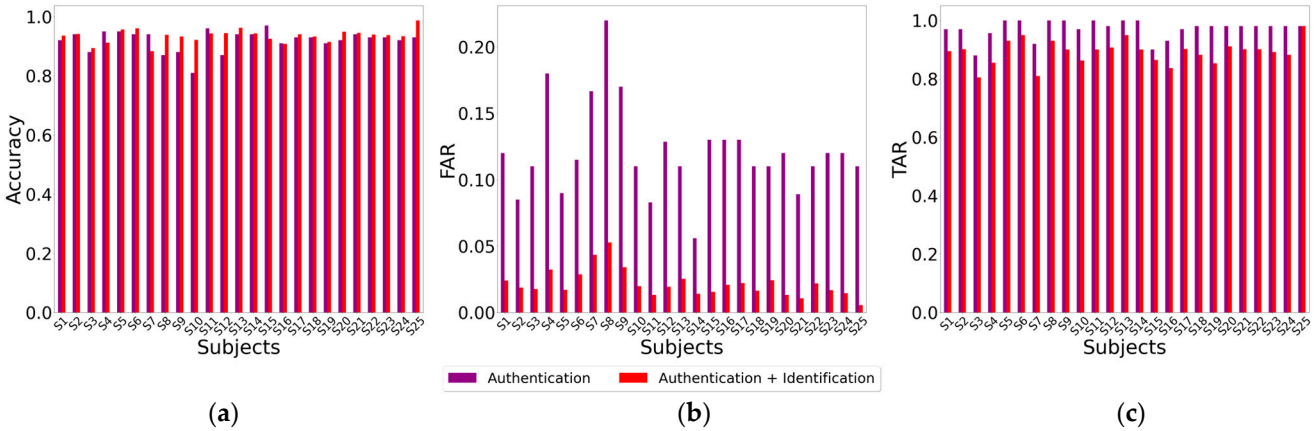

Figure 14. Accuracy (**a**), FAR (**b**) and TAR (**c**) for each subject: after the authentication stage (purple) and the identification stage (red).

Regarding the FAR parameter, Figure 14b demonstrates a remarkable improvement, showing that this system is strongly resistant to imposter attacks. One can find that the ratio between the authentication and identification stage accuracy is 0.12/0.02 = 6, which

means the number of false authorizations was reduced by approximately 6 times. The TAR parameter (Figure 14c) slightly decreased when the identification stage was added (average values: 0.97 vs. 0.90), as a result of the fact that the classification algorithm implemented does not offer 100% sensitivity, but no major differences are identified. In the light of the security measures and design requirements, these results can be considered accepted, the system reliably preventing impostors from gaining access as an authorized user.

To compare the performance of the proposed system with other relevant recognition technologies, a series of characteristics, namely universality, uniqueness, collectability, and permanence, was analyzed (Table 4):

Table 4. Comparison with other biometric technologies; ■—high; ▲—medium; ○—low; n/a—not available.

Biometrics	Universality	Uniqueness	Collectability	Permanence	Paper	Sample Size	Performance
Face	■	○	▲	○	[46]	40	Accuracy: Group: 88%, Individual: 75%
					[47]	48	Accuracy: 98%
ECG	■	○	■	▲	[48]	1020	False positive rate: 0.39% False negative rate: 1.57%
Fingerprint	■	■	■	■	[49]	10	Accuracy: 70%
Voice	▲	○	▲	○	[50]	10	Accuracy: 94%
					[51]	330	Accuracy: 93%
Iris eye movement	■	■	▲	▲	[52]	8	Accuracy: 89%
					[53]	24	Accuracy: 79%
					[54]	109	Accuracy: 85%
Posture pattern	▲	○	▲	○	[55]	30	True positive rate:91% False positive rate: 033% False negative rate: 8.68%
Wrist movement	■	○	○	▲	[56]	20	Accuracy: 85%
Our work	▲	■	▲	n/a		25	Accuracy: 93.5%

Also, for each subject, according their feedback, the types of images (like/dislike/neutral) which maximize the results, in terms of analyzed metrics, are identified. The obtained result has a major influence in the system configuration, because the images to be presented to the subject are chosen so that the performance of the application is maximized (Figure 15).

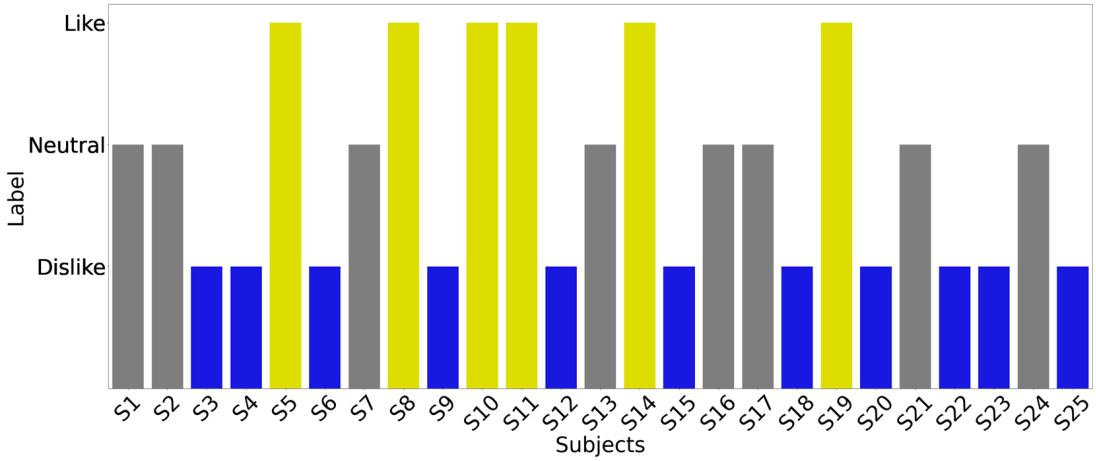

Figure 15. The most suitable types of images should be displayed to the users so that the results are maximized (yellow bars—like, gray bars—neutral, blue bars—dislike).

6. Security Analysis

The proposed brainwave-based biometric system does not store the password combination set but preserves the pattern obtained after the EEG processing (for the authentication stage) and the AI model (for the identification stage). Thus, considering the aforementioned testing scenarios, our login mechanism is robust to a false acceptance attack (defined as the case in which the system overrides processing and decision data because descriptors have an increased degree of similarity, accepting the user even though they are not the intended user). Also, the proposed system is robust to presentation attack and hill climbing attack (a form of brute force attack). For this type of attack, various instruments (such as camera, mask, silicone fingerprints, or synthetic voice generations) cannot impersonate the system because brainwave signals are unique, as we have demonstrated in this paper. Moreover, the EEG recording protocol (visual evoked potential) contributes in a fundamental and decisive way to system's resistance against this type of attacks, users cannot control these. According to [57], other recognition factors such as fingerprint, face, voice, and iris are vulnerable to enumerated profiles of imposters.

Otherwise, the implemented two-factor mechanism creates a strong resistance to the mentioned sources of vulnerability. Compared to SMS-based 2FA or time-based one-time passwords where an attacker can intercept the code (man-in-the-middle attack), successful authentication is achieved by the results of the machine learning algorithm, in the identification stage. After logging with predefined credentials (more specifically, username and EEG-based password), the personalized one-vs.-all classifier, built on specific descriptors, verifies the identity, without necessitating transmitting a code over the network or generating it via device.

7. Conclusions

The focus of this research has been on the configuration of an authentication and identification application based on the brain fingerprint.

Universality, *uniqueness*, *collectability* and *permanence* are the criteria used for designing the fingerprint-based authentication and identification proposed system. The authentication process is based on the recording and processing of visual evoked potentials (images), so it cannot be used by blind or severely neurologically impaired/visually impaired people. By using tactile or sound stimuli, the proposed algorithm can be used by people with different pathologies that make visual evoked potentials acquisition impossible; thus, *universality* is achieved.

The second requirement, *uniqueness*, was at the core of this work, since to extract the brain fingerprint means to determine a template applicable only to that subject. All approaches, namely channel selection, feature extraction for password configuration, and implementation of user identification algorithms, were subject-centered and aimed at maximizing inter-subject variation. The robustness of the system is supported on one hand by the authentication application, and on the other by the identification application. The performance, expressed in terms of a false acceptance rate of 0.025, true acceptance rate of 0.89, or accuracy: of 0.93, underlines, in a promising way, the significantly increased resistance to possible impostors after the identification stage. Moreover, these results are supported by the remarkable results obtained, worthy of comparison with the ones present in the literature. Table 5 shows a comparison of our method with previous studies.

The issue of *permanence* remains uncertain, as the literature does not report approaches to the study of the stationarity of the brain fingerprint and EEG signals, and there are no databases created for this purpose. Considering the fourth requirement, *collectability*, there are several limitations as it requires the use of high-performance equipment (the EEG headset). Also, the electrodes must be placed in approximately the same position each time, which requires end-user training.

Table 5. Comparison of statistical metrics with the existing approaches.

Work	Method	Accuracy (%)	FAR	FRR
	Proposed method	**93.50**	**0.025**	**0.021**
[23]	**Classification procedure:** the algorithm "WEKA"	95.60	0.023	0.023
[24]	**Classification procedure:** CNN	92.40	0.067	0.021
[8]	**Classification procedure:** SVM	98.00		
[6]	**Cryptographic algorithms**	89.50		0.026
[7]	**Cryptographic algorithms**	96.23	0.003	0.0003

To sum up, this paper presents a novel approach for EEG-based authentication and identification designing, considering essential concepts such as the *two-factor authentication (2FA)* system, resistance to the imposter attacks, and personalized algorithms. EEG-based authentication and EEG-based identification have been addressed singularly before in the literature, and it is well known that combining these methods can contribute to enhancing the system performance. The promising advantage of the thinking flow proposed in this article is users' improved power to control their data as well as the increased security and privacy.

Finally, regarding the future directions, the study of the stationarity of the brain fingerprint is considered, as it represents a milestone in the validation of the algorithm and the system. It should be considered whether the presence of fatigue or stress states fundamentally modifies the system performance. Also, the fact that the analysis has only been performed at the extraction feature level may not fully exploit the performance of the proposed customized system, which can be further improved by introducing features related to microstates analysis. Another direction should consider the database organization, finding a pattern for each image category.

Author Contributions: Methodology, M.-A.D. and M.-C.F.; Software, M.-A.D.; Validation, M.-A.D., I.-E.N. and M.-C.F.; Resources, M.-A.D.; Writing—original draft, M.-A.D.; Writing—review & editing, M.-A.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a grant from the National Program for Research of the National Association of Technical Universities—GNAC ARUT 2023.

Data Availability Statement: The data will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bidgoly, A.J.; Bidgoly, H.J.; Arezoumand, Z. A survey on methods and challenges in EEG based authentication. *Comput. Secur.* **2020**, *93*, 101788. [CrossRef]
2. Kotiuchyi, I.; Pernice, R.; Popov, A.; Faes, L.; Kharytonov, V. A framework to assess the information dynamics of source EEG activity and its application to epileptic brain networks. *Brain Sci.* **2020**, *10*, 657. [CrossRef]
3. TajDini, M.; Sokolov, V.; Kuzminykh, I.; Ghita, B. Brainwave-based authentication using features fusion. *Comput. Secur.* **2023**, *129*, 103198. [CrossRef]
4. Kaur, B.; Singh, D.; Roy, P.P. A Novel framework of EEG-based user identification by analyzing music-listening behavior. *Multimedia Tools Appl.* **2016**, *76*, 25581–25602. [CrossRef]
5. Kumar, P.; Saini, R.; Kaur, B.; Roy, P.P.; Scheme, E. Fusion of neuro-signals and dynamic signatures for person authentication. *Sensors* **2019**, *19*, 4641. [CrossRef]
6. Damaševičius, R.; Maskeliūnas, R.; Kazanavičius, E.; Woźniak, M. Combining Cryptography with EEG Biometrics. *Comput. Intell. Neurosci.* **2018**, *2018*, 1867548. [CrossRef]
7. Abdel-Ghaffar, E.A.; Daoudi, M. Personal authentication and cryptographic key generation based on electroencephalographic signals. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 101541. [CrossRef]
8. Hernández-Álvarez, L.; Barbierato, E.; Caputo, S.; Mucchi, L.; Encinas, L.H. EEG Authentication System Based on One- and Multi-Class Machine Learning Classifiers. *Sensors* **2022**, *23*, 186. [CrossRef]
9. Sun, Y.; Lo, F.P.-W.; Lo, B. EEG-based user identification system using 1D-convolutional long short-term memory neural networks. *Expert Syst. Appl.* **2019**, *125*, 259–267. [CrossRef]

10. Wang, M.; Hu, J.; Abbass, H.A. BrainPrint: EEG biometric identification based on analyzing brain connectivity graphs. *Pattern Recognit.* **2020**, *105*, 107381. [CrossRef]
11. Huang, G.; Hu, Z.; Chen, W.; Zhang, S.; Liang, Z.; Li, L.; Zhang, L.; Zhang, Z. M3CV: A multi-subject, multi-session, and multi-task database for EEG-based biometrics challenge. *NeuroImage* **2022**, *264*, 119666. [CrossRef] [PubMed]
12. Zhang, R.; Yan, B.; Tong, L.; Shu, J.; Song, X.; Zeng, Y. Identity Authentication Using Portable Electroencephalography Signals in Resting States. *IEEE Access* **2019**, *7*, 160671–160682. [CrossRef]
13. Zhao, H.; Chen, Y.; Pei, W.; Chen, H.; Wang, Y. Towards online applications of EEG biometrics using visual evoked potentials. *Expert Syst. Appl.* **2021**, *177*, 114961. [CrossRef]
14. Kong, W.; Wang, L.; Xu, S.; Babiloni, F.; Chen, H. EEG Fingerprints: Phase Synchronization of EEG Signals as Biomarker for Subject Identification. *IEEE Access* **2019**, *7*, 121165–121173. [CrossRef]
15. Salama, G.M.; El-Gazar, S.; Omar, B.; Hassan, A.A. Multimodal cancelable biometric authentication system based on EEG signal for IoT applications. *J. Opt.* **2023**, 1–15. [CrossRef]
16. Harakannanavar, S.S.; Renukamurthy, P.C.; Raja, K.B. Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends. *Int. J. Adv. Netw. Appl.* **2019**, *10*, 3958–3968. [CrossRef]
17. Zhang, B.; Chai, C.; Yin, Z.; Shi, Y. Design and implementation of an EEG-based learning-style recognition mechanism. *Brain Sci.* **2021**, *11*, 613. [CrossRef] [PubMed]
18. Beyrouthy, T.; Mostafa, N.; Roshdy, A.; Karar, A.S.; Alkork, S. Review of EEG-Based Biometrics in 5G-IoT: Current Trends and Future Prospects. *Appl. Sci.* **2024**, *14*, 534. [CrossRef]
19. Oikonomou, V.P. Human Recognition Using Deep Neural Networks and Spatial Patterns of SSVEP Signals. *Sensors* **2023**, *23*, 2425. [CrossRef]
20. Poulos, M.; Rangoussi, M.; Chrissikopoulos, V.; Evangelou, A. Person Identification Based on Parametric Processing of the EEG. In Proceedings of the ICECS '99, 6th IEEE International Conference on Electronics, Circuits and Systems (Cat. No. 99EX357), Paphos, Cyprus, 5–8 September 1999.
21. Chuang, J.; Nguyen, H.; Wang, C.; Johnson, B. LNCS 7862—I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves. In *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers 17*; Springer: Berlin/Heidelberg, Germany, 2013.
22. Curran, M.T.; Merrill, N.; Chuang, J.; Gandhi, S. One-step, three-factor authentication in a single earpiece. In Proceedings of the UbiComp/ISWC 2017—Adjunct Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers, Maui, HI, USA, 11–15 September 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 21–24. [CrossRef]
23. 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. [CrossRef]
24. 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* **2018**, *18*, 335. [CrossRef] [PubMed]
25. Sooriyaarachchi, J.; Seneviratne, S.; Thilakarathna, K.; Zomaya, A.Y. MusicID: A Brainwave-Based User Authentication System for Internet of Things. *arXiv* **2020**, arXiv:2006.01751. [CrossRef]
26. Vidaurre, C.; Blankertz, B. Towards a Cure for BCI Illiteracy. *Brain Topogr.* **2009**, *23*, 194–198. [CrossRef] [PubMed]
27. Das, B.B.; Ram, S.K.; Babu, K.S.; Mohapatra, R.K.; Mohanty, S.P. Person identification using autoencoder-CNN approach with multitask-based EEG biometric. *Multimedia Tools Appl.* **2024**, 1–21. [CrossRef]
28. Seyfizadeh, A.; Peach, R.L.; Tovote, P.; Isaias, I.U.; Volkmann, J.; Muthuraman, M. Enhancing security in brain computer interface applications with deep learning: Wavelet transformed electroencephalogram-based user identification. *Expert Syst. Appl.* **2024**, *253*, 124218. [CrossRef]
29. Yap, H.Y.; Choo, Y.H.; Yusoh, Z.I.M.; Khoh, W.H. Person authentication based on eye-closed and visual stimulation using EEG signals. *Brain Inform.* **2021**, *8*, 21. [CrossRef] [PubMed]
30. Sabeti, M.; Boostani, R.; Moradi, E. Event related potential (ERP) as a reliable biometric indicator: A comparative approach. *Array* **2020**, *6*, 100026. [CrossRef]
31. Merrill, N.; Curran, M.T.; Gandhi, S.; Chuang, J. One-step, three-factor passthought authentication with custom-fit, in-ear EEG. *Front. Neurosci.* **2019**, *13*, 354. [CrossRef] [PubMed]
32. Wen, D.; Jiao, W.; Li, X.; Wan, X.; Zhou, Y.; Dong, X.; Lan, X.; Han, W. The EEG signals encryption algorithm with K-sine-transform-based coupling chaotic system. *Inf. Sci.* **2023**, *622*, 962–984. [CrossRef]
33. Tasci, G.; Loh, H.W.; Barua, P.D.; Baygin, M.; Tasci, B.; Dogan, S.; Tuncer, T.; Palmer, E.E.; Tan, R.-S.; Acharya, U.R. Automated accurate detection of depression using twin Pascal's triangles lattice pattern with EEG Signals. *Knowl.-Based Syst.* **2023**, *260*, 110190. [CrossRef]
34. Ben Salem, S.; Lachiri, Z. CNN-SVM approach for EEG-Based Person Identification using Emotional dataset. In Proceedings of the 2019 International Conference on Signal, Control and Communication, SCC 2019, Hammamet, Tunisia, 16–18 December 2019; Institute of Electrical and Electronics Engineers Inc.: Piscataway Township, NJ, USA, 2019; pp. 241–245. [CrossRef]
35. Fidas, C.A.; Lyras, D. A Review of EEG-Based User Authentication: Trends and Future Research Directions. *IEEE Access* **2023**, *11*, 22917–22934. [CrossRef]
36. Cheng, S.; Wang, J.; Sheng, D.; Chen, Y. Identification With Your Mind: A Hybrid BCI-Based Authentication Approach for Anti-Shoulder-Surfing Attacks Using EEG and Eye Movement Data. *IEEE Trans. Instrum. Meas.* **2023**, *72*, 2505814. [CrossRef]

37. Zhang, S.; Sun, L.; Mao, X.; Hu, C.; Liu, P. Review on EEG-Based Authentication Technology. *Comput. Intell. Neurosci.* **2021**, *2021*, 5229576. [CrossRef]
38. Di, Y.; An, X.; He, F.; Liu, S.; Ke, Y.; Ming, D. Robustness Analysis of Identification Using Resting-State EEG Signals. *IEEE Access* **2019**, *7*, 42113–42122. [CrossRef]
39. Wan, X.; Zhang, K.; Ramkumar, S.; Deny, J.; Emayavaramban, G.; Ramkumar, M.S.; Hussein, A.F. A Review on Electroencephalogram Based Brain Computer Interface for Elderly Disabled. *IEEE Access* **2019**, *7*, 36380–36387. [CrossRef]
40. Petcu, A.; Pahontu, B.; Frunzete, M.; Stoichescu, D.A. A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2231. [CrossRef]
41. Alotaiby, T.; El-Samie, F.E.A.; Alshebeili, S.A.; Ahmad, I. A review of channel selection algorithms for EEG signal processing. *EURASIP J. Adv. Signal Process.* **2015**, *2015*, 66. [CrossRef]
42. Jaiswal, A.K.; Banka, H. Local pattern transformation based feature extraction techniques for classification of epileptic EEG signals. *Biomed. Signal Process. Control* **2017**, *34*, 81–92. [CrossRef]
43. Kuncan, F.; Kaya, Y.; Kuncan, M. A novel approach for activity recognition with down-sampling 1D local binary pattern features. *Adv. Electr. Comput. Eng.* **2018**, *19*, 35–44. [CrossRef]
44. Zickerick, B.; Thönes, S.; Kobald, S.O.; Wascher, E.; Schneider, D.; Küper, K. Differential Effects of Interruptions and Distractions on Working Memory Processes in an ERP Study. *Front. Hum. Neurosci.* **2020**, *14*, 84. [CrossRef]
45. Proverbio, A.M.; Pischedda, F. Measuring brain potentials of imagination linked to physiological needs and motivational states. *Front. Hum. Neurosci.* **2023**, *17*, 1146789. [CrossRef] [PubMed]
46. Wati, V.; Kusrini, K.; Al Fatta, H.; Kapoor, N. Security of facial biometric authentication for attendance system. *Multimed. Tools Appl.* **2021**, *80*, 23625–23646. [CrossRef]
47. Bisogni, C.; Castiglione, A.; Hossain, S.; Narducci, F.; Umer, S. Impact of Deep Learning Approaches on Facial Expression Recognition in Healthcare Industries. *IEEE Trans. Ind. Inform.* **2022**, *18*, 5619–5627. [CrossRef]
48. Louis, W.; Komeili, M.; Hatzinakos, D. Continuous Authentication Using One-Dimensional Multi-Resolution Local Binary Patterns (1DMRLBP) in ECG Biometrics. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2818–2832. [CrossRef]
49. Golec, M.; Gill, S.S.; Bahsoon, R.; Rana, O. BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0. *IEEE Consum. Electron. Mag.* **2022**, *11*, 51–56. [CrossRef]
50. Srivastava, S.; Chandra, M.; Sahoo, G. Speaker identification and its application in automobile industry for automatic seat adjustment. *Microsyst. Technol.* **2018**, *25*, 2339–2347. [CrossRef]
51. Kamiński, K.A.; Dobrowolski, A.P.; Piotrowski, Z.; Ścibiorek, P. Enhancing Web Application Security: Advanced Biometric Voice Verification for Two-Factor Authentication. *Electronics* **2023**, *12*, 3791. [CrossRef]
52. Ma, Z.; Yang, Y.; Liu, X.; Liu, Y.; Ma, S.; Ren, K.; Yao, C. EmIr-Auth: Eye Movement and Iris-Based Portable Remote Authentication for Smart Grid. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6597–6606. [CrossRef]
53. Harezlak, K.; Blasiak, M.; Kasprowski, P. Biometric identification based on eye movement dynamic features. *Sensors* **2021**, *21*, 6020. [CrossRef]
54. Zhang, Y.; Juhola, M. On Biometrics With Eye Movements. *IEEE J. Biomed. Health Inform.* **2016**, *21*, 1360–1366. [CrossRef]
55. Kaczmarek, T.; Ozturk, E.; Tsudik, G. Assentication: User Deauthentication and Lunchtime Attack Mitigation with Seated Posture Biometric. *arXiv* **2017**, arXiv:1708.03978.
56. Mare, S.; Markham, A.M.; Cornelius, C.; Peterson, R.; Kotz, D. ZEBRA: Zero-effort bilateral recurring authentication. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; Institute of Electrical and Electronics Engineers Inc.: Piscataway Township, NJ, USA, 2014; pp. 705–720. [CrossRef]
57. Wells, A.; Usman, A.B. Privacy and biometrics for smart healthcare systems: Attacks, and techniques. *Inf. Secur. J. A Glob. Perspect.* **2023**, *33*, 307–331. [CrossRef]