Using Brain Waves as New Biometric Feature for Authenticating a Computer User in Real-Time

Kusuma Mohanchandra *kusumalak@gmail.com*
Associate Professor/Department of Computer Science & Engineering
Dayananda Sagar of Engineering
Bangalore, 560078, India

Lingaraju G M *gmlraju@gmail.com*
Professor/Department of Information Science & Engineering
M S Ramaiah Institute of Technology
Bangalore, 560054, India

Prashanth Kambli *prash.kamblil@gmail.com*
Assistant Professor/Department of Information Science & Engineering
M S Ramaiah Institute of Technology
Bangalore, 560054, India

Vinay Krishnamurthy *vinayk.url@gmail.com*
Student, Department of Computer Science
Stony Brook University
Stony Brook - 11790, NY, USA

Abstract

In this paper we propose an Electroencephalogram based Brain Computer Interface as a new modality for Person Authentication and develop a screen lock application that will lock and unlock the computer screen at the users will. The brain waves of the person, recorded in real time are used as password to unlock the screen. Data fusion from 14 sensors of the Emotiv headset is done to enhance the signal features. The power spectral density of the intermingle signals is computed. The channel spectral power in the frequency band of alpha, beta and gamma is used in the classification task. A two stage checking is done to authenticate the user. A proximity value of 0.78 and above is considered a good match. The percentage of accuracy in classification is found to be good. The essence of this work is that the authentication is done in real time based on the meditation task and no external stimulus is used.

Keywords: Cognitive Biometrics, Authentication, Brain Computer Interface, Electroencephalogram, Power Spectral Density.

1. INTRODUCTION

In this computer driven era, with the increase in security threats, securing and managing the resources has become a more complex challenge. Maintaining and managing access while protecting the user's identity and computer resources has become increasingly difficult. Therefore, it is crucial to design a high security system that has a strong authentication process to authenticate an individual. Authentication, verifying the user, who he claims to be, is the central to all security systems. With the world getting ready to transit from Graphic User Interface (GUI) to Natural User Interface (NUI) technology, where it is possible to communicate with computers by using touch, gestures, voice, expressions, emotions and thoughts. In this context, we have made an attempt to build an authentication system based on thoughts.

The common authentication approaches are those based on personal identification number (PIN) and password. However, these can be easily compromised by methods such as 'shoulder surfing' [1]. The biometric approaches based on the biological characteristics of humans have distinct advantages over traditional methods, as they cannot be hacked, stolen or transferred from one person to another as they are unique for each person. But, as the biological characteristic of a person change with time and age, it is required to find an alternative biometric trait that can distinguish between individuals. Multimodal fusion for identity verification [2] has shown great improvement compared to unimodal algorithms where they propose to integrate confidence measures during the fusion process. These methods are used either to enhance the performance of a multimodal fusion algorithm or to obtain a confidence level on the decisions taken by the system.

Existing technologies mostly use fingerprints, speech, facial features, iris and signatures as a base for an authentication or an identification system. These traits however, are known to be vulnerable to falsification as it is possible to forge or steal. Therefore, new types of physiological features that are unique and cannot be replicated are proposed [3] for an identification system. This paper focuses its attention to the electroencephalogram (EEG) signal as a biometric. The EEG based biometrics is widely being considered in security sensitive areas like banks, labs and identification of criminal in forensic. It can be used as a component of National e-identity card in government sector, as they have proven to be unique between people.

Brain-computer interface (BCI) is an emerging technology which aims to convey people's intentions to the outside world directly from their thoughts, enhancing cognitive capabilities and is a direct communication pathway between a brain and an external device. A common method for designing BCI is to use EEG signals extracted during mental tasks [4]. EEG is the neurophysiological measurement of electrical activity in the brain recorded by scalp electrodes (sensors) and represents a summation of post-synaptic potentials from a large number of neurons. Studies have shown that Brain wave pattern for each individual is unique and thus can be used for biometric purpose. EEG-based biometry [5] is an emerging research topic. Very little work has been done in this area, focusing more on person identification than person authentication. Person authentication aims to accept or reject a person claiming an identity, i.e. comparing a biometric data to one template, while the goal of person identification is to match the biometric data against all the records in a database [6]. In our work, we have made an attempt to authenticate a system, rather than identification. EEG is used to extract reliable features of brain signals [7]. Brain waves measured by EEG represent a summary of brain electrical activity at a recording point on the scalp i.e. the fusion of delta, theta, alpha/mu, beta and gamma waves in frequency band.

FIGURE 1: User Wearing the Emotiv Epoc Headset.

In this work, we investigate the use of brain activity for person authentication. It has been studied that the brain-wave pattern of every individual is unique [8] and the signals captured through the EEG can be used for biometric authentication. Person authentication aims to accept or reject a

person claiming an identity. An EEG EPOC headset with 14 channels manufactured by Emotiv Inc. is used for signal acquisition. The data acquired from these multi sensors are coordinated and managed to give the desired performance. N. Xiong et al [9], presents a comprehensive review of multi-sensor management in relation to multi-sensor information fusion, describing its place and role in the larger context, generalizing main problems from existing application needs, and highlighting problem solving methodologies. The purpose of data fusion [10] is to produce an improved model or estimate of a system from a set of independent data sources.

We perform data acquisition, feature extraction, matching the feature vector with the stored template all in real time. As data from multiple channels is fusion, we have used Power Spectral Density as a reliable feature [11]. Hence Power Spectral Density is used as the key feature in this work. After obtaining the features, Principal Component Analysis (PCA) is performed to obtain relevant features from the high dimensional data. The obtained feature vector is then compared against a previously stored feature vector for the same person using template matching. A two stage checking is done to authenticate the user. A single biometric with multiple matches [12] is considered. The match is considered good if the result of the comparison is greater than the threshold value which has been set to 0.78 after repeated trials keeping in mind the need to satisfy low False Acceptance Error (FAE) and False Rejection Error (FRE). The decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances called as Equal Error Rate [6]. We have developed a GUI, to let a user lock his computer screen when required and unlock the same by recording his brain activity (EEG signals) as a password for the system. This authentication system was successfully demonstrated as a pilot project and proof of concept [13].

An identity authentication system has to deal with two kinds of events: either the person claiming a given identity is the one who he claims to be (in which case, he is called a *client*), or he is not (in which case, he is called an *impostor*). Moreover, the system may generally take two decisions: either *accept* the *client* or *reject* him and decide he is an *impostor* [6]. The main aim is to keep the False Acceptance Error (FAE) and the False Rejection Error (FRE) close to zero. The Education Edition SDK by Emotiv Systems includes a research headset: a (plus CMS/DRL references, P3/P4 locations) high resolution, neuro-signal acquisition by wireless sensors and processing wireless neuroheadset. Channel names based on the International 10-20 locations are: AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8 and AF4. The Education Edition SDK [14] also includes a proprietary software toolkit that exposes the APIs and detection libraries. The SDK provides an effective development environment that integrates well with new and existing frameworks.

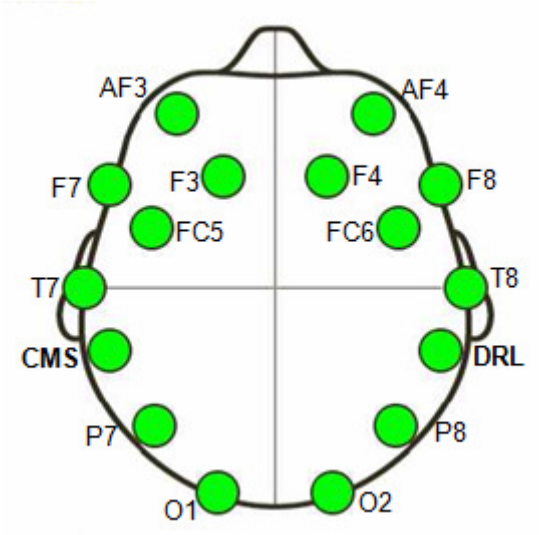

FIGURE 2: Illustration of Location of Electrodes on the Emotiv Headset [14].

2. RELATED WORK

EEG based person authentication was first proposed by Marcel [6]. They proposed the use of Power Spectral Density as the feature, and a statistical framework based on Gaussian Mixture Models (GMM) and Maximum A Posteriori Model (MAP) Adaptation on speaker and face authentication. The potential of their method is shown by simulations using strict train/test protocols and results. Person identification based on spectral information [15] extracted from the EEG is addressed by M. Poulos, et al, . Neural network classification was performed on real EEG data of healthy individuals to experimentally investigate the connection between a person's EEG and genetically specific information. The proposed method has yielded correct classification scores in the range of 80% to 100%, showing evidence that the EEG carries genetic information for person identification.

A novel two-stage biometric authentication [1] method was proposed by Ramaswamy Palaniappan. The feature extraction methodology includes both linear and nonlinear measures to give improved accuracy. Their results show that the combination of two-stage authentication with EEG features has good potential as a biometric as it is highly resistant to fraud. Principal Component Analysis (PCA) is used for dimension reduction of the feature vector keeping only the most discriminatory features, as the features have a high degree of redundancy.

3. METHODOLOGY

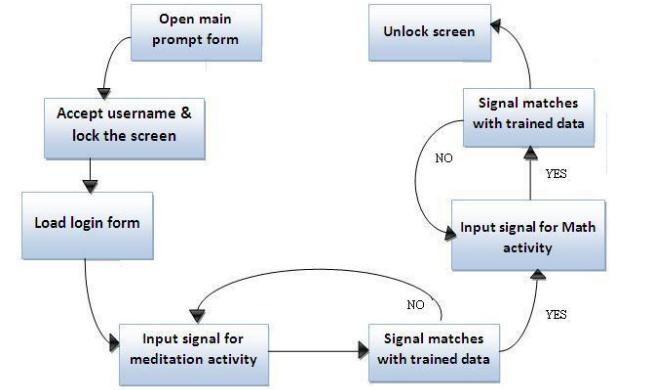

FIGURE 3: Framework of the Model.

A conceptual framework of the present work is shown in figure 3.

3.1 Data Acquisition

EEG signals are recorded with the Emotiv EPOC headset which uses 14 integrated sensors located at standard positions of the International 10-20 system (Fig: 2). Sensors are placed on the scalp using a conductive gel, after preparing the scalp area by light abrasion to reduce electrode-scalp impedance. The sampling rate is 128Hz [16]. The total time of each recording is 10 seconds. The subject is instructed to avoid blinking or moving his body during the data collection to prevent the noise caused due to artifacts [17]. So, no artifact rejection or correction is employed. Artifacts due to eye blinks produces a high amplitude signal called Electrooculogram (EOG) that can be many times greater than the EEG signals required by us [18]. The dataset from normal subjects are recorded for two active cognitive tasks during each recording session.

- *Meditation activity:* The subject is asked to meditate for a fixed period of time while his brain waves are recorded.

- *Math activity:* The subject is given non-trivial multiplication problems, such as 79 times 56 and is asked to solve them without vocalizing or making any other physical movements. The problems were designed so that they could not be solved in the time allowed [19].

3.2 Preprocessing and Feature Extraction

The EEG data is segmented. Channel spectral power for three spectral bands Alpha, Beta and Gamma is computed. 14 x 3 = 42 features are extracted for each segment of the data. PCA is applied to reduce the feature size. The first principal component accounts for as much of the variability in the data as possible, and each succeeding component accounts for as much of the remaining variability as possible [20]. We have considered only those components that contribute to 85% (this value has been chosen after repeated trials) of the total variance for signal matching. The power spectral density (PSD) reflects the 'frequency content' of the signal or the distribution of signal power over frequency [21]. PSD is a positive real function of a frequency variable associated with a stationary stochastic process. It is the measure of the power strength at each frequency. In other words, it shows at which frequencies variations are strong and at which frequencies variations are weak [18]. The unit of PSD is energy per frequency (width). Computation of PSD can be done directly by the method of Fourier analysis or computing auto-correlation function and then transforming it.
The Discrete Fourier transform is given by

$$X(f) = \sum_{i=1}^{N} x(i) w_N (i-1),$$

Where

$$w_N = \exp(2\pi i) / N,$$

is the Nth root of unity. Power spectral density is given by

$$S_x(f) = \frac{1}{N} \sum_{i=1}^{N} | X(f) |^2$$

The channel spectral power is the measure of the total power between two frequencies and is given by:

$$P_{f1,f2} = \int_{f1}^{f2} S_x(f) df,$$

where (f1, f2) is the frequency band and $S_x(f)$ is the power spectral density. The inter-hemispheric channel spectral power differences in each spectral band are given by P_{diff} = (P1 – P2) / (P1 + P2) where P1 and P2 are the powers in different channels in the same spectral band but in the opposite hemispheres.

3.3 Classification

The obtained feature vector is compared against a previously stored feature vector for that subject, using Euclidean Distance for template matching. The match is considered good if the result of the comparison is greater than the threshold value which has been set to 0.78 after repeated trials keeping in mind the need to satisfy low False Acceptance Error (FAE) and False Rejection Error (FRE). A proximity value of 0.78 and above is considered a good match.

3.4 Implementation

The authentication system was realized by developing an application which would lock and unlock the screen. Initially the screen is locked and a subject's EEG signals for two mental tasks

are recorded and stored as a reference, called the training phase. If the screen is to be unlocked, the subject's brain waves are recorded again and matched with the earlier stored sample. If there is a considerable match, then the screen is unlocked, otherwise it will stay locked. The description of the working prototype is outlined as:

- *Training of the system:* The brain waves of the user are recorded when he performs the mental tasks such as meditation and math activity.
- *Feature extraction:* The channel spectral power in the alpha, beta and gamma spectral bands of both the mental tasks is computed. Feature reduction technique is applied, to reduce the dimension of the features.
- *Creating user profile:* These features are stored in a separate file as the user's profile.
- *Authenticating:* The brain waves of the person are recorded in real time for the same set of activities as in the training. Features are extracted from these recorded waves. Feature reduction is performed using Principal Component Analysis and these features are matched with the previously stored features. The feature extraction and matching part are coded in MATLAB, while the UI part is designed and coded in C#. The MATLAB codes are converted to Common Language Runtime (CLR) compliant library (*.dll file). These files are then referenced in C# by means of the *using* statement and adding an appropriate reference.

The User Interface diagram (Fig 4) explains the various stages and steps involved from the user's perspective. It depicts the different forms involved in the application for user interface. The following steps act as a walkthrough for the application.
Step 1: The initial screen which is the main prompt screen (Fig 5) facilitates the user to perform the lock screen, add/remove user, change account name and restore activities.

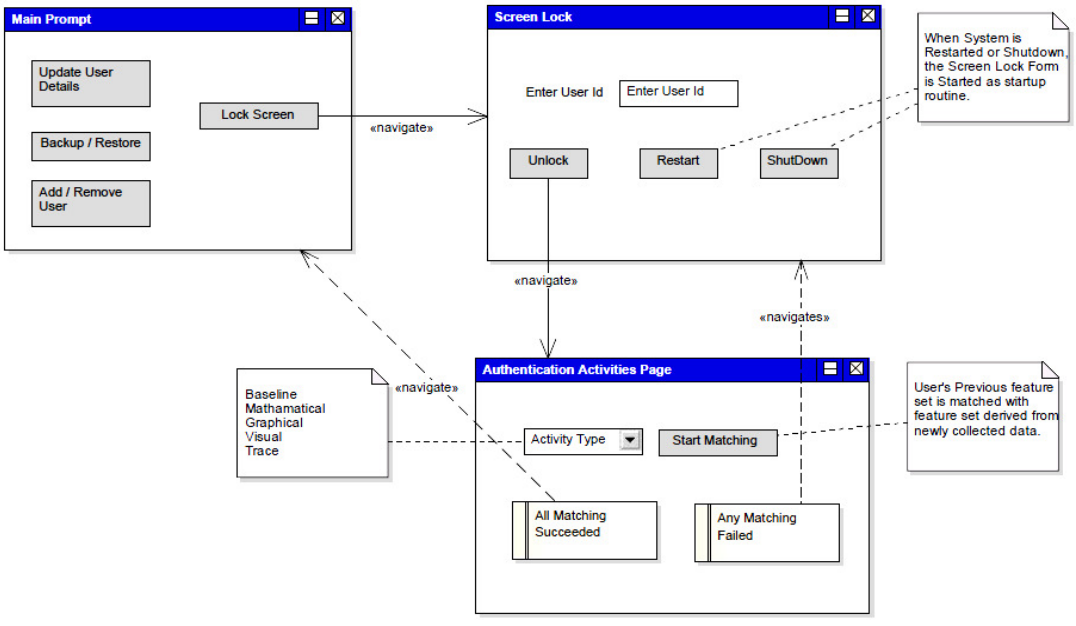

FIGURE 4: User Interface Diagram.

Step 2: We add a new user as there are no existing users initially. The training form opens wherein we train the system for authentication. The training is based on two activities, Meditation and Math activity. While the subject is performing these activities, the signals are recorded and stored.

Step 3: Once the training process is complete, the user returns to the main prompt form (Fig 5). The user can now lock the screen by clicking on the lock screen option. The login form appears wherein user name has to be specified for unlocking the screen (Fig 6). There are 3 available options, Unlock, Restart and Shutdown.

Step 4: When the unlock option is pressed by the user an authentication form appears. Two activities, for which the system has been trained earlier, must be performed for authentication, one after the other.

Step 5: If the authentication is successful then the main prompt form is displayed and the screen is successfully unlocked, else the authentication fails and the screen remains in the locked state.

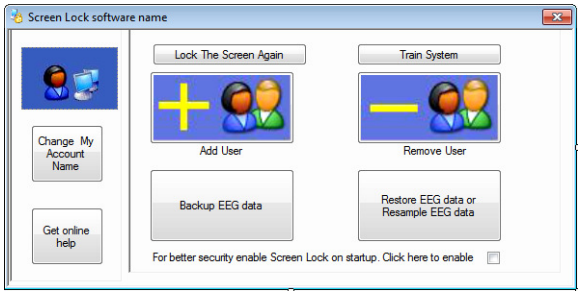

FIGURE 5: Main Prompt Window.

4. CONCLUSION

In this work, we investigate the use of brain activity for person authentication. It has been shown in previous studies that the brain-wave pattern of every individual is unique, and that the EEG can be used for biometric authentication. Person authentication aims to accept or reject a person claiming an identity. We perform EEG recording, feature extraction and matching of the feature vector with the stored feature vector, all in real time. This system seems to be the most reliable system of authentication as it is a type "*What I am"* system rather than the "What I Have" (Iris/Fingerprint scan) or "What I Know" (Password) variants of authentication system. Additionally, this system is designed without using any type of external stimulus. This work, however, needs more refinement such as,

i. Recording must be done in clinical conditions where there are no external interferences (noise free environment).

ii. Training the users to perform the various mental tasks with full concentration.

iii. Handling high dimensional data.

iv. Devising a more or less perfect matching algorithm that gives 0 FAE and 0 FRE.

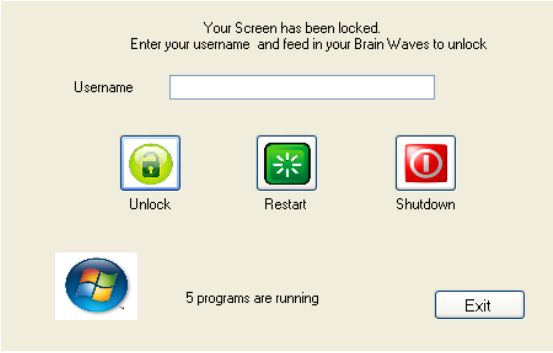

FIGURE 6: User login window

5. REFERENCES

[1] Palaniappan, R. (2008). "Two-stage biometric authentication method using thought activity brain waves." *International Journal of Neural Systems*, *18*(01), pp. 59-66.

[2] Bengio, S., Marcel, C., Marcel, S., & Mariéthoz, J. (2002). "Confidence measures for multimodal identity verification." *Information Fusion*, *3*(4), pp. 267-276.

[3] Abdullah, M. K., Subari, K. S., Loong, J. L. C., & Ahmad, N. N. (2010). "Analysis of the EEG Signal for a Practical Biometric System." *World Academy of Science, Engineering and Technology*, *68*, pp. 2067-2071.

[4] Gürkök, H., & Nijholt, A. (2012). "Brain–Computer Interfaces for Multimodal Interaction: A Survey and Principles." *International Journal of Human-Computer Interaction*, *28*(5), pp. 292-307.

[5] He, C., Lv, X., & Wang, Z. J. (2009, April). "Hashing the mAR coefficients from EEG data for person authentication." *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, pp. 1445-1448.

[6] Marcel, S., & Millán, J. D. R. (2007). "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation." *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *29*(4), pp. 743-752.

[7] Majumdar, K. (2011). "Human scalp EEG processing: Various soft computing approaches." *Applied Soft Computing*, 20*11*(8), pp. 4433-4447.

[8] Dieckmann, U., Plankensteiner, P., & Wagner, T. (1997). "Sesam: A biometric person identification system using sensor fusion." *Pattern recognition letters*, *18*(9), pp. 827-833.

[9] Xiong, N., & Svensson, P. (2002). "Multi-sensor management for information fusion: issues and approaches." *Information fusion*, *3*(2), pp. 163-186.

[10] Gao, J. B., & Harris, C. J. (2002). "Some remarks on Kalman filters for the multisensor fusion." *Information Fusion*, *3*(3), pp. 191-201.

[11] Tao, Q., & Veldhuis, R. (2009). "Threshold-optimized decision-level fusion and its application to biometrics." *Pattern Recognition*, *42*(5), pp. 823-836.

[12] Ross, A., & Jain, A. (2003). "Information fusion in biometrics." *Pattern recognition letters*, *24*(13), pp. 2115-2125.

[13] Lingaraju G M, Kusuma M, Vinay K, Rakshath K, Prakash S Y, Dharini R, "Person Authentication System Using Brain Waves as Biometric", *Conference on Evolutionary Trends in Information Technology*, Visvesvaraya Technological University, Belgaum, India, pp 47, 20-22nd May 2011 (CETIT2011).

[14] http://www.emotiv.com/eeg/features.php

[15] Poulos, M. Rangoussi, N. Alexandris, A. Evangelou, M. (2001). "On the use of EEG features towards person identification via neural networks." *Informatics for Health and Social Care*, *26*(1), pp. 35-48.

[16] del R Millan, J., Mouriño, J., Franzé, M., Cincotti, F., Varsta, M., Heikkonen, J., & Babiloni, F. (2002). "A local neural classifier for the recognition of EEG patterns associated to mental tasks." *Neural Networks, IEEE Transactions on*, *13*(3), pp. 678-686.

[17] Fatourechi, M., Bashashati, A., Ward, R. K., & Birch, G. E. (2007). "EMG and EOG artifacts in brain computer interface systems: A survey." *Clinical neurophysiology*, *118*(3), pp. 480-494.

[18] Hosni, S. M., Gadallah, M. E., Bahgat, S. F., & AbdelWahab, M. S. (2007, Nov). "Classification of EEG signals using different feature extraction techniques for mental-task BCI." In *Computer Engineering & Systems, 2007. ICCES'07. International Conference on* (pp. 220-226). IEEE.

[19] He, C., Lv, X., & Wang, Z. J. (2009, Apr). "Hashing the mAR coefficients from EEG data for person authentication." In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on* (pp. 1445-1448).

[20] http://www.fon.hum.uva.nl/praat/manual/Principal_component_analysis.html

[21] Saa, J. F. D., & Gutierrez, M. S. (2010). "EEG Signal Classification Using Power Spectral Features and linear Discriminant Analysis: A Brain Computer Interface Application." LACCEI'2010, Innovation and Development for the Americas, Jun 1-4, 2010, Arequipa, Perú.