Security Solutions Using Brain Signals

Anupama.H.S[1], Anusha M[2], Aparna Joshi[3], Apoorva N[4], N.K.Cauvery[5], Lingaraju.G.M[6]
[1]Department of Computer Sc. and Engineering, R. V. College of Engg., Bangalore, India
[2,3,4,5]Department of Information Sc. and Engineering, R. V. College of Engg., Bangalore, India
[6]Department of Information Sc., M. S. Ramaiah Institute of Tech., Bangalore, India

Article Info

Article history:

Received Feb 21, 2018
Revised Mar 7, 2018
Accepted Mar 19, 2018

Keyword:

Brain Signals
Security
Solutions

ABSTRACT

A brain computer interface is a direct neural interface or a brain–machine interface. It provides a communication path between human brain and the computer system. It aims to convey people's intentions to the outside world directly from their thoughts. This paper focuses on current model which uses brain signals for the authentication of users. The Electro-encephalogram (EEG) signals are recorded from the neuroheadset when a user is shown a key image (signature image). These signals are further processed and are interpreted to obtain the thought pattern of the user to match them to the stored password in the system. Even if other person is presented with the same key image it fails to authenticate as the cortical folds of the brain are unique to each human being just like a fingerprint or DNA.

Corresponding Author:

Anupama.H.S
Department of Computer Sc. and Engineering,
R. V. College of Engg., Bangalore, India
Email: anupamahs@rvce.edu.in

1. INTRODUCTION

A Brain-Computer Interface (BCI), often called a Mind-Machine Interface (MMI), or sometimes called a brain–machine interface (BMI) is a direct communication pathway between the brain and an external device [1]. Brain-computer interface (BCI) is an emerging technology which aims to convey people's intentions to the outside world directly from their thoughts [2], enhancing cognitive capabilities. BCIs are often directed at assisting, augmenting or repairing human cognitive or sensory-motor functions. BCIs are used in various applications, such as wheelchair, robotic arm controllers, mental spellers and neuroprosthetics applications which aim at restoring damaged hearing, sight and movement [3].

BCI is collaboration between a brain and a device that enables signals from the brain to direct some external activity. By reading signals from an array of neurons and using computer chips and programs to translate the signals into action, BCI can enable a person suffering from paralysis to write a book or control a motorized wheelchair or prosthetic limb through thought alone. EEG is the signal that is used to acquire the signals from the brain. EEG is a record of the electric signal generated by the cooperative action of brain cells, or more precisely, the time course of extracellular field potentials generated by their synchronous action. Neurons are responsible for sending the instructions generated by brain to various parts of the body. These neurons will pass the instructions from one to another, during this course of action Na+ and K+ ions will react leading to the generation of an electric potential. During every activity such a potential is generated which is measured as EEG.

Security systems involve knowledge based, object based and/or biometrics based authentication. They have shown to be vulnerable to several drawbacks such as simple insecure password, shoulder surfing, theft crime, and cancelable biometrics [15]. Cognitive biometrics or electrophysiology, where only modalities using biosignals (such as brain signals) are used as sources of identity information, gives a solution for those vulnerabilities [16] and [17]. The motivation behind exploring the feasibility of electrophysiology is that biosignals cannot be casually acquired by external observers. They also can be of great value for disabled patients or users missing the associated physical trait [18]. This makes such signals difficult to synthesize and therefore improves the resistance of biometric systems to spoofing attacks. Besides electroencephalogram (EEG), as a biometric modality, could be used to send covert warning when the authorized user is under external forcing conditions, as implemented in [19].

2. PURPOSE/SCOPE/MOTIVATION

The purpose of this work is to develop a biometric security system. A new idea has been proposed to develop this system. This system takes EEG signals recorded during a user's activity as input and authenticates the user. The input EEG waves are processed and a unique signature is generated. This signature is used for user identification. The need for robust security system is increasing day by day. The existing security systems such as passwords, Personal Identification Numbers (PIN), biometric systems which include fingerprint technology, retinal scan are becoming vulnerable to attacks. This is because, passwords and PINs can be guessed by brute force approach, fingerprints can be obtained when an user touches any physical object. However, EEG waves emerging from brain can neither be guessed nor copied. The cortical folds of the brain are unique to each human being just like a fingerprint or DNA [10]. Even though the electrodes are placed on the same position on the brain, the EEG signals for thoughts or actions originate from different parts of the brain leading to a unique signature of a user. This was the motivation for this work. The fact that thought of a person is unique can be used as a password to open a lock like a bank vault or other systems where high level of encryption is necessary.

3. METHODOLOGY

The different stages of BCI are signal acquisition, filtering, feature extraction, classification and external application. They are explained below.

Signal Acquisition: Electroencephalography (EEG) signals are acquired from noninvasive headsets and these readings are stored in a file for further processing. Signals can be acquired from either dry electrodes or gel electrodes. Here in this work headset used is BESS (Brain Electrical Scan System) which is of 16 electrodes. Brain Electrical Scan System - BESS, built over years of research, is a highly sophisticated EEG-ERP system that acquires processes and analyzes bioelectrical activity within the brain. This system is supplied with saline electrodes, which capture the electrical activity in 16 channel configuration with 2 earlobe electrodes and 1 ground electrode as shown in Figure 1.

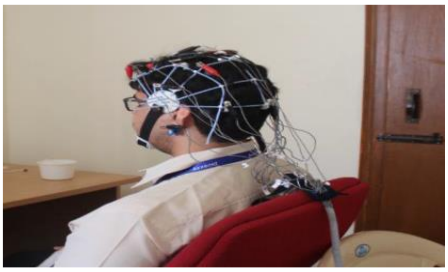


Figure1. BESS saline electrodes

This system contains features to provide the stimulus in multi-modality spectrum. It is used in field of research and has significant clinical application. It can be employed in sectors such as corporate, armed forces as well.

Filtering: Once the signals are acquired it is necessary to filter them in order to remove the noise, external and internal artifacts. Mathematical and statistical methods are used to reduce the noise present in these signals. The digitalized EEG data must be filtered to remove noise and other artifacts using EEGLAB. After the removal of noise, EEG data coming from individual brain activity must be separated and the remaining artifacts must be removed. Running RUNICA module in EEGLAB proves that the test case is a success. The RUNICA module applies ICA on the selected EEG channels; this data after independent component analysis must be obtained in matrix form. If the weighted matrix is obtained then the test case is a success.

Feature extraction: Feature extraction is the process of analyzing the signals to distinguish pertinent signal characteristics. These features form a feature vector which is used as a unique signature. The filtered and processed EEG data must be transformed into frequency domain, using wavelet transformation. The mean signal value will be obtained after wavelet transformation. The EEG signals obtained from multiple channels acts as 2D data, whereas the wavelet transformation can be applied only on 1D signal. Thus data must be given in matrix format and 2D wavelet transformation function must be used on matrix. The data obtained after filtering must be processed further to obtain features and hence generate signature. The signature for each of the person is generated separately.

Classification: The classification step aims at automatically estimating the class of data as represented by a feature vector. Classification of the data is done using machine learning algorithms. Late learners or early learners approach can be used to classify the data. A classification model is created only when a data element is being classified in late learners approach. The k-Nearest Neighbor algorithm falls into this category [11, 12].

External Application: The commands from the classification algorithm are provided to external devices.

4. SYSTEM ARCHITECTURE

EEG based biometric security system is decomposed into sub-systems that provide some related set of services. The design process based on system architecture is concerned with establishing a basic structural framework for a system. It involves identifying the major elements of the system and communications between these elements. Figure 2 shows the existing system architecture.

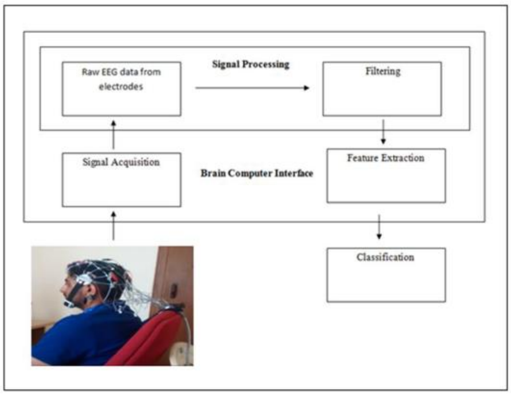


Figure 2. System Architecture

Saline electrodes along with the BESS software is used to record EEG signal transmission. The raw EEG data from electrodes are read using EEGLAB toolbox. These raw data, treated as signals are filtered and then sent for the feature extraction .The features extracted from a feature vector which is used as a unique signature. The final step is where the extracted data is classified in real time using the classification algorithms. The feedback is sent back to the user.

Electroencephalography (EEG) signals are obtained from the electrodes in the form of sensor readings and stored in the file EEG.txt. Only 7 channel values are taken into consideration. Mean of each column of these electrode readings is taken and stored in the database. Once these mean values are stored in the database, the system is ready for prediction. The classification algorithms used is k-Nearest Neighbour algorithm.

The user first trains the device for mentioned number of objects. Not all the values are stored in the database for future reference. To increase decrease the computing time of the overall system, only the mean value of 16 electrode values are taken into consideration and this sequence of mean values are stored as 1 tuple in the database. To ensure that a good data set is acquired, the process of training will be repeated for the same object multiple times with the same user as well as different users. After training the device the user can use the device for prediction. The Classify class is used for prediction. When the user uses the device for prediction, the compare function classifies the obtained data into one of the trained objects by using the user specified classification algorithm. The obtained result is sent as a feedback to user through user interface. The user can train and predict for any object any number of times. The implemented security solution can be broadly represented in the form of a flowchart as shown in Figure 3.

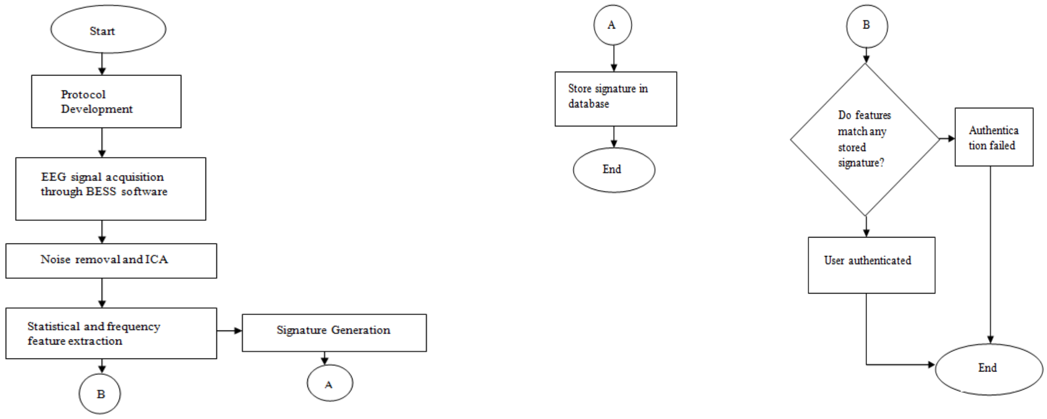

Start
Protocol Development
EEG signal acquisition through BESS software
Noise removal and ICA
Statistical and frequency feature extraction
Signature Generation
B
A
A
Store signature in database
End
B
Do features match any stored signature?
Authentication failed
User authenticated
End

Figure 3. Flowchart of the overall brain signal security solution system

Figure 3 represents flowchart of the entire system. The system begins with protocol development for the collection of EEG signals using SSVEP. This is followed by using the protocol to acquire raw EEG data, and further this data is digitalized, and noise in EEG signals is simultaneously removed. Next step includes feature extraction and signature generation. The signature for each user is unique which is used in authenticating the user.

5. RESULTS AND DISCUSSION

This is an important stage of analysis where the results are analyzed for correctness and matched with the expected output for any anomaly. In Figure 4, raw EEG data which are acquired when the user is displayed with SSVEP protocol is shown.

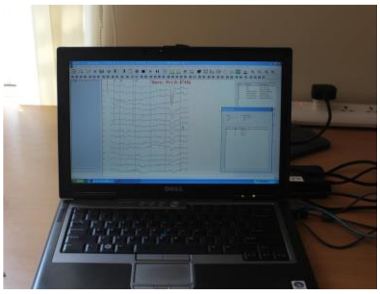
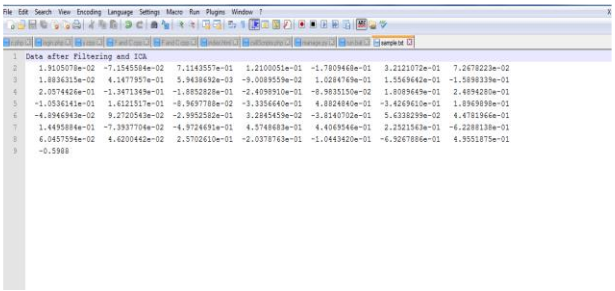


Figure 4. EEG data during acquisition state



```
Data after Filtering and ICA
   1.9105078e-02  -7.1545584e-02   7.1143557e-01   1.2100051e-01  -1.7809468e-01   3.2121072e-01   7.2678223e-02
   1.8836315e-02   4.1477957e-01   5.9438692e-03  -9.0089559e-02   1.0284769e-01   1.5569642e-01  -1.5898339e-01
   2.0574426e-01  -1.3471349e-01  -1.8852828e-01  -2.4098910e-01  -8.9835150e-02   1.8089649e-01   2.4894280e-01
  -1.0536141e-01   1.6121517e-01  -8.9697788e-02  -3.3356640e-01   4.8824840e-01  -3.4269610e-01   1.8969898e-01
  -4.8946943e-02   9.2720543e-02  -2.9952582e-01   3.2845459e-02  -3.8140702e-01   5.6338299e-02   4.4781966e-01
   1.4495884e-01  -7.3937704e-02  -4.9724691e-01   4.5748683e-01   4.4069546e-01   2.2521563e-01  -6.2288138e-01
   6.0457594e-02   4.6200442e-02   2.5702610e-01  -2.0378763e-01  -1.0443420e-01  -6.9267886e-01   4.9551875e-01
   -0.5988
```

Figure 5. EEG data after filtering

The EEG signals in the form of sinusoidal waves are acquired directly from the user and are stored. In Figure 5, the EEG data after subjecting to filtering and ICA using MATLAB is shown. The raw EEG data is first subjected to filtering to remove noise and then ICA is applied which gives a weighted matrix. After filtering, features are extracted from the data. Figure 6 represents the feature vector values for the authentic user. It is seen that the features mean, standard deviation, variance, maximum, minimum, zero crossing rate and wavelet transformation mean differs when the values are taken before food and after food. The brain signals generated after food for the same protocol is different from that which are generated before food.

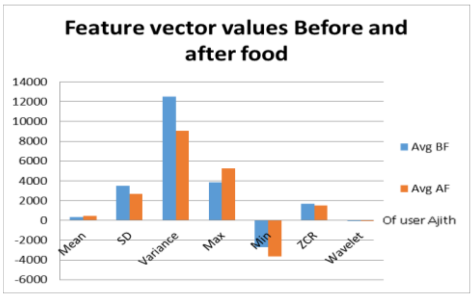


Figure 6. A graph showing comparison between feature vector values for authentic user before and after food

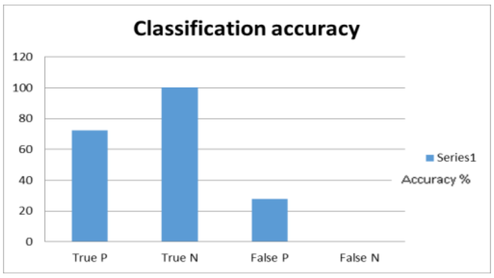


Figure 7. A graph showing true positive, true negative, false positive and false negative values for kNN algorithm

The feature extraction is done for several other users whose EEG data were collected. It is seen that the features mean, standard deviation, variance, maximum, minimum, zero crossing rate and wavelet transformation mean differs from one user to another. It can be observed that variance of three users differs the most. Figure 7 depicts a graph showing true positive, true negative, false positive and false negative values obtained by applying kNN algorithm.

From Figure 7, it is seen that the true positive value for kNN is 72.22%, true negative is 100%. False positive is 27.78% and false negative is 0%. This shows that, the percentage of times system allows wrong user to authenticate is 0%. However, nearly 27.78% of the times the right user also won't be classified as authentic user by kNN.

It is seen that the total accuracy of the system is 77.78%. The percentage of time system identifies right user correctly and denies wrong user is 77.78%. However, nearly 22.22% of the times, system fails to identify the user correctly. The implemented work is able to generate a unique signature for the main subject and authenticate his identity successfully by matching the stored signature with the signals recorded during testing/runtime. The match is successful regardless of external conditions such as time of the day and internal conditions such as anxiety, hunger etc. The system gives a negative result for the signals for the remaining two subjects, thus giving a true negative accuracy of 100%.

6. CONCLUSION AND LIMITATIONS

Over the course of the project, learning on different signal processing techniques, different feature extraction methodologies, different classification strategies etc., has been done. The work presents the techniques that can be used to obtain EEG signals and develop an end to end application by processing these signals. This provides methods to efficiently process EEG signals, remove artifacts without losing relevant information, and obtain features from these signals and classify based on objective. Multiple filtering and feature extraction techniques has been used to obtain an error free, noise free, large signature, which helps in better classification.

The limitations of the product are not negative aspects to the work done. However, no product can fulfill all the needs of the user. With respect to this, the following might be the limitations of this software package. Some important limitations as follows:

a. The system is designed to identify a limited number of users only.
b. The obtained data from the device should be in EDF/ASCII format only.
c. As the EEG waves vary with every activity of the user, training the user for data acquisition beforehand is necessary.

REFERENCES

[1] Avid Roman-Gonzalez, "EEG Signal Processing for BCI Applications, Human Computer Systems Interaction: Backgrounds and Applications", *Advances in Intelligent and Soft Computing*, 2012.

[2] Anupama, H.S, Cauvery, N.K and Lingaraju, G.M, "Brain computer interface and its types - a study", *International Journal of Advances in Engineering & Technology*, May 2012.

[3] Patrick Carberry, "Brain Computer Interfaces (BCI) and Neuroprosthetics", *Biomedical Engineering*, Seminar III, April 7, 2008.

[4]. M. Teplan, "Fundamentals of EEG measurement", *Institute of Measurement Science*, Slovak Academy of Sciences, Dúbravskácesta 9, 841 04 Bratislava, Slovakia, 2002.

[5]. Grant S. Taylor and Christina Schmidt, *"Empirical Evaluation of the Emotiv EPOC BCI Headset for the Detection*

of Mental Actions", 9th Working IEEE/IFIP Conference on Software Architecture (WICSA), 187-193, 2011.

[6] "*Brain-Computer Interfaces, Applying our Minds to Human-Computer Interaction*", Springer London Dordrecht Heidelberg New York- vol.1, Springer-Verlag London Limited, 2010.

[7] Mauss, I. B. and Robinson, M. D., "Measures of emotion: A review," *Cognition and Emotion*, vol. 23, 2009, pp. 209-237.

[8] R. Paranjape, J. Mahovsky, L. Benedicenti, Z. Koles, "*The electroencephalogram as a biometric*", Proceedings of the Canadian Conference on Electrical and Computer Engineering, 2:1363–1366, 2001.

[9] J. Thorpe, P.C. van Oorschot, and A. Somayaji, "*Pass-thoughts: authenticating with our minds*", Proceedings of the 2005 workshop on New security paradigms, New York, 2012.

[10] Lotte F., Congedo M., Lecuyer A, "A review of classification algorithms for EEG- Analysis of Brain Signals References Dept. of ISE, RVCE 2015-16 59 based brain-computer interfaces", *Journal of Neural Engineering*, Vol 4,pp R1-R13, 2007.

[11] K-NearestNeighbour http://saravananthirumuruganathan.wordpress.com/2010/05/17/a-detailed-introduction-to-k-nearest-neighbor-knn-algorithm/ as on March 12th, 2015.

[12] Oliver Sutton, "*Introduction to k NearestNeighbour Classification and Condensed Nearest Neighbour Data Reduction*", February, 2012.

[13] Haider Hussein Alwasiti, IshakAris and AdznanJantan, "Brain Computer Interface Design and Applications: Challenges and Future", *World Applied Sciences Journal* 11, vol 7, IDOSI Publications, 2010.

[14] Pfurtscheller et al., "Current trends in brain computer interface (BCI) research," *IEEE Trans Rehab. Eng.*, vol. 8, pp. 216–219, June 2000.

[15] Khalifa W, Salem A, Roushdy M, Revett K, *"A survey of EEG based user authentication schemes"*, Informatics and Systems (INFOS), 8th International Conference, IEEE, p.BIO–55, 2012.

[16] Karthikeyan DT, Sabarigiri B, "Enhancement of multi-modal biometric authentication based on iris and brain neuro image coding", *Int J Biometrics Bioinform (IJBB)* 2011; 5(5):249–56.

[17] Svogor I, Kisasondi T, *"Two factor authentication using EEG augmented passwords*", Information Technology Interfaces (ITI), Proceedings of the ITI 34th International Conference, IEEE, 2012.

[18] ReveRevett K, Deravi F, Sirlantzis K, "*Biosignals for user authentication towards cognitive biometrics?*" Emerging Security Technologies (EST), 2010 International Conference, IEEE, p. 71–76, 2010.

[19] Su F, Zhou H, Feng Z, Ma J., "*A biometric-based covert warning system using EEG*", In: Biometrics (ICB), 2012 5th IAPR International Conference on IEEE, 2012.

[20] Poulos, M., Rangoussi, M. N., Alexandris, A. and Evangelou, "On the use of EEG features towards person identification via neural networks", *Medical Informatics & the Internet in Medicine*, 2001.