USER AUTHENTICATION AND CRYPTOGRAPHY USING BRAIN SIGNALS – A SYSTEMATIC REVIEW

Vaibhavi Lakhani, Vraj Baxi
•
Department of Computer Engineering
G H Patel College of Engg. & Tech.
Gujarat Technological University
vaibhavilakhani1999@gmail.com

Abstract

Human brain cells communicate with each other through electrical impulses and this electric field is measured by an electroencephalogram (EEG). These signals are individually unique and non-trivial to collect and henceforth it has emerged as a powerful and most reliable amongst the other biometrics due to its profoundly unique nature, which makes it impracticable to steal or mimic. The brain waves or signals can be utilized as biometric authentication to provide a secure and robust data exchange. In this paper, analyzing the active portions and the various states of the human brain to generate the cryptographic keys from brainwave signals are reviewed to provide better security to the data. This review also facilitates the user-authenticating ability of an EEG-based person authentication (EBPA) system when clients are in a variety of brain states during performing mental tasks to login.

Keywords: EEG; Brain Wave Signals; Authentication; Cryptography; Crypto-biometric System; Biometric System

I. Introduction

The interaction between humans and computers is at the periphery of a great leap forward with direct contact via a brain interface. Brain-based Computer Interface (BCI) is a fast-growing, emerging technology with applications in Virtual Reality, health tracking, medicine, mobile cloud computing, and robotic control. One of the major topics in this field is to ensure security and privacy when humans and machines are communicating digitally with brain signals. Brain-computer interface (BCI) and brain-machine interface (BMI) systems are systems that "*give their users communication and control channels that do not depend on the brain's normal output channels of peripheral nerves and muscle.*" [1].

BCI technology helps its users to communicate without physical force but through brain movements with computerised controls [2]. Personal privacy and security issues need to be highly valued when attempting to interact with a brain interface. Therefore, continuous authentication and on-demand authentication in the field of biometrics are proposed. Brain-computer interfaces can be classified into three main groups: Non-Invasive, Semi-Invasive, and Invasive Invasive [3]. In invasive techniques, special devices have to be used to capture data (brain signals), these devices are inserted directly into the human brain by a critical surgery [4, 5]. In Semi-invasive, devices are inserted into the skull on the top of the human brain. In general, non-invasive are considered the

safest and low-cost types of devices [4, 5]. However, these devices can only capture "weaker" human brain signals due to the obstruction of the skull. The detection of brain signals is achieved through electrodes placed on the scalp [3, 4, 5].

There arenumerous ways to develop a non-invasive brain-computer interface referred to as neuroimaging [6], such as EEG (electroencephalography), MEG (magnetoencephalography), or MRT (magnetic resonance tomography). An EEG-based brain-computer interface is the most preferred type of BCI for studying. EEG signals are processed and decoded in control signals, which a computer or a robotic device comprehends readily [6]. The processing and decoding operation is one of the several complicated phases of building a good-quality BCI [6-7]. EEG along with BCI allows a person to control external devices or the neuroprosthetic applications (it helps disabled patients to control prosthetic limbs by thinking about the movements).

This paper is divided into several sections: Section 1 is the introduction; Section 2 describes the study related to types of brainwaves; Section 3 comprises the description of EEG and analysis of its data collection; Section 4, we understand the method of user authentication followed by biometric cryptography in section 5, while Section 6 explains the benefits and drawbacks of the crypto-biometric systems that are discussed extensively in this review; Section 7 concludes this paper followed by references.

III. Understanding the Brain

1. Different Types of Brainwaves

Brainwaves are generated by synchronized electrical pulses from masses of neurons communicating with each other. Brainwaves are detected using sensors placed on the scalp. These electrical activities vary on what a person is doing. There is much difference between the brainwaves of a sleeping person with the brainwave of a person is wide awake. The mental state of a person can be examined by observing a brainwave pattern [9].

For extreme anxious people produces high beta waves, while a person who has ADD/ADHD produces slow alpha/theta waves. According to [9], the bands of frequencies are the ones responsible for defining each rhythmic activity and are divided as follows:

- Delta: (0.2Hz-3Hz) refers to deep dreamless sleep
- Theta: (3Hz-8Hz) represents the light sleep and extreme relaxation.
- Alpha: (8Hz-12Hz) refers to an awake person but relaxed.
- Beta: (12Hz-27Hz) refers to the wide awake.
- Gamma: (27Hz-higher) represents a high level of focus and concentration in the individual.

On the another hand, the mental state of the object plays an essential role in defining the frequency, which leads to giving a wave classification that is highly related to the state of mind of the subject [9]. An example of a human brain electrical scan can be found in Figure 1 [11] where the image illustrates the more active parts of the brain in red for different waves (clockwise starting from top left: Delta, Theta, Beta, and Alpha) [11].

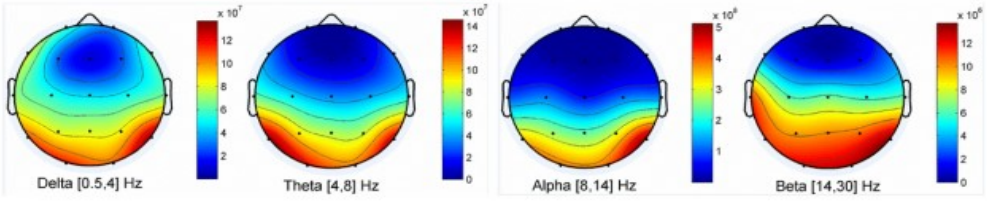

Figure 1: *Brain electrical activity by wave type [11].*

III. Analysis

2. EEG Analysis

Electroencephalogram (EEG) records the brain's electrical activity by measuring the voltage fluctuations on the scalp surface with the simple placement of the electrodes on the skin [14]. Those signals can be influenced by mood, stress, and mental state of the individual [6] which makes them very difficult to be obtained under force and threat. Besides, brain signals are related to the subject's genetic information, making them unique for every individual and stable over time [15]. Hence, brain signals are more reliable and secure and have been proposed as an identification and authentication biometric [16].

EEG-based identification and authentication have been examined often and these preliminary works have demonstrated that the EEG brainwave signals could be used for individual identification and authentication. There are two main approaches used for the analysis of EEG data; these approaches define when and how the data should be analyzed. First is *Event-related Potential Based Technique.* In short, event-related potentials (ERPs) are neural activities that occur as results of stimuli, responses, or decisions. In general, ERPs are used to study neural activities as a response to various stimuli, both physical and mental, and are investigated in many different research fields [12]. Second is *Resting State-Based Technique.* A resting-state EEG recording is a recording obtained when using a device to monitor someone's brain when he/she is not reacting to any kind of stimuli, and it is usually acquired when the subject is not moving or thinking of anything in particular [13].

3. Data Collection and Analysis

The EEG dataset used in this study of [2] was gathered at Pace University. The experiments were conducted with 32 volunteers ranged in ages between 20 and 35, and had a college degree. 13 of the participants were female and 19 were male. All of the participants had normal or corrected to normal vision. Over 70% were daily consumers of caffeine; either from coffee or black/green tea. Before the experiments, participants were required to have a good sleep the night before (at least 5 hours). The average amount of sleep was 7.14 hours.

The EEG signals were measured using 8-channel EEG sensors and 2 Cyton board reference sensors to receive the data. The EEG sensors were placed at the Fp1, Fp2, C3 , C4, Cz, Pz, O1, and O2 channels. The measurement data were measured at 200Hz for a 60-second resting state with eyes closed for 30 seconds, then eyes opened for 30 seconds. A 2-minute length video was started after the resting period. The streaming of EEG data was captured using the OpenBCI GUI application. After data streaming ends, a text file is often created containing float (converted from analogue signals) 8-channel data along with millisecond (ms) timestamps [2].

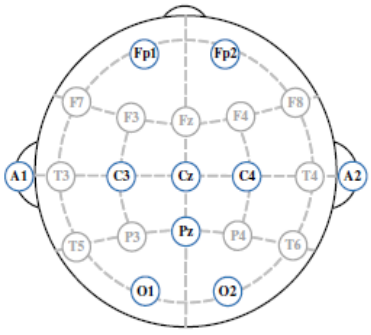

Figure 2: *Chosen Electrodes Locations on OpenBCI Headset [2]*

IV. User Authentication

1. Authentication Model

The brain biometric authentication system typically has two parts: the data acquisition part and the decision part. Fig. 3 [2] illustrates the general approach of an authentic brain biometric system. In the data acquisition stage, EEG sensors capture brain electrical activity, while the user engages with some protocols, such as resting, pass-thought, visual stimulation, or imagery. Data are transferred for digitization and decision-making; this can occur wirelessly or with wired sensors. Once the data are digitized, the decision-making stage begins. The first step in decision-making often involves signal preprocessing to enhance signal quality [26]. Then various computational features are extracted. When the feature set has been determined and confirmed, the biometric computations are performed. These may be simple statistical analyses or more complex machine learning approaches (e.g., Neural Network [NN], Support Vector Machine [SVM]). When the system is performing authentication, its output will be a binary acceptance/rejection [26].

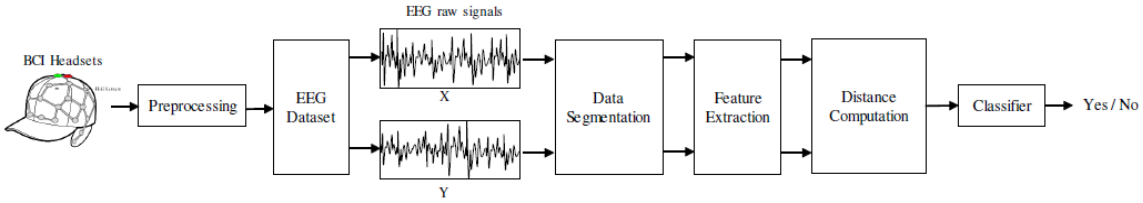

Figure 3: *EEG authentication model [2].*

2. Authentication

Today, multiple companies have a dataset containing some biometrics, which is used to track an employee's work hours and prevent unauthorized people from entering the company's premises. A good biometric for authentication should minimally achieve the following requirements [17]: Universality, Distinctiveness, Permanence, Collectability, Acceptability, Performance, and Anti-circumvention.

Table 1 is a shorter version of a table presented in Jain Ross and Prabhakar [17], which presents a comparison of different biometric identifiers based on the requirements listed above. [18] added "Cost" because the price affects the popularity of the biometric. "L" means several hundred dollars, "M" means several thousand dollars, and "H" is over $10,000 ("NA" means that to the best of our knowledge, there is no such system available) [18].

Using EEG signals for authentication purposes provides distinctive benefits such as requiring the clients to be alive when recording, being unintrusive and impossible to mimic [19] As a result, an EEG-based person authentication (EBPA) system includes merits of both password-based and biometric-based ones but excludes their disadvantages. Due to those interests, a variety of EEG modalities, different features, and classification algorithms have been proposed [20]. [21] proposes an EBPA system in different brain states as illustrated in Figure 4 in order to speculate on how different affective states impact on this system. In the enrolment phase, each user's brain-wave is elicited by stimuli when that user is in a variety of brain states, namely like, dislike, familiar, and unfamiliar.

EEG data corresponding to those experienced states are first processed and then features are extracted. These features are then utilized to train the models for that user.

During the verification phase, EEG signals corresponding with different brain states of each user are recorded, processed, and features are extracted similarly to the enrolment phase. Then the extracted features are provided to the classifier as different testing datasets to calculate matching scores. Based on those scores, the system decides to accept the true client or reject the imposter. This decision is used to evaluate the influence of various human affective states on the performance

of an EBPA system.

Similar to like and dislike brain states, the longer epoch data are used, the lower EER value the authentication system can obtain with the unknown affective state. The performance of an EBPA system is judged by Decision Error Trade-off (DET) curve, in which the x-axis presents False Rejection Rate (FRR) and False Acceptance Rate (FAR) is shown on y-axis [21]. When the system has multiple DET curves corresponding with different brain states, the value at the point where FAR and FRR are equal, so-called Equal Error Rate (EER), is used to manage the smaller EER value or the lower DET curve, both meaning a better system.

The data of the three typical sub-bands, namely alpha (4-12Hz), beta(12-30Hz), and gamma (30-45Hz) were filtered, extracted features, and then separately fed into the classifier.

Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Anti-Circumvention	Static/ Dynamic	Cost [ab]
Ear	M	M	H	M	M	H	M	S	L
Face	H	L	M	H	M	H	L	S	M
Finger-print	M	H	H	M	H	M	M	S	L
Hand geometry	M	M	M	M	M	M	M	S	L
Iris	H	H	H	M	H	L	H	S	L
Voice	M	L	L	M	L	H	L	D	L
DNA	H	H	H	L	H	L	H	S	NA
Retina	H	H	H	M	H	L	H	S	L
Mouse move-ment	L	M	L	H	M	H	H	D	NA
Hand-writing	L	M	L	L	M	H	H	D	NA
Key-stroke dynamics	M	M	L	H	M	M	H	D	L
Brain-waves	H	M	L	M	H	M	H	S/D	NA

Table 1: *A* Comparison of Biometric Identifiers (L/M/H) [18]

Gui et al[16] proposed a general framework for EEG- Based User authentication. They used a single noise channel for noise reduction by ensemble averaging and low pass filter. Wavelet packet decomposition was used for feature extraction and then a neural network was adopted for classification. Four different scenarios were discussed to emulate different cases in the authentication. The SCENARIO I of identifying all the 32 subjects had the worst accuracy ranging from 5.75% to 10.68%. The hidden layer of 25 neurons had the best accuracy and increasing the neurons did not help improve the performance. SCENARIO II using the side-by-side method showed better performance at identifying all the 32 subjects. The accuracy for 32 sub-models varied from 28.71% to 36.27% and 40 neurons got the highest accuracy of 36.27%. When using fewer neurons, the accuracy decreased to about 31% to 33%. SCENARIO III was the case of identifying

one specific person from others. The hidden layer of 45 neurons had the best average accuracy of 94.04%. Increasing or decreasing the neuron number did not change the accuracy too much. SCENARIO IV was testing the case of identifying a small group of individuals from others. The 496 cases were to identify the specific 2 persons from the other remaining 30 subjects. With 20 neurons in a hidden layer, the accuracy was the highest of 90.03%. The minimum accuracy was 70.06% and the maximum is 99.2%. They concluded that the side-by-side method improved the performance of identifying all the subjects as mentioned in Fig. 6. Due to the improvement in the training datasets, the classification rates reached about 33% and 47% and was about 5 times the accuracies of identifying all the 32 subjects.

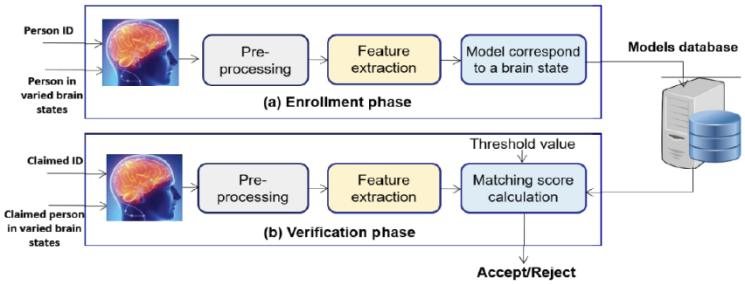

Figure 4: *exhibits the performance of the authentication system in different brain states for each brain wave band [21].*

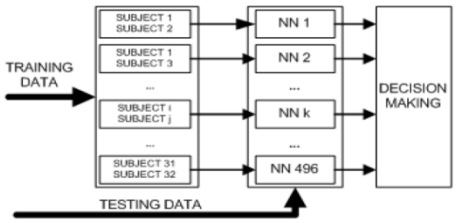

Figure 6: *General Structure of Side-by-Side Method [16]*

V. Cryptography

1. Cryptography Model

To perform key generation some sort of tasks are given to the sender and analyzing the brain signal based on input tasks. After analyzing the brain waves finds out dominant waves generate binary value equivalent. At the receiver side, the same activity will be used for checking analyses of brain waves which is passes to the signal to the binary converter and produces a key. That key will be used for decrypting the ciphertext. So none other than the sender can retrieve the secret information [9]. This cryptographic scheme will be applicable when any confidential data stored in the central database can be secured using a brain signal as a biometric. In the novel approach [9] fig 7(a) entitles about the security of saving cryptographic keys by using the key binding technique with the help of brain waves generated from neuron actions in the brain.

After binding key with brain signals which will be stored as a secured template. The secured template will be further analyzed for the verification phase. In verification phase inputting brain waves and features are extracted from the input opposite of key binding called key releasing will happen reproduces the correct key if the inputting brain wave will be valid, otherwise error key will appear and it will cause an error while the decryption process. Fig 7 (b) [9] represents a biometric key generation from brain waves of different mental activities of the same person. In this approach initially, brain signals are captured using sensors then it is given to the feature extraction stage. Here relevant features are extracted and those extracted features were responsible for the generation of brain biometric key [9].

In terms of computer science and information security, cryptography is usually associated with

the process of making plaintext (ordinary processable data) into ciphertext (encrypted unreadable data) and vice versa. Several methods of generating, binding, and storing private keys using biometrics have been developed. These cryptosystems are called crypto-biometric systems [22]. The first example of an EEG-based cryptosystem was created in 2007 [23]. It used an EEG scan performed with 61 electrodes to generate a 61 bit key to randomize a Huffman tree, which was then used to encrypt the data. The recording was done while the subject was focusing on a picture containing black and white stripes. This experiment was conducted with 10 subjects, and 40 EEG scans were extracted at various times. The true positive (correct decryption by the genuine subject) rate was 82.05–100%, and the true negative rate (correct decryption by the impostor subjects—not the one whose scan was used for encrypting the image) was lower than 27.22%, but the most important feature of this encryption is that each EEG recording is one second long. For encryption key generation, recorded signal is converted into filtered signal and the energy is computed from the signal which is normalised for further use.

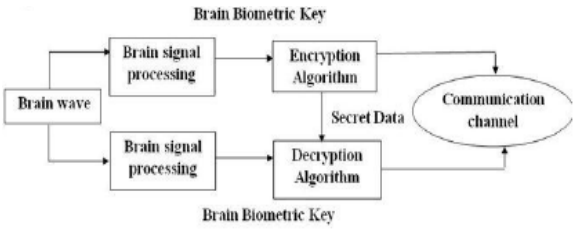

Figure 7(a): *Key binding using brain waves [9]. [9].*

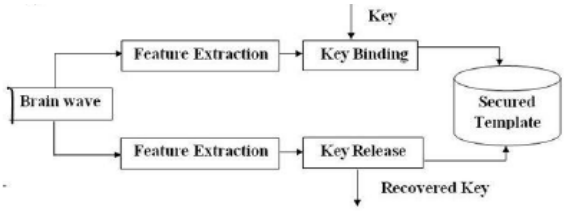

Figure 7(b): *Biometric key generation from brain waves*

Bajwa and Dantu [24] suggested a key generation method using EEG scans for user authentication and encryption, but they didn't conduct an encrypting experiment. They also showed promising results, using a single key for both authentication and cryptography, and provided a discussion about the trade-offs between accuracy and complexity.

Tuiri et al [25] proposed two symmetric cryptographic algorithms that are considered to fulfill the unique biometric sequence. They used two key generation techniques such as Diffie-Hellman based key exchange and AES based key generation scheme. The system applied SVM as a classifier for accuracy and ability to separate the classes using the concept of hyperplane separation to the data, mapping the predictors onto a new, higher-dimensional space in which they can be distributed linearly. False Acceptance Rate (FAR): is the measure of the likelihood that the Neuro key system will incorrectly accept the derived key from an unauthorized user. False Rejection Rate (FRR): is the ratio of the number of times the Euro key system will incorrectly reject the derived key of a genuine user to the total attempts. As for increasing the accuracy and decreasing the amount of data to work on, a spectra based electrode selection is performed for each subject. In subject classification measurements, the F-measures and the ROC res are calculated using Support Vector Machine and Bayesian Network; the experiment has achieved an accuracy of 97.5% for the SVM classifier, and 95.6% for the Bayesian Network. The Diffie-Hellman exchange generated key has given an HTER (half total error rate) mean rate of 3.4% averaged over the subjects and the electrodes. As for the AES base biometric crypto-key, the rate was higher, 4.1% for the same activities.

VI. Benefits and Drawbacks

Crypto-biometric systems have several unique advantages as compared to other conventional biometric systems used today. First of all, to able to produce EEG signals, one has to be alive and in a conscious state. However, biometrics such as DNA, fingerprints, face can be preserved after several hours of death. Secondly, electrical brain operations are taken into account by calculating

the voltages that decrease significantly over the distance. Hence, the electrodes must either be on or near the consumer to calculate the voltage. So, the key password created by the user cannot, therefore, be used without user awareness. Thirdly, EEG signals are very sensitive to the state of mind mentioned in the above-discussed sections. Therefore, any attempt of oppression that could trigger the user into discomfort will invalidate the crypto-biometric. Finally, a consumer cannot reveal a biometric feature unless they are not aware of it. Thus, high-precision identification with the non-volatile EEG feature can be achieved. These crypto-biometrics, given many such advantages mentioned above, have the potential to be used for authentication and security.

Despite the many proponents, these are still not commonly accepted because extensive research still needs to be carried out. As the brain is continuously active, many background signals of interest may superimpose each other when the neurons are responding to a variety of tasks. So, the difficulty may arise in finding the location of the origination of these response signals. Also, as the signals generated are weak on the scalp hence the acquisition of EEG signals is very sensitive to endogenous and exogenous noise. Hence a much detailed understanding of frequency localization, optimal sensor location depending on employed acquisition protocol, and discriminative information are required. They may also pose some drawbacks in user acceptability in which there are some worries related to "mind-reading" and emotional analysis by the data controller. This may make the user uncomfortable. While using EEG biometrics, the target response from the brain needs to be outlined by using specific protocols. A major limitation of the EEG signal is when people wear a gaming headset that uses EEG. In this scenario, if an individual is performing a bank transaction and the hackers may monitor the bank password, then the money can be credited into the hacker's account. Thus, while Brain signal based authentication has many benefits, the utmost care should always be taken to stay safe from various potential attacks. Furthermore, one of the most important limitations is the user inconvenience when a number of electrodes are placed on the scalp of the user. Hence minimization of the number of electrodes is a critical factor to be considered for user convenience.

VII. Conclusion

In this paper, we presented a survey of brain biometrics, which possess some unique characteristics and advantages over conventional biometrics and thus have gained increasing attention in the community. Initially, we learned the essential knowledge about the brain and how it emulates the electric signals that can be used in various areas. After then, we also examined the different states of the human brain that can affect and influence the behavior of the frequencies and biometric cryptosystems. Furthermore, we learned a brief description of the EEG and its related data collection and analysis. Moreover, there is a profound account of the user authentication models and methods to make the system robust for data transmission. We progressed through many literary works and studied the results for better support. In the following section, we learned about the cryptography of brainwave signals using different techniques such as AES, DES, Huffman tree, etc. Further, there is an overview of the bio-cryptographic system which leads to an easy understanding of the security through brainwave signals. Overall, in the aforementioned review, we examined all the aspects needed for developing a crypto-biometric system for user authentication and security of the data.

References

[1] J. R. Wolpaw, N. Birbaumer, W. J. Heetderks, D. J. McFarland, P. H. Peckham, G. Schalk, E. Donchin, L. A. Quatrano, C. J. Robinson, and T. M. Vaughan, " Brain-computer interface technology: a review of the first international meeting." *IEEE Transactions on Rehabilitation Engineering* 8, 2 (2000), 164–173

[2] Li, S., Savaliya, S., Marino, L., Leider, A. M., & Tappert, C. C. "Brain Signal Authentication for Human-Computer Interaction in Virtual Reality*" 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC),* 2019.

[3] Bhise, P. R., Kulkarni, S. B., & Aldhaheri, T. A., "Brain Computer Interface based EEG for Emotion Recognition System: A Systematic Review,*" 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA),* 2020.

[4] Baher Soliman, Mariam Tadros, Marian Abdel-Shahid, Mina Guirguis, Mina Mikhail, Nadine Shehad, "Brain Computer Interface", Thesis Project Proposal, The American University in Cairo Computer Science Department.

[5] Raymond Carl Smith, "Electroencephalograph based Brain Computer Interfaces", A thesis presented to University College Dublin (NUI) Dublin, Ireland, Feb 2004.

[6] S. Marcel and J. D. R. Millan, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 743–748, 2006.

[7] T. Gasser, P. Bacher, and H. Steinberg, "Test-retest reliability of spectral parameters of the EEG," *Electroencephalography Clin. Neurophysiol.*, vol. 60, no. 4, pp. 312–319, 1985.

[8] Ning Zhuang, Ying Zeng, Li Tong, Chi Zhang, Hanming Zhang, and Bin Yan," Emotion Recognition from EEG Signals Using Multidimensional Information in EMD Domain", BioMed Research International, Vol 2017, pp-09, August 2017

[9] V. Akhila, C. Arunvinodh, K. Reshmi, and K. Sakthiprasad, "A new cryptographic key generation scheme using psychological signals," Procedia technology, vol. 25, pp. 286–292, 2016.

[10] M. Teplan. 2002. Fundamentals of EEG measurement. *Measure. Sci, Rev.* 2, (2002), 1–11.

[11] A. Delorme and S. Makeig, "EEGLAB: An open source toolbox for analysis of single-trial EEG dynamics including independent component analysis," *J. Neurosci. Methods* 134, 1 (2004), 9–21.

[12] S. J. Luck. 2012. "Event-related potentials," In *Handbook of Research Methods in Psychology*. APA, vol. 1, 1–18.

[13] N. Soffer-Dudek, D. Todder, L. Shelef, I. Deutsch, and S. Gordon, "A neural correlate for common trait dissociation: Decreased EEG connectivity is related to dissociative absorption," *J. Personal.* 87, 2 (2019), 295-309.

[14] E. Maiorana, G. E. Hine, D. La Rocca, and P. Campisi, "On the vulnerability of an EEG-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures," In *IEEE 6th Int'l Conf. Biometrics: Theory, Appl. and Syst. (BTAS)*, pages 1-6, Sept 2013.

[15] A. Zquete, Bru. Quintela, and J. P. da Silva Cunha, "Biometric authentication using brain responses to visual stimuli." In A. L. N.Fred, J. Filipe, and H. Gamboa, editors, *BIOSIGNALS*, pages 103–112. INSTICC Press, 2010.

[16] Gui, Q., Jin, Z., & Xu, W. (2014). "Exploring EEG-based biometrics for user identification and authentication." *2014 IEEE Signal Processing in Medicine and Biology Symposium* (SPMB), 2014.

[17] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition." *IEEE Trans. Circ. Syst. Video Technol.* 14, 1 (2004), 4–20.

[18] Ofir Landau, Rami Puzis, Nir Nissim, "Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security" in *Cyber Space , ACM Computing Surveys, Vol 53 Isuue 1.*

[19] T. Pham, W. Ma, D. Tran, D. S. Tran, and D. Phung, "A study on the stability of eeg signals for user authentication. In *2015 7th International IEEE/EMBS Conference on Neural Engineering (NER)*, pages 122–125, April 2015.

[20] Hong Ji Lee, Hyun Seok Kim, and Kwang Suk Park, "A study on the reproducibility of

biometric authentication based on electroencephalogram(eeg) " In Neural Engineering (NER), *2013 6th International IEEE/EMBS Conference* on, pages 13–16, IEEE, 2013.

[21] Tran, N., Tran, D., Liu, S., Ma, W., & Pham, T. (2019), "EEG-based Person Authentication System in Different Brain States" *2019 9th International IEEE/EMBS Conference on Neural Engineering (NER),* 2019.

[22] D. Panchal. 2013. *Bio-Crypto System*. Doctoral Dissertation. Indian Institute of Technology, Kharagpur.

[23] K. V. R. Ravi, R. Palaniappan, and C. Eswaran, "Data encryption using event-related brain signals." In *Proceedings of the International Conference on Computational Intelligence and Multimedia Applications*. Vol. 1, 540-544, 2007.

[24] G. Bajwa and R. Dantu. 2016, "Neurokey : Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms." *Comput. Secur.* 62 (2016), 95–113. 2016.

[25] Tuiri, S. E., Sabil, N., Benamar, N., Kerrache, C. A., & Koziel, G, "An EEG Based Key Generation Cryptosystem using Diffie-Hellman And AES," *2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM),* 2019.

[26] Qiong Gui, Maria V Ruiz-Blondet, Sarah Laszlo, Zhanpeng Jin, "A Survey on Brain Biometrics," *ACM Computing Surveys, Volume 51, Issue 6,*feb 2019.sity Science, 1989.