electronics

MDPI

Article

The Effect of Ironic Process Theory on Brain Signal-Based Encryption for IoT Devices

Ahmet Furkan Aydogan [1], Cihan Varol [1,*], Narasimha Karpoor Shashidhar [1], Amar Rasheed [1], Van Vung Pham [1] and Murat Karabatak [2]

[1] Department of Computer Science, Sam Houston State University, Huntsville, TX 77340, USA; axa184@shsu.edu (A.F.A.); nks001@shsu.edu (N.K.S.); axr249@shsu.edu (A.R.); vxp030@shsu.edu (V.V.P.)
[2] Department of Computer Science, Firat University, Elazig 23119, Turkey; mkarabatak@firat.edu.tr
* Correspondence: cvarol@shsu.edu

Abstract: Numerous encryption methods have been published to secure IoT devices in the last decade. Existing encryption methods still have disadvantages when it comes to securing IoT devices. On the other hand, a new encryption method using brain signals in IoT devices is gaining attention as a new solution. The encryption method based on brain signals essentially involves a hypothesis called imposed recall based on ironic process theory. The imposed recall was created with the expectation that imposing a specific choice on the subjects during the acquisition of brain signals would allow for better separation of EEG data. This paper presents experiments and approaches to prove the validity of the imposed recall hypothesis. With the experiments, the effects of ironic process theory on brain signal-based encryption can be observed. While performing the tests, varying approaches, including Granger causality, were applied to analyze the results. The results show that the imposed recall hypothesis can successfully reconstruct EEG data. The structured signals were determined to be effective in capturing matches of brain signals on subjects at different time intervals. Thus, the imposed recall hypothesis can be used in various fields, such as authentication, questioning, and identification, by reserving brain signals to be obtained from individuals. In addition, it was reported that it is possible to acquire the ability to provide security in both devices with limited hardware, such as IoT devices or complex systems.

Keywords: ironic process theory; IoT; encryption; brain signal; IoT device security; electroencephalography

Citation: Aydogan, A.F.; Varol, C.; Shashidhar, N.K.; Rasheed, A.; Vung Pham,V.; Karabatak, M. The Effect of Ironic Process Theory on Brain Signal-Based Encryption for IoT Devices. *Electronics* **2024**, *13*, 4804. https://doi.org/10.3390/electronics13234804

Academic Editors: George A. Tsihrintzis, Fahed Alkhabbas, Victor R. Kebande and Sadi Alawadi

Received: 30 October 2024
Revised: 23 November 2024
Accepted: 4 December 2024
Published: 5 December 2024

1. Introduction

The Internet of Things (IoT) is the name given to devices that have the capacity to process and share data both internally and across a local network [1]. The number of IoT devices that will be in use by 2025 is estimated at 27.1 billion [2]. IoT devices have a wide range of applications, such as outdoor surveillance, road toll and traffic management, city asset tracking, police evidence tracking, parking management, and fire services monitoring. In addition, IoT devices have a market size of over USD 22 billion [3]. Due to the high usage and market size of IoT devices, the rate of exposure to cyber-attacks and security needs are increasing in parallel. Solutions for securing IoT devices, including endpoint security, gateway security, and professional security services, are valued at over USD 3 billion [4]. The first solution to secure IoT devices is encryption. However, IoT devices are inherently limited in physical size. Therefore, the use of components with high computational processing capacity, such as CPUs, RAM, or GPUs, in IoT devices is limited [5].

Traditional encryption methods rely on mathematical computations. Symmetric and asymmetric encryption methods are the well-known solutions to such a situation. In order to extend security procedures for IoT devices, scientific authorities have developed various encryption approaches. The approaches involve lightweight, hybrid, authenticated encryption with associated data (AEAD) and post quantum encryption methods.

The listed encryption methods bring certain advantages as well as disadvantages [6]. In summary, symmetric and asymmetric encryption are secure for now but require a lot of processing capacity. Lightweight encryption is low-cost but not fully functional in terms of security. Hybrid encryption can cause security problems because of the information channeled through it. Quantum methods are still under development. AEAD methods need much more costly calculations because they are quantum adversarial. As a result, encryption approaches created to secure IoT devices fail to achieve the triad of cost–security–effectiveness [7].

Biological-based approaches are also available to secure IoT devices to reduce costs, increase security, and ensure effectiveness. However, technological innovations have reached a point where the ability to expose fingerprints or imitate facial recognition systems by artificial intelligence and deepfake is no longer a challenge [7]. A study by Bontrager et al. showed that fingerprint recognition systems can be easily exploited with MasterPrints-based dictionary attacks. In the study, existing fingerprints are trained with a generative adversarial network (GAN). Then, synthetic fingerprints are generated by modifying the latent variables with an approach called latent variable evolution (LVE). The rolled and capacitive success rate with the proposed method is 77.34% [8]. In addition, a study by Korshunov et al. showed that face recognition systems can be beaten by deepfake technology. The study by Korshunov and Marcel demonstrated that face recognition systems can be easily deceived by deepfake videos. Korshunov et al. used a generative adversarial network (GAN) to generate deepfakes. The study utilized the VidTIMIT database and included low- and high-resolution videos. The best detection method, based on image quality metrics and a support vector machine, achieved an equal error rate of 8.97% [9].

In summary, there are still vulnerabilities in traditional and innovative encryption methods that have been introduced to address the security challenges of IoT devices. Therefore, the development of encryption methods for IoT devices remains an important aspect. Encryption methods to be developed for IoT devices focus on cost, security, and efficiency. There have been limitations to the approaches that have been taken to cover the three focus areas indicated. In addition, the user factor also obviously contributes to security vulnerabilities. In this case, it would be a significant contribution to work on the security of IoT devices, which will offer advantages in terms of cost, security, and efficiency, as well as limit the negative impact of the human factor on the security mechanism.

Academic studies have focused on improving IoT device security by adding new features. Upon understanding that IoT devices will provide a performance advantage with human interaction, the studies extended to the combination of the physical characteristics of people and IoT technology. Blood pressure measurement, heart rhythm, and step counting features are among the first areas of use of IoT technologies, which recently started to be replaced with other valuable areas for one's needs. Electroencephalography (EEG)-based applications, one of the innovative IoT device-based works, remain popular. EEG provides a chart of the electrical signals that occur due to brain activity. In addition, EEG data can convey emotional changes such as happiness, sadness, stress, and pain about a person while successfully transmitting physical changes such as eye and hand coordination and gestures. The idea of controlling IoT devices with brain frequencies has emerged recently, and many similar projects continued to be developed using EEG data. An innovative project called the Brain–Machine Interface (BMI) is one of the leading studies that will direct the research in this area. For instance, the study, recently announced as a Neuralink project by Tesla Company, clearly reveals the potential of using brain frequencies to control technological devices in the future [10].

The first states of the mentioned EEG applications were generally based on the interpretation features of IoT devices used in the health field. Pap et al. [11] show that the brain frequencies obtained using the NeuroSky Mindwave EEG headset examined the eye movements using machine learning algorithms contained in the IoT device. They aimed to integrate the analysis of the existing data into the health system. Immediately after

IoT devices merged with EEG systems, Abdellatif et al. [12] tried to make signal data more consistent. As a result of the previous research work, it has been revealed that EEG signal data can be used more comprehensively with IoT devices not only in health systems but in many different areas [12]. Guk-Han et al. [13] focused on using IoT devices and EEG data in military fields. With the help of smart combat helmets, analyzing the mental responses of soldiers with their current and future positions to generate ideas for decision mechanisms [13]. De Buyser et al. [14] aimed to have better and faster control of intelligent home systems using EEG signals of IoT devices. The system employs smart glasses and EEG data to trigger the desired IoT operations instantly [14]. Another article using IoT devices and EEG data was presented by Carrasquilla-Batista et al. [15], which processed the data received from the Brainwave Headset of NeuroSky device using the Raspberry Pi and aimed to control wheelchairs as well as wearable technologies. The studies above generally tried to improve the control mechanisms of IoT devices with brain frequencies. However, security procedures for IoT devices need to be strengthened for cyber-attacks and the security of the systems. Alrawi et al. [16] examined the existing encryption methods and showed that despite the rapid development of IoT devices, encryption methods are unsuccessful in catching up with this emerging technology.

One of the essential features of encryption systems is that they perform better if they are individualized. However, someone who knows a particular person can aim to log into that person's account. This will fail the individuality protection mentioned above. Even though encryption enhancements containing individuality are successful as an idea, it is understood that they include technical weaknesses. A brain signal-based encryption method for IoT devices has been created to ensure that personality is integrated successfully with encryption methods. Although its primary purpose is to ensure the security of today's increasing IoT systems and to make easy use simultaneously, it is a study that can show the potential to work with many different systems in the future. As a simple summary, the brain signal-based encryption method for IoT Devices is used to trigger the tasks of IoT devices by reading the electrical signals generated by a user-determined memory in the brain. As a known fact, although two or more individuals have the potential to have the same memories, the difference in emotions felt by each person will cause differences in the brain waves that the person will create. The described system will make creating a fully secure IoT system easier by taking individuality to the top. As an additional security measure, the system can eliminate the weaknesses of bionic encryption systems previously created to bring individuality to the fore.

This paper provides details of a low-cost, secure, and effective methodology for securing IoT devices that limits the negative effects of the human factor. The encryption method to be detailed uses brain signals to create a convenient encryption method for IoT devices. As a result of the chemical interactions of neurons in the human brain, communicating among themselves, brain signals become observable at any moment. Devices called EEG make it possible to measure brain signals on the micro-volt scale [17].

Since the production of quantifiable outputs is biologically inexpensive, it can replace the data that has to be produced by symmetric–asymmetric encryption methods or versions thereof. In the proposed system, vulnerabilities will be prevented as users do not have any input, such as a password. In this way, uniqueness can be achieved more advantageously than with fingerprints or facial recognition systems used in the same biological-based encryption. In addition, brain signals cannot be tracked by external observers and will not be possible to mimic. All the advantages of brain signals can replace the standard input–output structure used in classical encryption methods or biological-based encryption techniques.

Instead of users providing a password or other input, as in conventional methods, brain signals replace the input. However, since the chemical interactions that take place in the brain are not controlled, the main challenge is to stabilize the signals that will be used instead of the password. To make an analogy, the system always demands the correct password, but it is known that brain signals from a particular person at various time

intervals can vary. At this stage, we are trying to produce a stabilization in the brain signals by introducing the imposed recall hypothesis based on the ironic process theory.

Restricting the processing stages of EEG signals may be thought to sacrifice the accuracy of the data obtained. Thus, an "imposed recall" strategy is recommended to preserve the accuracy of EEG data. The imposed recall hypothesis is based on a short-term redirection of brain frequencies to a memory from a limited choice. The imposed recall hypothesis is closely related to a psychological phenomenon called ironic process theory. Namely, ironic process theory is a paradox that occurs when the brain increases the importance of a thought when it is not intended to be focused on that thought. One of the most famous examples of ironic process theory is that when we say, "don't think of the white bear", we think of nothing but a white bear.

At this stage, the person increases focus by entering a coherent concentration of thought. The imposed recall hypothesis predicts that a free choice between the options presented to the person during EEG recording can stabilize the EEG data. In this way, the person will be able to make free-willed choices from a limited pool of options. For example, a person might be asked to choose a number between 1 and 10. The person is free to choose any number, but the possible numbers that can be chosen are limited. The existence of a choice pool limit is thought to make the concentration time much faster when the person is told to think about the number they have chosen. Reducing the concentration time may lead to more stable results in short-term EEG recordings. In addition, the presence of free will in the choices would ensure that the choices still have a psychological background. For example, let us assume that locking a door reminds one of his/her graduation memories. Even though that person is not alone at the same graduation ceremony, graduation will feel different for that person than for everyone else. So, even if one is thinking about the same ceremony at the same time as his/her friend, the brain frequencies you produce will be unique. If the explanations are exemplified by the previously mentioned memory of the graduation ceremony, it is like asking a person how they felt when they received their diploma. The person is concentrated on a small fragment of memory, but the brain frequencies that emerge from the thoughts are still unique. Short-term EEG data with high intensity will be much easier to process. Following the rising trend of using brain signals in the digital world, we laid the foundations of the imposed recall hypothesis in our study called "A New Security Mechanism for IoT Devices: EEG Signals" [18].

This study's primary objective is to assess the effect and validity of the imposed recall hypothesis based on ironic process theory by employing more sophisticated cases.

The Background section includes details on using EEG devices and acquiring brain signals from subjects to provide an encryption methodology for IoT devices. The background section also provides a cover of the imposed recall hypothesis based on ironic process theory. The examination of the Effects of Ironic Process Theory on Brain Signals section examines the effects of the imposed recall hypothesis on the brain signals of the subjects with the created experimental scenario. We analyze the results of the effects of the imposed recall hypothesis on the subjects using methods such as Gaussian distribution, Simpson's rule, and expectation maximization. The third section includes steps to check the effects and validity of the results in the background section with additional scenarios. In the Discussion section, the structures of the experiments in the study are compiled, and observations are included. In the conclusion section, the results of the study are evaluated. Finally, the future works section addresses the possible implications of the study and its influence on research topics.

2. Background

In traditional encryption methods, different approaches are used to convert inputs into data that cannot be read by an attacker. In the encryption method created for IoT devices using brain signals, EEG data play an active role in both inputs and outputs. Brain signals are the result of chemical changes led by neurons. EEG devices are used to measure the electrical data generated by the brain. In [18], the EEG device used to acquire users'

brain signals was Emotiv Insight 2.0. The device used during the experiments contains five electrodes: AF3, T7, Pz, T8, and AF4 [19]. Sensor data are provided in microvolts (µV) in EEG devices; the Emotiv Insight 2.0 has a peak-to-peak (pp) range of 8400 microvolts (µV). This means that the range detected by the device is −4200 µV to +4200 µV. However, users see float values instead of microvolts as output. In this case, there is a phase of conversion of microvolt values from analog to digital. Emotiv Insight 2.0 uses a 16-bit analog-to-digital converter (ADC). So, each generated datum has a resolution of 16 bits. Least significant bit (LSB) is used to represent the smallest possible increment of a measurable value. Thus, the LSB of Emotiv Insight 2.0 with 16-bit resolution and a dynamic range of 8400 µV will be 0.128 µV. As a result, the EEG data provided to the end user need to be incremented or decremented by 0.128 µV to show change [20]. The range in which the data can be contained is 16-bit. Each electrode can create 128 samples per second. That is, a subject produces 1280 lines of data for each electrode during 10 s of recording.

In addition, the outputs of the obtained data can be extracted in CSV format. Consistency is the most critical factor in EEG devices. In particular, as brain–computer interface (BCI) applications are developed, EEG signals are expected to yield the same results in the long run. Although BCI applications that can be created with EEG devices used in medical fields are possible, it is unwise for the end user to use a large and complex system in their daily lives. The consistency of mobile EEG devices is a phenomenon that may raise a question mark for users. However, Grummett et al. [21] found that Emotiv devices are comparable to medical EEG devices. While the authors' study was carried out, medical EEG devices placed close to the buds in the skull of the Emotiv devices yielded results that were similar to those of medical devices. Emotiv devices were proven to reflect mental activities in medical standards [21].

For our tests, numerous subjects took part in the experiments for the encryption method being created. Various scenarios have been developed to create and validate the proposed encryption method. The hypothesis of the scenarios is based on the ironic process theory. The ironic process theory creates a paradoxical effect by leading individuals to intentionally avoid thinking about a particular idea. In contrast, this study uses a process called imposed recall. The imposed recall hypothesis is based on the concept that individuals are unable to prevent recalling the choices made from a limited pool of options by transforming them into memories and recalling them when the phenomenon is encountered again. For this reason, all the scenarios in the experiments are based on the imposed recall hypothesis.

The imposed recall hypothesis predicts that a free choice between the options presented to the person during EEG recording can stabilize EEG data. In this way, the person will be able to make free-willed choices from a limited pool of options. For example, a person might be asked to choose a number between 1 and 10. The person is free to choose any number, but the possible numbers that can be chosen are limited. The existence of a choice pool limit is thought to make the concentration time much faster when the person is told to think about the number they have chosen. Reducing the concentration time may lead to more stable results in short-term EEG recordings. In addition, the presence of free will in the choices would ensure that the choices still have a psychological background. For example, let us assume that locking a door reminds one of his/her graduation memories. Even though that person is not alone at the same graduation ceremony, graduation will feel different for that person than for everyone else. So, even if one is thinking about the same ceremony at the same time as his/her friend, the brain frequencies each individual produces will be unique. Short-term EEG data with high intensity will be much easier to process [18].

Six different subjects were involved in the first experiment to check whether translating the ironic process theory into imposed recall would actually work. In the preliminary experiments, data were acquired from the EEG device while the subjects were looking at a computer screen. The subjects were shown four different photos of different locations. In the last photo, the subjects are instructed that they have an imaginary wallet. They

are asked to hide this wallet in an area in the photo. Figure 1 contains photos of the environments used in the preliminary experiments.

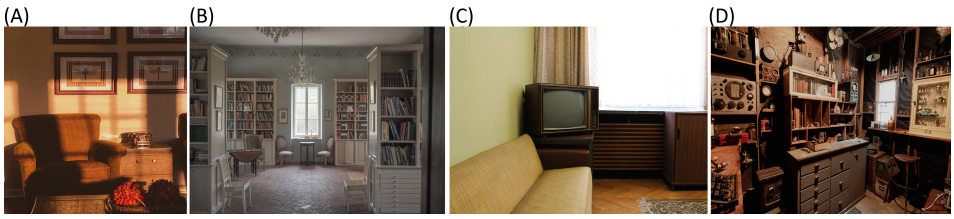

Figure 1. Photo (**A**) contains a dresser with an antique telephone on it and a chair. The second photo (**B**) is a library. The third photo (**C**) contains an old television and a cabinet. The fourth photo (**D**) is a workspace with many drawers and cabinets. Notice that each photo contains a drawer or cabinet. The benefits of this feature in the photographs will be revealed in free choices.

Figure 2 provides a summary of how the preliminary experiments were conducted. Table 1 reports which photo was used to hide the imaginary wallet by the subjects participating in the preliminary experiments.

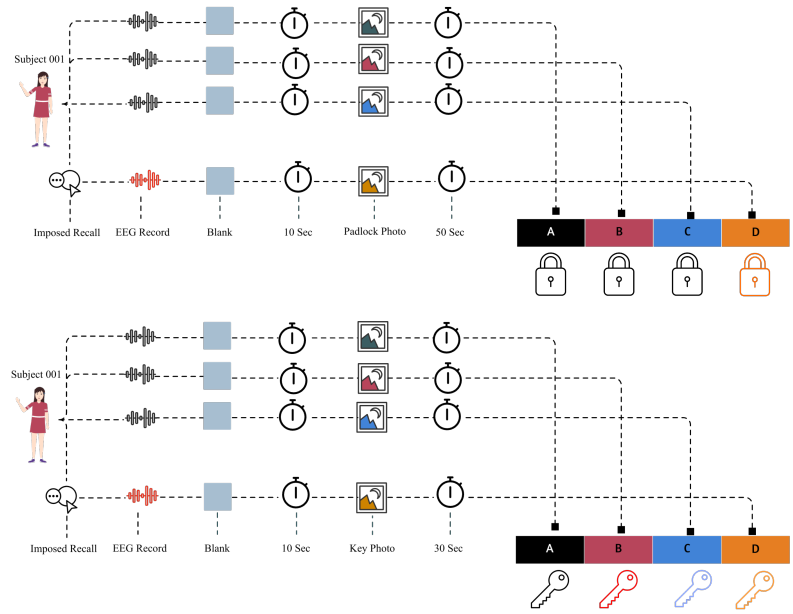

Figure 2. When the EEG data started to be acquired, each subject looked at a blank screen for the first 10 s. The purpose of showing the blank screen is to reduce the stress level of the subjects and to allow time for noises to be avoided during the correction of their posture. Then, a photograph is shown on the screen for 50 s. The figure shows that subjects undergo imposed recall before the 4th photograph. It should be noted that the sequence of pictures shown to subject 002 was shifted back one step compared to the previous subject. If the recordings of the sample subjects in the figure contain imposed recall, they are named "Subject 001 Padlock Photo D 1 Minute" and "Subject 002 Padlock Photo C 1 Minute". Even if the records do not contain the imposed recall, they will continue as "Subject 001 Padlock Photo A 1 Minute" and "Subject 002 Padlock Photo A 1 Minute". This is intended to ensure fairness in the crossing of records between each other, which will be shown in the following steps to understand how possible a padlock-key match is. In the second phase of the preliminary experiments, 40-s recordings were taken to measure the matches. Similarly, the first 10 s of the experiments were blank screens. Then, the previous sequence of photo display was repeated. In the second phase, no imposed recall was applied to the subjects because they already knew which photo was the padlock.

Table 1. Each subject is represented by an ID number. The photos that the subject in the first experiment scenario focus on are represented as the "Selected Padlock Photo".

Subject ID	Selected Padlock Photo
007	Picture C
011	Picture B
012	Picture D
033	Picture D
068	Picture D
083	Picture A

According to our hypothesis, this choice made by the subjects will intensify the brain signals and produce the same kind of brain signals when the same location is encountered later. The first EEG recordings of these four photos are called padlock. In the second stage, the subjects are shown the previous photos again. The data obtained at this stage is called the key. No intervention is made on the subjects while key data are obtained. At the end of the experiment, there are four different Padlock and Key files for each subject. If the imposed recall hypothesis is successful, only the padlock files, where the subjects hide the imaginary wallet, and the key files, where the records containing the same image are present, should match. Figures 3–6 are provided to clarify the enhancement of signal intensities with imposed recall. In the figures, the X axis shows the distribution of the EEG data, while the Y axis reflects the intensity levels of the data.

In Figure 3, the 1 min padlock and 30 s key data of subject 007 photograph "C" are shown on the same axis with respect to the electrodes. In particular, it is observed that the intensity measurements of the 30 s recordings are larger for each electrode in the matched images.

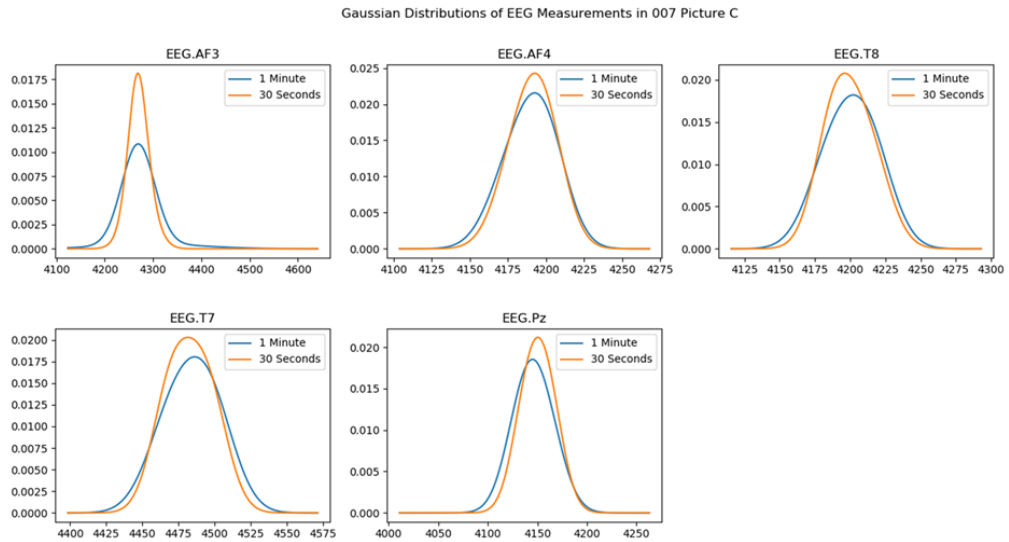

Figure 3. Gaussian distribution in same axis of 1 min padlock and 30 s key picture C records of Subject 007 by electrode basis.

However, for subject 007, when the 1 min recording remained the padlock photograph "C" and the 30 s key recording belonged to another photograph, the above-mentioned situation remained only for limited electrodes. Figure 4 shows the distributions of the 1 min padlock photograph "C" and the key 30 s photograph "D" for subject 007 on the same axis. As can be seen, the 30 s intensities were higher than the 1 min recording only at electrode AF3.

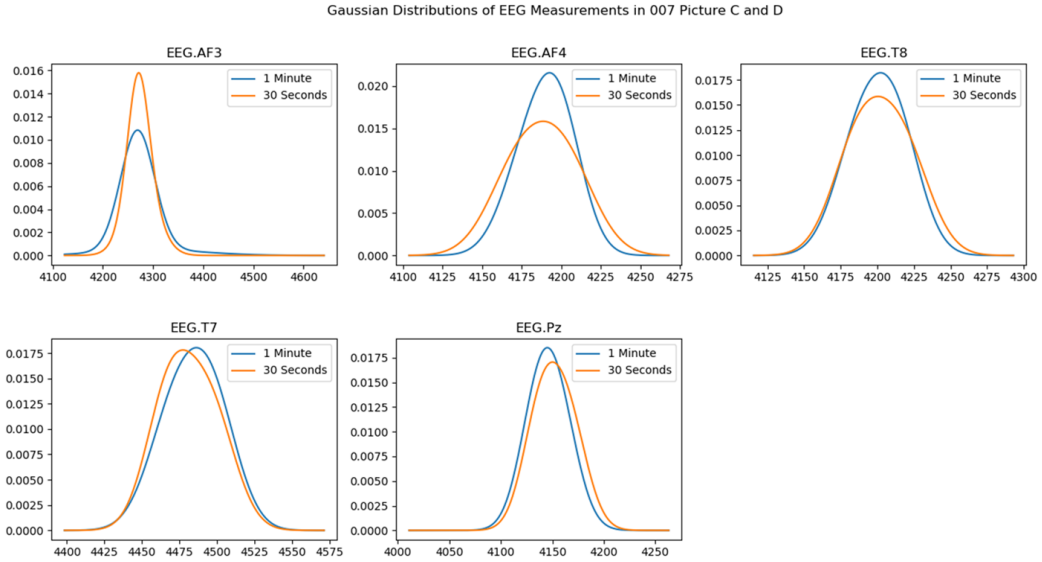

Figure 4. Gaussian distribution in same axis of 1 min padlock picture C and 30 s key picture D. records of Subject 007 by electrode basis.

When the representations on the same axis were continued with another subject, 083, it was observed that the 1 min padlock and 30 s key photograph "A" recordings were similarly shaped. However, for subject 083, the number of electrodes for which the 30 s recordings were observed to be superior in intensity was three. Figure 5 below shows the situation by placing the electrode at points T8, T7, and Pz.

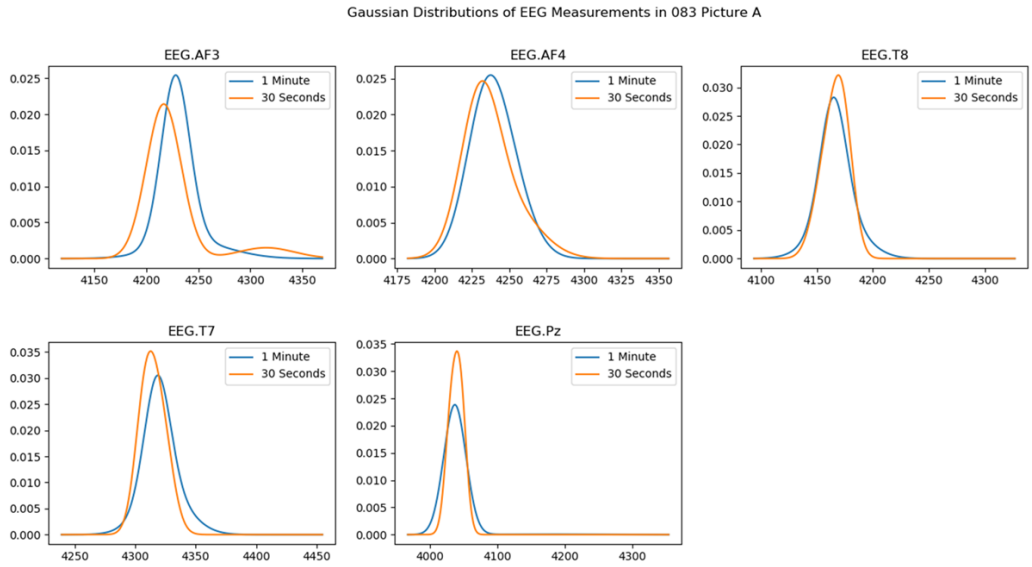

Figure 5. Gaussian distribution in same axis of 1-minute padlock and 30-second key picture A records of Subject 083 by electrode basis.

For subject 083, when the 1 min padlock photograph "A" and the 30 s key photograph "D" were selected, the intensity dominance returned to the 1 min recordings. In Figure 6 below, the intensity dominance of the 1 min recordings at all electrodes except Pz can be easily seen.

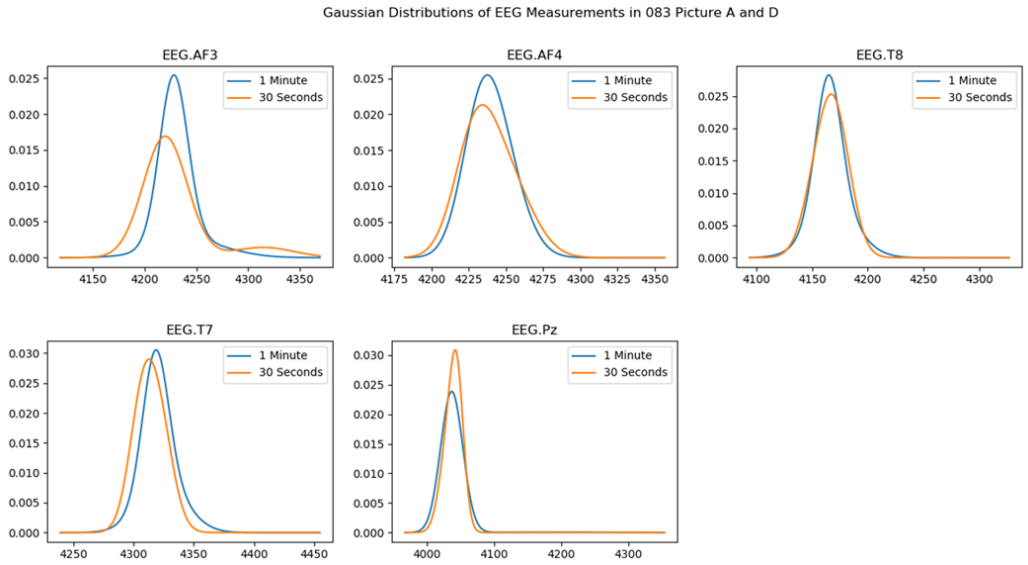

Figure 6. Gaussian distribution in same axis of 1 min padlock picture A and 30 s key picture D records of subject 083 by electrode basis.

At this stage, the EEG data obtained from the subjects were analyzed with a series of algorithms for comparison. The padlock and key files of all subjects were cross-compared to each other. Therefore, it was also checked whether the key files created by two different subjects hiding wallets in the same photo could unlock each other. Simpson's rule divides the interval into sub-regions to calculate the area under the curve and approximates the curve in each sub-region as a quadratic function [22]. Initially, the main objective is to approximate the curve with a series of parabolic arcs and find the area of each parabolic segment. By applying Simpson's rule, the intersection points of the data in the padlock and key files of the subjects were determined. Then, the area shared by the slopes between the determined points was calculated. As a result of the calculations, it was determined that the distribution of the data belonging to the key files overlapped 7.69% more when the subjects saw the photo where they kept the imaginary wallet again. In addition, we observed differences in the density of the padlock records where the subjects kept the imaginary wallet and the key data recorded in the same image. In correct padlock and key comparisons, key data have a higher density.

Once expectations were met, unsupervised machine learning algorithms were applied to find an approach that was always valid for each subject. Namely, if the correct padlock and key matches make a difference in the densities and distributions, there will be a difference in the clustering. For each subject, the padlock and key data for the correct photo should be clustered together. Several steps were used to obtain the outputs for the clusters. The z-score was obtained by subtracting each value in the data set from the mean and dividing by its standard deviation [23]. Z-score normalization makes revealing relationships between data easier. The output data were clustered using the expectation maximization (EM) algorithm to reveal hidden connections between the data distributed in Gaussian mixture modeling [24]. EM adopts the Mahalanobis distance method. Mahalanobis distance takes into account data distributions to find data similarities, which is exactly what is desired [25]. Logarithmic likelihood is used to measure the performance of the resulting clusters. EM data were repeated three times with K-fold cross-validation to get a better clustering performance. In addition, the possibility of a potential mismatch was considered by crossing recordings in which different subjects saw the same photos. During the experiments, it was determined that using only the AF3-Pz-AF4 electrode combination would be sufficient for subjects to identify the correct padlock and key pairings. The user data from the AF3-Pz-AF4 electrode combinations were able to identify 90 percent of the correct padlock and key combinations. The main factor for the identification was the correct

padlock and correct key comparisons, which contained much more one-way clustering than all other encounters with incorrect key files.

In the final analysis, since Emotiv Insight 2.0 has 128 samples per second, and each of these 128 data are in a 16-bit range, this results in a key range of 2048 bits per second for each electrode. This key range would be 10,240 bits per second for five electrodes. For example, in the preliminary experiments, 50 s of data remained after the padlock records were cleaned. So, altogether, a range of 512,000 bits were recorded for the padlock. This would be 307,200 bits for 30 s of key recordings. However, unlike key ranges, key sizes will be relatively larger because the end user will see float values rather than microvolts. Since the float data type is 32-bit, a 50 s padlock record can have a maximum size of 1,024,000 bits. In addition, the Shannon entropy of the obtained values is, on average, 3.26 bits per digit. On the other hand, all the aforementioned values will have no counterpart in the proposed system because there is no relationship between password and encryption as in classical encryption methods. Instead, padlock and key records perform authentication based on clustering.

Thus, IoT devices without powerful components were able to acquire data to be used in massive bit-rate encryption without expending any power. The big advantage was that users were already generating brain signals instead of using any mathematical operations.

3. Examination of the Effects of Ironic Process Theory on Brain Signals

The primary aim of this section is to conduct a thorough examination of previously established results to bolster hypotheses proposed by various methods. At this stage, an extended experiment was conducted to check the imposed recall hypothesis supported by the ironic process theory. In the extended experimental scenario, the aim was to test the accuracy of the results and hypotheses proposed in the preliminary experimental phase under different conditions. One of the main differences between preliminary and extended experiments is in the orientation of the subjects. As will be remembered, in preliminary experiments, the first scenario involved an intervention called imposed recall. Imposed recall was intended to increase the subjects' focus and thus capture conjugate signals in the second phase. In extended experiments, users are shown playing cards without any intervention. Our aim is to explore how signals are constructed in the absence of interference between users. In this phase, we will examine the consequences of the difference in intervention between the preliminary and extended experiments. So, the validity of the Imposed Recall hypothesis and the structure of brain signals at the moment of decision will be revealed, which may lead to further studies.

The experimental scenario included five different playing cards: the back-facing card, diamond 3, diamond 4, spade 3, and spade 4. The back-facing card was introduced to replace the blank screen shown to subjects in the preliminary experiments. Figure 7 below illustrates the cards used in the experiments.

Figure 7. Demonstration of the cards used in the experimental scenario.

The new experimental scenario has two phases. In the first stage, subjects sit in front of a screen with EEG devices attached. The experiment is started without informing the subjects about the content of the experiment. A face-down card is presented for 10 s. Afterwards, diamond 3, diamond 4, spade 3, and spade 4 cards are shown for 10 s each.

The total recording time for the first phase is 50 s per subject. The 50 s recording obtained is referred to as "Undetermined Padlock". This is because the subjects have no preference regarding the cards, and they are not imposed upon in any way about what to think when they see the cards. Undetermined padlock recordings will be used in the following stages both to question the imposed recall and perform verification. An illustration of the first phase is given in Figure 8.

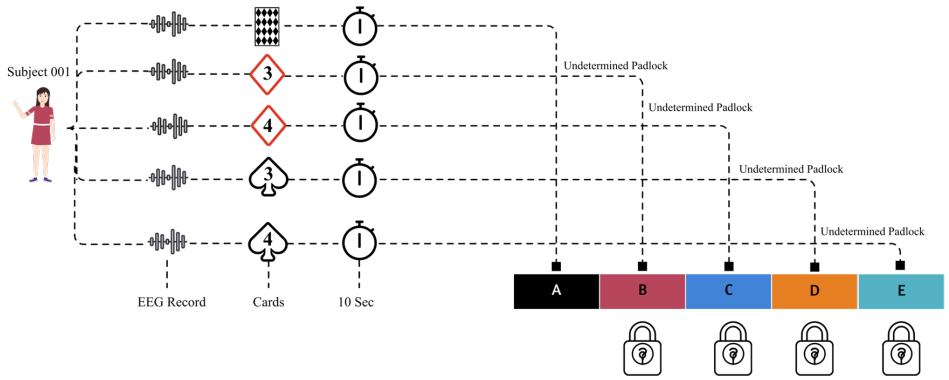

Figure 8. Demonstration of the recording of EEG signals as undetermined padlock in the first phase for subject 001.

Before the second phase, subjects are asked to choose one of the cards they have seen. The card choices made by the subjects in the extended experiments are shown in Table 2. In the second phase of the experiments, each card is shown again for 10 s without changing the order of the cards shown in the first phase. Before the end of the experiment, the face-down card is shown once more, and a new sequence is introduced. At this time, the order of the cards is changed to spade 3, diamond 4, diamond 3, and spade 4 for 10 s each. Thus, a total of 100 s are recorded in the second phase of the experiments. Out of the 100 s recorded, 20 s consists of face-down cards. The first 50 s of the 100 s of data will be used as padlock and the remaining 50 s as key. An illustration of the second phase is shown in Figure 9.

The method to be used to detect differences between the two experiments is Granger causality. The main reason for choosing the Granger causality is that it is widely used in approaches based on the estimation of the activities of two different brain regions. In addition to causal relationships between the regions, it also helps to estimate the propagation patterns of neural activity. Its use in analyzing the interactions of neural time series remains popular. In addition, the Granger causality targets linearity. If the neural activities under study also have nonlinear interactions, the focus is still on uncovering linear data. Due to all these advantages, it has been the main choice for this study [26]. The Granger causality will help to reveal the relationship between two time series. Presenting a simplified example of the Granger causality will clarify its working principle. As an example, considering house and automobile prices, is it possible to predict the future trends of house or automobile price increases based on these two price graphs that have changed over the years? Approaches using the Granger causality can reveal predictive relationships between time series. However, it should be noted that the Granger causality predicts the next stage of the data between two time series trend-wise, not value-wise. So, instead of numerical data from house prices to automobile prices, it can predict upward or downward trends. In addition, the direction of comparison of causality is also important. Namely, while a positive trend can be detected by comparing house to automobile series, the same may not be true between automobile and house prices.

The Granger causality can be recognized as useful in the preliminary and extended experiments to establish the validity of the imposed recall hypothesis. In the first stage, the focus is on the imposed recall in the preliminary experiments. When applying the Granger causality to the recordings, data are divided into one-second chunks of one-second

EEG data. Recall that in the preliminary experiments, the padlock recordings consisted of 60 s in total. However, the first 10 s of the 60 s consisted of a blank screen with noise cancellation. After the blank screen data were deleted, 50 s of raw padlock data remained. So, each subject had 50 datasets for each image. Since there are image records for four different locations for each subject, there are 200 padlock records in total. Each padlock datum contains 128 lines of data for each electrode. In total, 128 lines of data are equivalent to the sample rate per second of the Emotiv Insight 2.0. The data segmentation process described above was applied to the subject records from both the preliminary and extended experiments. The only difference between the recordings was the recording duration.

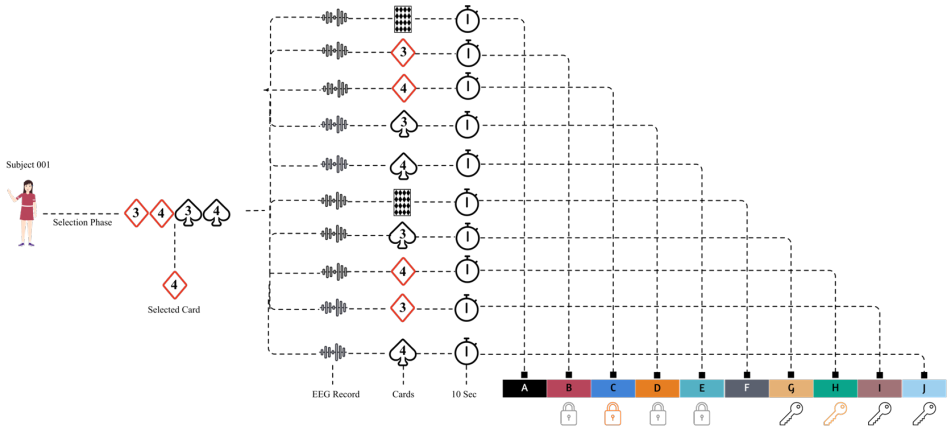

Figure 9. Demonstration of the card selection and recording of EEG signals in the second phase for subject 001.

Table 2. Distribution of subjects, showing their choices in the first phase of the extended experiments.

Subject ID	Selected Card
002	Spade 4
003	Spade 4
004	Diamond 3
011	Diamond 4
014	Diamond 3
018	Diamond 4
021	Diamond 3

The Granger causality is a method used in EEG data. In general, it is useful to perform 100 ms of estimates for each second of EEG data [27]. Therefore, it is necessary to check every 100 ms of padlock data obtained from the subjects and divided into one second. The Granger causality provides estimates using time lags. The lag helps to determine how long past values of a time series affect the current values of another time series. Since a control of 100 ms is needed during the experiments, 128 lines of data should contain 12.8 lag. Therefore, the number of lags was set as 13 in the studies. Since the Granger causality poses hypotheses about trends instead of numerical data, different statistical tests were used to perform the analysis for the rejection or acceptance of the hypotheses.

The first of the tests used is the SSR (sum of squared residuals) F-test. The SSR F-test compares a restricted model with fewer parameters with an unrestricted model with more parameters [28]. As an example, let us consider applying the results of the Granger causality to house and automobile prices using the SSR F-test. In the first stage, the SSR F-test will analyze the intertemporal data for car prices as a restricted model. Namely, it will examine the trends of car prices in the past for trend forecasting of current car prices. In the second stage, it will try to estimate the trend forecasts of automobile prices with temporal lags of both automobile and house prices. This stage, which is characterized as an unconstrained model, examines whether the past trends of house and car prices can be used to predict

future car price trends. Secondly, the SSR chi-squared test was used. The main difference between the SSR chi-squared and the F-test is in the realization of the statistical distribution. Namely, in the F-test, the inference between two models is performed by normalizing the differences of the sum of squares. In chi-squared, the inference is based on the logarithmic difference of the sum of squares [29]. Thirdly, the LR (likelihood ratio) test was used. Unlike the others, the LR test uses the maximum likelihood method. Namely, the most probable value among the data is selected and included in the comparisons as the main parameter. While performing these approaches, the LR test is based on the chi-squared distribution [30]. Therefore, it is possible to confuse the LR and chi-squared tests. Finally, Params F-test (unconstrained model) was used. Differently, the Params F-test focuses more on the performance of the unconstrained model in trend forecasting. The name implies that it uses the F-test in the distributions when performing the calculations. In all tests, the rejection of the null hypothesis is fixed at a p-value below 0.05. In the calculations performed to prove the validity of imposed recall, the records of subjects 033, 068, and 083 were used. The main characteristics of these specifically selected subjects are that two of them chose picture "D", and one of them chose picture "A" as padlock. In this way, it will be possible to better observe the differences between the same and different padlock selections in cross-queries.

An illustration of how the Granger causality was used to analyze the subjects' records is given in Figure 10. Figure 10 shows how the Granger causality is used to analyze the data of the recordings of picture A of subjects 033 to 068 on electrode AF3. The plot consists of two phases. The first stage includes all data from the AF3 electrode of the subjects. The Y axis shows amplitude, and the X axis shows time. The vertical vectors on the signals represent one-second segments of data. The vertical red vector indicates the segment where the Granger causality is currently estimated. The second stage of the plot contains the vectors of values for the tests mentioned earlier. The Y axis reflects the p-values of the mean of the lag values, while the X axis represents how many segments have already been analyzed. There are 13 lag values in total for each segment. The figure comparing subjects 033 and 068 at electrode AF3 is presented in the second s. So, in total, there are two vectors containing the mean of the 26 lag values. In the first second, it is observed that the average of the lag values decreases up to a p-value of 0.10. However, in the second second, the average p-value of the lag values increases up to 0.40. The dashed red vector has a p-value of 0.05, which is the level at which the null hypothesis cannot be rejected. Thus, it can be said that it is more likely to make inferences with the data between two different subjects in the first second than in the second second. However, since none of the values was below 0.05, no definitive conclusion was obtained.

Figure 11 shows the completed Granger causality calculations performed on the AF3 electrode of the padlock recordings of picture A of subjects 033 and 068. As can be seen in the figure, between the 10th and 13th second, the test values increased up to a p-value of 0.7. As can be seen from the figure, subject 068 has a signal spike with high amplitude values in the same seconds, while this is not the case for 033. This reflects the fact that the trend analysis of the signal values between subjects 033 and 068 is very unlikely to be performed. However, this changes in the following seconds. For example, signals between two subjects, even if fluctuating between 20 and 23 s, can complement each other in trend analysis. The p-values of the data are almost as close as 0.02, giving promise that a trend can be inferred. The results obtained by performing the details of the procedures given in Figures 10 and 11 for all subjects, electrodes, segments, and combinations are encouraging. First, considering that a one-second trend similarity would not be sufficient for proof, we focused on studies on the existence of a 2 s trend prediction hypothesis. In other words, the signals of the two subjects, being compared at similar electrodes, should be such that a trend can be inferred for two seconds at the identical moment. Thus, pairs of subjects must have produced signals with the same trends at the same time for two seconds. In addition, as exemplified earlier, the experiments were conducted bidirectionally rather than unidirectionally. For example, besides the 033 to 068 comparison, 068 to 033 signals were

also examined as a secondary direction. In total, 24,000 s of data resulted. In total, 312,000 different lag values were analyzed. Out of 312,000 lag values, 26 consecutive lag values with a *p*-value less than 0.05 were searched. Twenty-six lag values corresponded to 2 s of data. There was no 2 s trend prediction for the padlock recordings of the subjects in the preliminary experiments.

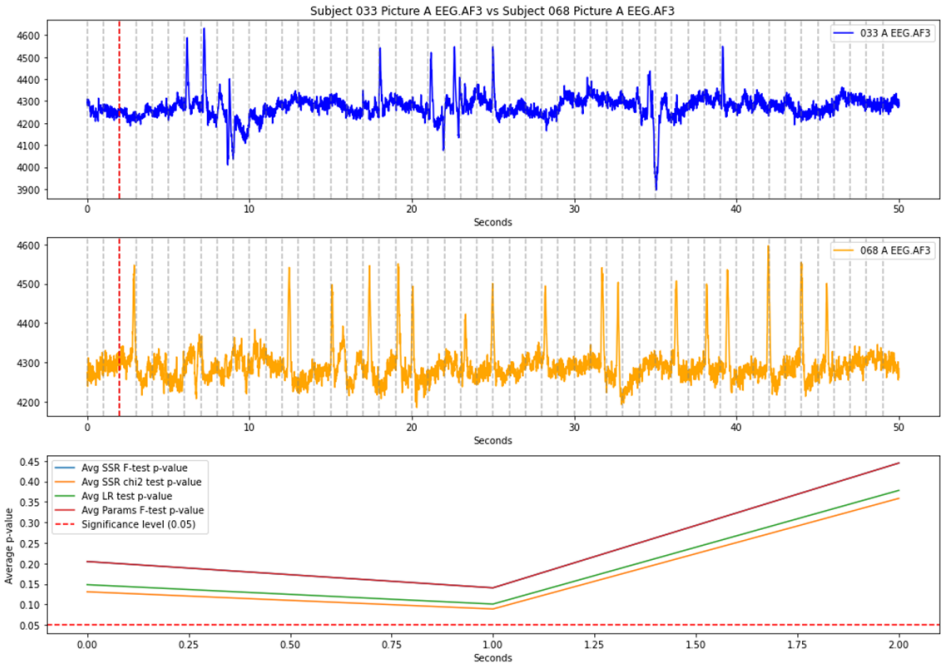

Figure 10. Visualization of the Granger causality analysis of the padlock recordings of picture A of subjects 033 and 068 through the AF3 electrode.

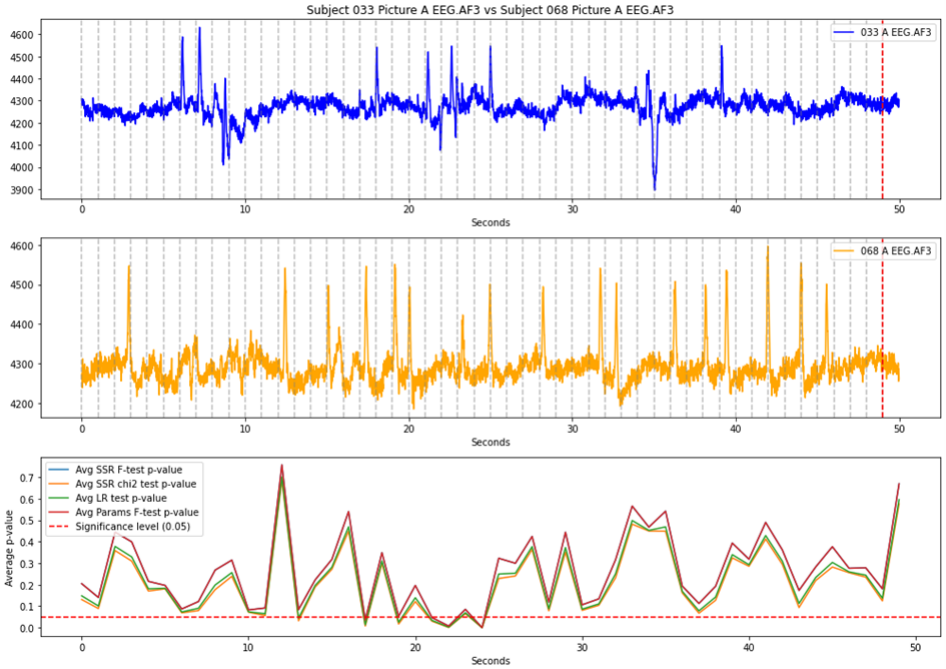

Figure 11. Visualization of the completed Granger causality Analysis of padlock records of picture A of subjects 033 and 068 via the AF3 electrode.

Also, the recordings of seven different subjects of the extended experiments were analyzed. In the undetermined padlock recordings obtained in the first phase of the

extended experiments, there were eight different 2 s trend estimates. The records of the subjects in Table 3 include the data from the first phase of the extended experiments, where the undetermined padlock records provided 2 s of trend estimation. In the columns of Table 3, Subject 1 and Subject 2 represent the subjects in the compared data. The focused channel emphasizes the electrode on which the Granger causality takes place. The selections section contains information about the cards that Subject 1 and Subject 2 selected after the first phase of the extended experiments. The trend column contains the playing card data corresponding to the segment where Subject 1 and Subject 2 have a trend similarity. As shown in Figure 9, a single record contains four different playing card sequences. In the first stage, diamonds 3, diamonds 4, spades 3, and spades 4 cards were included, respectively. Since each subject recording is segmented and cross-compared, a trend value of D3–D3 indicates that a trend was detected in the first 10 s of the 10-segmented data of Subject 1 and Subject 2. A result like D3–S4 emphasizes that there is a trend between the segments of the first 10 s of Subject 1 and the segments of the 30 to 40 s of Subject 2 data. The time interval represents the two-second intervals within each trend. Based on the previous example, if the trend is D3–D3 and the time interval is 8 to 10, this represents that the subjects have trend similarity in seconds 8 to 10 of the first 10 s of data from Subject 1 to Subject 2. The SSR F, SSR chi, LR, and Param columns are the average *p*-values for the 26 lag calculations of the tests performed. According to the data in the table, all subjects, except subject 021, had trend similarity, while the dominance was in 003. None of the trend data are identical to the cards of the subjects' choices.

Table 3. Selection of subjects participating in the preliminary experiments for the Granger causality.

Subject 1	Subject 2	Focused Channel	Selections	Trend	Time Interval	SSR F	SSR Chi	LR	Param
003	002	AF3	S4–S4	D3–D3	8 to 10	0.015	0.003	0.006	0.015
003	002	AF3	S4–S4	D4–S4	2 to 4	0.010	0.002	0.004	0.010
003	002	AF4	S4–S4	D4–S4	6 to 8	0.004	0.002	0.003	0.004
003	004	T7	S4–D3	D3–D4	1 to 3	0.003	0.002	0.0005	0.003
003	011	AF3	S4–D4	D3–S4	8 to 10	0.002	0.002	0.001	0.002
003	014	T8	S4–D3	S4–S4	3 to 5	0.014	0.005	0.005	0.014
011	018	Pz	D4–D4	D3–S4	2 to 4	0.002	0.0003	0.0002	0.002
018	003	AF3	D4–S4	S3–S4	8 to 10	0.003	0.0003	0.0002	0.003

As is well known, both experiments involved different concepts. Inferences that can be made at this stage are limited. However, it is still interesting to note that none of the data in the preliminary experiments showed a trend. Moreover, in the preliminary experiments, there was a total of 50 s of data for each image, whereas in the extended experiments, there were 10 s of data for each image. Could it be that the reason why the padlock recordings in the preliminary experiments did not contain a trending pair, while the indeterminate Padlock recordings in the extended experiments showed more than one trend, is because the subjects were not exposed due to an imposed recall?

To investigate the reason for the lack of a trend in the preliminary experiments, the next focus was on the second phase of preliminary and extended experiments. As is well known, the first stage of the preliminary experiments involved an imposed recall in which subjects were asked to hide an imaginary wallet somewhere in the picture. In the second phase of the preliminary experiments, it was assumed that subjects would focus on the wallet when the image of the environment in which they kept the wallet was projected again. In the extended experiments, the first phase involved a section in which no information was given to the subjects. However, before moving on to the second phase, the subjects were asked which of the cards they chose. The second stage of the extended experiments was to generate a padlock in the first 50 s and a key in the second 50 s by remembering the previously selected cards. The main difference between the two experiments was that a case and a task were imposed on the subjects in the preliminary

experiments. However, in the extended experiments, subjects were not informed about what to do with the card they chose. Briefly, the first phase of the pre-experiments includes the stage of the task. The second phase of pre-experiments is about remembering the choices. Conversely, in extended experiments, the first phase does not have parameters that differentiate the subjects. The first 50 s of the second phase of the extended experiments are about remembering choices (padlock generation), and the last 50 s (Key generation) are about the stage of the task because the card order has been changed. So, there is a completely opposite effect between the two experiments. Overall, in preliminary experiments, it is difficult to have trend similarity between the padlock and key because, in the first phase, subjects were directed to a task, which caused them to focus their attention on specific elements, such as an imaginary wallet. This task-oriented focus may have prevented broader patterns or trends from emerging in the data. Conversely, the second phase of the preliminary experiments involved remembering where they had hidden the wallet, and this was more about recalling memory than identifying trends.

On the other hand, the extended experiments involved a less structured approach in the first phase, in which subjects simply saw the cards and no other instructions were given. This lack of an imposed task may have allowed for more natural and varied responses, which may explain the emergence of multiple trends in indeterminate padlock recordings. The second phase of the extended experiments was divided into padlock generation (first 50 s) and key generation (second 50 s), in which subjects were asked to recall their card selection and then perform a task based on this memory. This structured recall and task performance may lead to the emergence of observable trends over time. The main element of the trend similarity differences between the two experiments may be due to the presence or absence of imposed recall tasks. In the preliminary experiments, the imposed recall may have limited the signals generated by the subjects, leading to a concentration of trends to certain values. However, the relatively unconstrained initial phase of the extended experiments may be involved in the emergence of trend tendencies. This may demonstrate that the experimental design, in particular the inclusion or exclusion of imposed recall, significantly influenced the observed data trends.

To prove these assumptions, the Granger causality is invoked one more time. If the hypotheses are correct, the relationships between task data and remembering data should not be trend-similar, while trend similarity should be detected between remembering and tasking data. In other words, there should be no trend between the padlock (task) and key (remembering) in the preliminary experiments. However, there should be a trend when comparing the key to the padlock. Conversely, in the extended experiments, there should be a trend between the padlock (remembering) and key (task) but not between the key (task) and padlock (remembering).

4. Results

The inspections started with comparing the padlock and key data from preliminary experiments. Table 4 contains padlock to key comparisons for the subjects of preliminary experiments. A total of four trend correlations were detected. None of the trend similarities obtained reflected the correct padlock and key combination. On the other hand, no trend pairs were found for subject 068. The emerging trends focus on the AF3–Pz–AF4 channels, which are examined in the unsupervised machine learning and signal adaptation phases. At this stage, the expectation is that the two-second trend similarity in Table 5 may emerge but that the emerging trends should not reflect the actual choices. This is because the predictability of the task over memories cannot be stable because the tasks have more parameters (imposed recall).

Table 4. Results of the Granger causality to the trend similarity detection of padlock-to-key records of data from preliminary experiments.

Subject 1	Subject 2	Focused Channel	Selections	Trend	Time Interval	SSR F	SSR Chi	LR	Param
033	033	Pz	D–D	A–D	2 to 4	0.006	0.001	0.001	0.006
033	083	AF4	D–A	B–A	3 to 5	0.008	0.002	0.003	0.008
033	083	AF3	D–A	C–B	15 to 17	0.013	0.004	0.006	0.013
083	083	AF3	A–A	D–B	17 to 19	0.00004	0.00002	0.00001	0.00004

The data in Table 5 reflects the key to padlock trend analysis of the preliminary experiments. The results capture only one trend similarity. Interestingly, the trend similarity reflects the correct key–padlock choices. The similarity of the detected trend was revealed in the examinations performed on the AF3 electrode.

Table 5. Results of the Granger causality to the trend similarity detection of key-to-padlock records of data from preliminary experiments.

Subject 1	Subject 2	Focused Channel	Selections	Trend	Time Interval	SSR F	SSR Chi	LR	Param
068	083	AF3	D–A	D–A	8 to 10	0.005	0.001	0.002	0.005

More than one inference can be made from the data presented at this stage. First, subject 068, who did not appear in the task–remembering phase, provided the correct padlock–key combination with 083 in the remembering–task comparison. However, the padlock–key selections of 063 and 033 belonged to the same D picture. Therefore, it has been shown that different subjects treated with imposed recall can produce different data even if they have the same task. Shortly, the working principle of the crossover procedures once again validated the hypothesis that two different subjects focusing on the same picture can produce two different results.

Secondly, the previously proposed assumption that the task–recall relation would fail to reflect correct choices, whereas the recall–task relation would show correct choices in trend similarity, was confirmed in the preliminary experiments. In order to test the accuracy of the argument once more, we focused on extended experiments. In the extended experiments, it was emphasized that the relationship between task–remembering was reversed compared to the preliminary experiments. Therefore, the padlock–key results should be obtained as the opposite of Tables 3 and 4. In Table 6, the padlock–key comparison of the subjects of the extended experiments is presented. The calculations show that in the extended experiments, the correct padlock–key combination for subject 011 was obtained in the padlock-to-key comparison. In addition, in contrast to the preliminary experiments, the result shows that subject 011 achieved trend similarity with his own data, not with another subject.

Table 6. Results of the Granger causality to the trend similarity detection of padlock-to-key records of data from extended experiments.

Subject 1	Subject 2	Focused Channel	Selections	Trend	Time Interval	SSR F	SSR Chi	LR	Param
011	011	T7	D4–D4	D4–D4	4 to 6	0.004	0.0006	0.001	0.004

In the next stage, the key-to-padlock comparison of the extended experiments was performed. The number of records with similarity in two-second trends is 17. However, no trend similarity pair could reach the correct key–padlock combination. In short, there was a contrast between the preliminary and extended experiments, as argued.

In summary, there are structural differences between the preliminary and extended experiments. The most important difference is that there is no imposed recall in the

extended experiments. The subjects in the preliminary experiments were given a task. The task (padlock) was to hide an imaginary wallet in one of the parts of a picture. Then, when the subjects saw the pictures, they involuntarily focused on where the wallet was hidden. This second phase was called (key) remembering. In extended experiments, subjects were shown playing cards. No intervention was performed while the playing cards were shown. The data generated by the subjects in the first phase were called undetermined padlock. After the first phase, the subjects were asked to choose one of the cards they had seen. The second phase consisted of two stages. In the first phase, the cards were shown in sequential order, as in the undetermined padlock phase. In this stage, the subjects had to remember only the card they had chosen. The second stage was a projection of the cards in a changed order. Here, the subjects were pushed into a task phase. In fact, the second stage was a non-invasive imposed recall. Having the subjects choose cards after the first phase focused them on seeing their own cards during the display of the cards in a complex order. So, the phases in the extended experiments led to a design that was different from the preliminary experiments. As a manifestation of this, the analysis of the data obtained from the subjects revealed different results.

5. Discussion

In the revealed results, the padlock phase of the preliminary experiments with imposed recall showed no trend similarity with any user. On the other hand, the undetermined padlock phase, the part without imposed recall in the extended experiments, found a trend similarity in all subjects except subject 021. Whereas in the preliminary experiments, the size of the data being compared was far bigger.

Secondly, in the preliminary experiments, the order was task to remembering. In the extended experiments, the two stages of the second phase were remembering to task because subjects were involuntarily drawn to a task in the second stage. Expectations were that the task to remembering trend similarities would not achieve correct padlock-to-key trend similarity because the task phase contains more parameters. So, the padlock-to-key comparisons in the preliminary experiments should not have reflected the correct choices, but the extended experiments should have the contrary. Table 6 shows that in the extended experiments, padlock-to-key comparisons were able to detect the correct selections. This was not the case in the preliminary experiments. On the other hand, the key-to-padlock trend analysis in the preliminary experiments should have reflected the right choices because inferences were made from highly parameterized data. The opposite should have happened in extended experiments. As shown in the key-to-padlock trend similarity analysis in Table 5, this inference was correct. There was a difference between the results from the task–remembering comparisons. In the preliminary experiments, the trend analysis was captured between two different subjects. In the extended experiments, in contrast, the trend was similar to the subject's own recording. The reason for the occurrence of this situation is thought to be that the imposed recall is either expressly or involuntarily. In the preliminary experiments, subjects were task-oriented. On the other hand, a similar trend occurred on the T7 electrode in the extended experiments. This could be a representation of the temporal part, which plays a role in the recall of objects. As a result, the hypothesis that imposed recall discriminates across data is proved. Therefore, if there is no padlock–key correspondence belonging to the same person, it is not possible for the Task data of any user to reveal the Remembering data of any user. The effect of the use of imposed recall between scenarios on stages such as task and remembering was revealed. In the brain signal-based encryption method that can be used in IoT devices, the imposed recall hypothesis based on ironic process theory was put forward. However, additional studies were needed to elaborate the imposed recall hypothesis and to prove its validity. This paper focuses on these goals with a new experimental scenario.

Extended experiments have a different approach and design than preliminary experiments. The first difference is the concepts involved in the experiments. While the preliminary experiments included pictures of the places, the extended experiments used

playing cards. In addition, the method of implementation of imposed recall also differs. There are two phases in the extended experiments. The first phase consists of showing the playing cards on the screen without any information to the subjects, such as back-faced cards, diamond 3, diamond 4, spade 3, and spade 4, respectively. For each card, 10 s of data were collected. In other words, there are 50 s of data in total. The purpose of the backward card is the same as the blank screen in the preliminary experiments and was eliminated. Since the subjects were not informed in the first phase, the data generated were called undetermined padlock. As can be noticed, imposed recall has not yet been applied.

After the undetermined padlock recordings, the subjects were asked to select a card they saw. They were not told what to do with their choice. However, in the preliminary experiments, it was stated that the choices would be used to hide an imaginary wallet. This led to the term non-invasive imposed recall. Non-invasive imposed recall exists to reveal what might change when subjects' choices are made without a purpose.

The second phase of extended experiments consists of two stages. In the first phase, the cards were shown sequentially for the first 50 s, as in the unterminated padlock recordings. The data obtained from the first stage serve as the padlock. However, it should be noted that only 10 s of data contain correct padlock records. Then, the order of the cards was changed and shown for another 50 s. Second-stage data serve as the key. Again, only 10 s of data contain the correct key.

It was thought that changing the order of the cards would involuntarily push the subjects into a task schema. At this stage, it would be useful to explain the task–remembering phenomenon in the pre-experiments. In the preliminary experiments, imposing padlock on the subjects to hide the imaginary wallet is a task. In the second stage, seeing the picture where the wallet is hidden is related to remembering (key). This sequence is reversed in extended experiments. In extended experiments, after the subjects have made their choices, the sequential presentation of the cards should be aimed at remembering the choices made. On the other hand, changing the order of the cards forced the subjects into an involuntary task scheme to wait for the display of the cards of their choice. In this case, the recordings in the extended experiments were in the form of remembering to task. The new concepts, such as undetermined padlock, non-invasive imposed recall, and task–remembering, were used at different stages for useful inferences.

6. Conclusions

The new concepts introduced are used for the validity of the imposed recall hypothesis, a secondary method for proving the relationship between padlock and key recordings, and the detection of a behavioral feature of whether choices are decided even before subjects are directed to make their card choices in extended experiments. The Granger causality is used to draw inferences.

In the preliminary experiments, it was necessary to have data without imposed recall in order to determine the effects of exposing subjects to imposed recall in the first stage. Padlock records of the preliminary experiments compared with the undetermined padlock records obtained from the extended experiments revealed an interesting point. The Granger causality applied to the padlock records of the preliminary experiments did not produce any trend similarity. However, the Undetermined padlock records of the subjects in the extended experiments showed a lot of similar trends. The inferences made at this stage showed the effectiveness of both the concepts introduced in the construction of the experimental mechanism and the success of imposed recall in separating the data.

Secondarily, the concepts of non-invasive imposed recall and task–remembering were key to the success of the secondary method in proving the relationship between padlock and key recordings. In the preliminary experiments, padlock recordings were obtained in which imposed recall involved tasking in the first stage. Then, the pictures were shown to the subjects again and the resulting key recordings were part of the remembering concept. In the extended experiments, imposed recall was not directly presented, which led to the opposite emergence of the task–remembering aspect. When the Granger causality is applied

to the padlock–key records of the preliminary and extended experiments, evidence for the existence of the counterfactual is obtained. In this way, the effective role of imposed recall in structuring, focusing, and accurately predicting consequences on the data is demonstrated. Indeed, the changes in success rates between the two experiments were highly divergent. After analyzing the resulting data with the Granger causality, all expectations were met. In this way, the validity of the imposed recall hypothesis was demonstrated.

7. Future Works

With the revelation that structured signals can capture the matches of brain signals on subjects at different time intervals, steps have been taken in studies that can be carried out in different domains. In future work, we will put forward an approach that can be beneficial in various fields such as education, criminal investigation, entertainment, digital and physical security, and military fields. We must assume that more than one suspect at a crime scene is in a state of denial. Recreating the crime scene using virtual reality or augmented reality and matching the suspects' brain frequencies when seen in the virtual crime scene can reveal the real culprit. In another scenario, cyber attacks could be carried out. Let us consider an individual who refuses to share a password during questioning. A neural brute-force attack will be revealed by projecting continuously changing password combinations on the screen and examining the brain signal intensity levels when the data obtained with the EEG device is analyzed in real-time. Undoubtedly, the studies can be extended considerably because the ability to observe neural signal pairings revealed by the imposed recall hypothesis approach based on ironic process theory provides the ability to adapt to broad insights.

Author Contributions: Conceptualization, A.F.A. and C.V.; methodology, A.F.A.; software, A.F.A.; validation, C.V., N.K.S., A.R., V.V.P. and M.K.; formal analysis, C.V.; investigation, A.F.A.; resources, A.F.A.; data curation, C.V.; writing—original draft preparation, A.F.A.; writing—review and editing, C.V.; visualization, A.F.A.; supervision, N.K.S., A.R., V.V.P. and M.K.; project administration, C.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author due to confidentiality agreement for EEG data of individuals. Limitations may be imposed on approved data sharing requests in order to protect the privacy of individuals.

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

References

1. Ranger, S. *What Is the IoT? Everything You Need to Know About the Internet of Things Right Now*; ZDNET: Tokyo, Japan, 2020.
2. Hasan, M. *State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally*; IoT Analytics: Hamburg, Germany, 2022.
3. Goasduff, L. *Global Government IoT Revenue for Endpoint Electronics and and Communications to Total $21 Billion in 2022*; Gartner: Stamford, CT, USA, 2021.
4. Bamiduro, W. *Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018*; Gartner: Stamford, CT, USA, 2018.
5. Zhang, C.; Shen, T.; Bai, F. Toward Secure Data Sharing for the IoT Devices With Limited Resources: A Smart Contract-Based Quality-Driven Incentive Mechanism. *IEEE Internet Things J.* **2023**, *10*, 12012–12024. [CrossRef]
6. Farooq, M.U.; Waseem, M.; Khairi, A.; Mazha, S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6. [CrossRef]
7. Aydogan, A.F.; Varol, C.; Rasheed, A.; Shashidhar, N.K. A Review of Encryption Techniques in IoT Devices. *Int. J. Secur. (IJS)* **2023**, *14*, 17–37.
8. Bontrager, P.; Roy, A.; Togelius, J.; Memon, N.D.; Ross, A. DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9.
9. Korshunov, P.; Marcel, S. DeepFakes: A New Threat to Face Recognition? Assessment and Detection. *arXiv*, **2018**, arXiv:1812.08685.
10. Hamilton, A. *Elon Musk's AI Brain Chip Company Neuralink Is Doing Its First Live Tech Demo on Friday. Here's What We Know So Far About the Wild Science Behind It*; Business Insider: Amsterdam, The Netherlands, 2020.

11. Pap, I.A.; Oniga, S.; Alexan, A. Machine Learning EEG Data Analysis for eHealth IoT System. In Proceedings of the 2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 21–23 May 2020.
12. Abdellatif, A.A.; Khafagy, M.G.; Mohamed, A.; Chiasserini, C.F. EEG-Based Transceiver Design with Data Decomposition for Healthcare IoT Applications. *IEEE Internet Things J.* **2018**, *5*, 3569–3579. [CrossRef]
13. Jo, G.H.; Jeon, S.B.; Chung, H.; Song, Y.J. Sensor Data Analysis and Visualization of IoT System for Combat Helmet. *Adv. Sci. Lett.* **2017**, *23*, 10342–10345. [CrossRef]
14. De Buyser, E.; De Coninck, E.; Dhoedt, B.; Simoens, P. Exploring the Potential of Combining Smart Glasses and Consumer-Grade EEG/EMG Headsets for Controlling IoT Appliances in the Smart Home. In Proceedings of the 2nd IET International Conference on Technologies for Active and Assisted Living (TechAAL 2016), London, UK, 24–25 October 2016.
15. Carrasquilla-Batista, A.; Quirós-Espinoza, K.; Gómez-Carrasquilla, C. An Internet of Things (IoT) Application to Control a Wheelchair Through EEG Signal Processing. In Proceedings of the 2017 International Symposium on Wearable Robotics and Rehabilitation (WeRob), Houston, TX, USA, 5–8 November 2017.
16. Alrawi, O.; Lever, C.; Antonakakis, M.;; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019 .
17. Gümüş, A.E.; Uyulan, Ç.; Guleken, Z. Detection of EEG Patterns for Induced Fear Emotion State via EMOTIV EEG Testbench. *Nat. Eng. Sci.* **2022**, *7*, 148–168. [CrossRef]
18. Aydogan, A.F.; Varol, C.; Vanli, A.; Varol, H. A New Security Mechanism for IoT Devices: Electroencephalogram (EEG) Signals. In Proceedings of the Proceedings of the Second International Conference on Advances in Computing Research (ACR'24), Lecture Notes in Networks and Systems, Madrid, Spain, 3–5 June 2024; Daimi, K., Al Sadoon, A., Eds.; Springer: Cham, Switzerland, 2024; Volume 956._26. [CrossRef]
19. Rușanu, O.A. The Development of Brain-Computer Interface Applications Controlled by the Emotiv Insight Portable Headset Based on Analyzing the EEG Signals Using NODE-Red and Python Programming Software Tools. In *Open Science in Engineering, Lecture Notes in Networks and Systems*; Auer, M.E., Langmann, R., Tsiatsos, T., Eds.; Springer: Cham, Switzerland, 2023; Volume 763._82. [CrossRef]
20. Emotiv. Technical Specifications—Insight 2.0 Manual. 2023. Available online: https://emotiv.gitbook.io/insight-2-user-manual/introduction/technical-specifications (accessed on 1 January 2023).
21. Grummett, T.S.; Leibbrandt, R.E.; Lewis, T.W.; DeLosAngeles, D.; Powers, D.M.W.; Willoughby, J.O.; Pope, K.J.; Fitzgibbon, S.P. Measurement of Neural Signals from Inexpensive, Wireless and Dry EEG Systems. *Physiol. Meas.* **2015**, *36*, 1469. [CrossRef] [PubMed]
22. Velleman, D.J. The Generalized Simpson's Rule. *Am. Math. Mon.* **2005**, *112*, 342–350. [CrossRef]
23. Cheadle, C.; Vawter, M.P.; Freed, W.J.; Becker, K.G. Analysis of microarray data using Z score transformation. *J. Mol. Diagn.* **2003**, *5*, 73–81. [CrossRef] [PubMed]
24. Do, C.B.; Batzoglou, S. What is the expectation maximization algorithm? *Nat. Biotechnol.* **2008**, *26*, 897–899. [CrossRef] [PubMed]
25. Xiang, S.; Nie, F.; Zhang, C. Learning a Mahalanobis distance metric for data clustering and classification. *Pattern Recognit.* **2008**, *41*, 3600–3612. [CrossRef]
26. Subramaniyam, N.P.; Hyttinen, J. Characterization of Dynamical Systems Under Noise Using Recurrence Networks: Application to Simulated and EEG Data. *Phys. Lett. A* **2014**, *378*, 3464–3474. [CrossRef]
27. Cohen, M.X. *MATLAB for Brain and Cognitive Scientists*; Amsterdam University Press: Amsterdam, The Netherlands, 2017.
28. Gonthier, P.; Bernardi, E.; Pecoraro, L.; Garbelotto, M. Selection processes in simple sequence repeats suggest a correlation with their genomic location: Insights from a fungal model system. *BMC Genom.* **2015**, *16*, 1–12. [CrossRef] [PubMed]
29. Moore, D.S. Tests of chi-squared type. In *Goodness-of-Fit Techniques*; Routledge: London, UK, 2017; pp. 63–96.
30. Sur, P.; Chen, Y.; Candès, E.J. The likelihood ratio test in high-dimensional logistic regression is asymptotically a rescaled chi-square. *Probab. Theory Relat. Fields* **2019**, *175*, 487–558. [CrossRef]