Online Electroencephalogram (EEG) based Biometric Authentication using Visual and Audio Stimuli

Harshit, Rajbir Singh
Computer Science and Engineering
Indian Institute of Technology
Patna, India
{harshit.cs13, rajbir.ee13}@iitp.ac.in

Kavitha P Thomas, Smitha K. G. and A. P. Vinod
School of Computer Science and Engineering
Nanyang Technological University
Singapore
{ptkavitha, smitha, asvinod}@ntu.edu.sg

***Abstract*— Biometric recognition of individuals has been widely employed in establishing secure and trustworthy systems nowadays. However, due to its increased demand and usability, the associated security risks have been increased, which necessitates finding of more robust biometric traits than existing modalities. Recently, brain signal recorded by Electroencephalogram (EEG) technique has been reported as a potential biometric candidate on account of its high degree of uniqueness, stability and universality. This paper presents an EEG-based biometric authentication system employing brain patterns in response to a number of visual or auditory stimuli by seeing/hearing self, familiar and unfamiliar faces/voices. The system employs power spectral density (PSD) features extracted from alpha, beta and gamma bands of EEG for biometric authentication. The PSD values of multi-band EEG signals from 14 channels form template feature vector for each subject, and are stored in the database during enrollment phase. During online authentication, test feature vector is correlated with the respective template vector and the obtained correlation value is compared with a pre-defined threshold value. Based on the authentication experiments performed on 5 healthy subjects, the proposed system offers an overall accuracy of 79.73% with a false acceptance rate (FAR) of 13.91% and false rejection rate (FRR) of 26.6%.**

Keywords—EEG, biometric, authentication and error rate.

I. INTRODUCTION

A biometric system is basically a pattern recognition system which can authenticate or identify a person exploiting his/her physiological and/or behavioural personal characteristics [1]. The system operates by collecting biometric data from an individual, creating feature set from the acquired data, and comparing this feature set against the template saved in the database in order to recognize a person. Upon employing physiological and/or behavioural personal characteristics (finger print, iris, face etc.) in biometric systems, they rely on "something we are" for security enhancement rather than "something we know" (for eg. PIN, personal identification number) or "something we have" in conventional person recognition schemes using access cards [2]. Authentication by "something a user knows" is the most popular authentic mechanism, where a user has to provide both ID and a password. The system is simple, accurate, and effective. However, password based authentication is not immune from malicious attacks such as offline dictionary attack, popular password attack, exploiting user mistakes, and exploiting multiple password use. Authentication by "something a user has" is an authentic mechanism that is based on objects a user possesses, such as a bank card, a smart card, and a USB Dongle etc. This kind of authentication requires users always bringing and providing the physical authentication object when accessing the system. Presenting the foreign object causes inconvenience too. In additional, tokens can be physically stolen, be duplicated, as well as be hacked by engineering techniques [3]. Securing the tokens itself is a challenge. Therefore, a feasible alternative which depends on 'something the user is" is extremely desirable in security enhancement.

A number of biometric features extracted from fingerprint [3], voice [3], palm print [4], hand geometry [5], iris [6], face [7], ear force fields [8], heart signals [9] and odor [10] have been successfully employed in today's real time automatic systems in the area of information retrieval, automatic banking, control of access to security areas, buildings, etc. But they are vulnerable to various kinds of malicious abuse, attack and theft, especially in today's ubiquitous web-enabled environment. The finger-print system, which has been extensively investigated and proved to be scientifically unique across the entire human population, can be easily falsified using artificially generated finger-prints known as "gummy fingers" [11] and it can be obtained by force too. Another popular biometric using face recognition technique can be easily spoofed using printed face models [12]. Hence, it is highly desirable to develop innovative biometric identification/authentication techniques for achieving better information security and more robust communication in both personal and business data management and control.

In order to alleviate the limitations of the existing modalities, the emerging biometric trait based on brain wave has potential capabilities [13]. Electroencephalogram (EEG) technique allows to measure electrical activity of brain waves in a simple way by placing electrodes on the scalp [14]. An EEG recording reflects the summation of the synchronous activities of thousands of millions of neurons that have similar spatial orientation. Electrodes catch the electrical activity of millions of neurons in the brain in units of microvolt and carries representative and meaningful information on the

Sponsored by MOE AcRF-Tier-1 Grant Singapore.

978-1-4673-7791-1/16/$31.00 ©2016 IEEE

subject's specific mental tasks and neural responses. It is the most commonly used non-invasive brain signal acquisition method because of its high temporal resolution, ease of use, low cost and portability. Brain waves recorded by EEG are unique to a particular person and linked to his genetic behaviour. So it is impossible to copy or imitate someone else's EEG patterns.

On account of the unique biometric properties of brain waves, EEG has been exploited widely during the last decade. EEG waves are easily collectible, and feasible to handle with the help of wireless and portable headsets/equipments such as emotive Epoc [15], which are becoming popular in various EEG based applications nowadays. In conventional scalp EEG, EEG recordings are obtained by placing electrodes on various regions of the scalp, according international system of electrode placement. Recorded EEG carries information regarding brain's unique and distinct response corresponding to the given external or internal stimuli. The associated potential change of EEG in response to any stimuli is called as event-related potentials (ERPs) [16]. EEG during brain's rest state or ERPs to visual or audio stimulus have been exploited in EEG based biometric studies [17].

Though many studies explore ERPs associated with visual stimuli termed as Visually Evoked Potential (VEP) in biometric systems, very few studies have investigated the biometric properties of EEG towards audio stimulus. Also there are no studies related to biometric systems investigating combined use of visual or audio stimuli which can improve the robustness of system by eliminating any chance of spoofing compared to single stimulus based systems. The study in [18] reports the usability of self-face as useful visual stimulus in biometric system. It is based on the fact that when a person watches own face, his EEG amplitude is higher compared to that obtained when he watches familiar or unfamiliar faces. This peculiarity can be utilized to recognize a person using his EEG [19]. Also, [20] reports that EEG features are distinct when a person hears his own voice, familiar voice and unfamiliar voice. Motivated by these facts, we present a biometric authentication system incorporating EEG patterns in response to self-voice, self-face, familiar voice and unfamiliar voice. The performance of the system is then evaluated using recognition accuracy, false acceptance rate (FAR) and false rejection rate (FRR) in an online paradigm. FAR is the percentage of imposters that are falsely accepted by the system as clients whereas FRR is the percentage of clients that are falsely rejected as imposters.

The rest of the paper is organized as follows. Section II presents the complete framework of the authentication model. Section III focuses on the experimental set up. Section IV discusses the results of the proposed system. And Section V concludes the work.

II. Proposed Framework

The biometric authentication framework consists of two phases, namely enrollment and authentication as shown in Fig.1. Each phase starts with raw EEG data acquisition via Emotiv Epoc headset. The headset has 14 EEG channels namely AF3, AF4, F3, F4, F7, F8, Fc5, Fc6, T7, T8, P7, P8, O1 and O2 according to 10-20 international system of electrode placement. After recording the data, the raw EEG signals pass through feature extraction stage. In the enrollment phase, the extracted representative feature vector for each subject is named as the template vector. This template vector is stored in the database as a representative vector for the each subject. Then, the feature vector extracted during the authentication phase is correlated with the template vector for each subject and correlation value is compared with a predefined threshold to accept/reject the claimed subject. Threshold is the minimum correlation required to accept a subject as a true client.

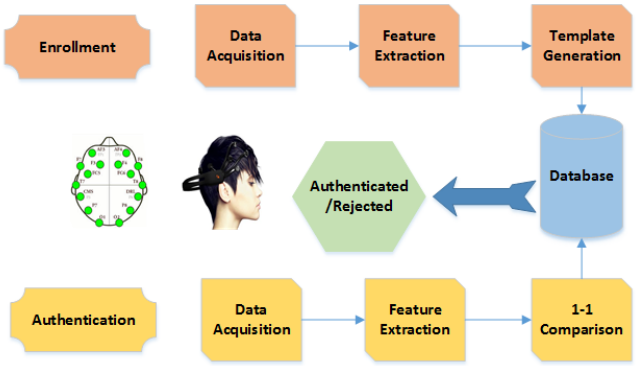

Fig. 1 Basic Schematic of biometric authentication.

A. Signal Processing stages

Multi-channel raw EEG signals acquired through the EEG headset undergo a number of signal processing stages as given in Fig. 2. Various stages are as follows.

1) Baseline filtering: Baseline filtering is to remove the DC-drifts in the signal. It is done by subtracting the mean of a few sec pre-stimulus EEG signal from stimulus-related EEG for each EEG channel. The stimulus related brain responses are recorded in the designed experiment after 10 sec. The average of 3 seconds is taken as baseline for each EEG channel. This baseline is subtracted from original data to get the baseline corrected EEG. It is iteratively done for all 14 channels.
2) Bandpass filtering: The multi-channel EEG signal is then decomposed into 4 EEG sub bands namely theta (4-8 Hz), alpha (8-12 Hz), beta (12-30 Hz), gamma (30-40 Hz) using 4 Butterworth band pass filters in the respective frequency ranges. Then it undergoes time division power spectrum analysis to extract features.
3) Power Spectrum Analysis: From the onset of stimulus presentation, the received EEG samples are divided into 5 equal segments and the power value p is calculated for each segment as shown in eqn. (1).

$$p_C^B = \frac{1}{N}\sum_{k=1}^{N} x_C^B(k)^2 \qquad (1)$$

where, $x_C^B(k)$ is the amplitude of k^{th} sample of C^{th} channel EEG signal of B^{th} band and N equals the number of samples. This computation is repeated for all bands and

channels. The average value of *p* across 5 segments is computed for each channel and for each band. These 4 band power values from 14 EEG channels form the subject-specific representative feature vector *P* which is of size 4 x 14.

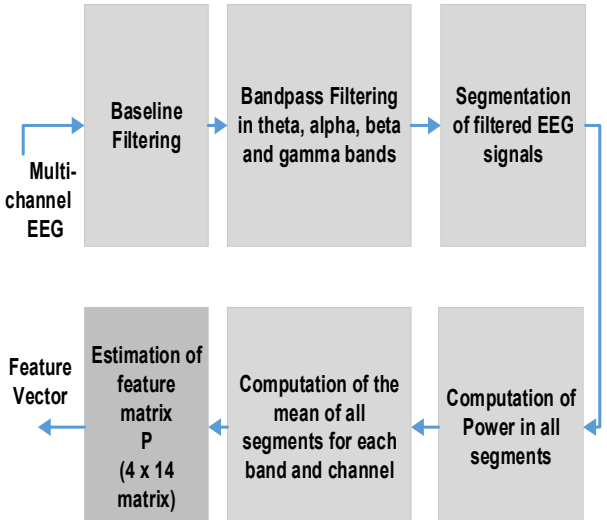

Fig. 2 Proposed feature extraction stage.

This feature set has to be extracted for all the audio and visual stimuli presented to the subject. Offline analysis shows that self-face, self-voice, unfamiliar voice and familiar voice are consistently giving reasonable correlation and matching with the threshold values, and therefore they are used as online stimuli.

B. Authentication

In online authentication when a subject claims a certain identity, the proposed system computes the feature vector for various bands and channels in response to the stimuli provided in the similar manner as described in Section II. A. Alpha and beta bands are considered in matching process for visual stimuli whereas only gamma is considered in audio stimuli. If the correlation of the template vector with the online feature extracted from the EEG for a specific band is greater than the threshold, a match count which is assigned as zero in the beginning is incremented. There are 10 stimuli in online experiment consisting of 2 familiar voice, 2 unfamiliar voice, 3 self-voice and 3 self-face stimuli. If the match count satisfies a set of conditions as explained in Fig. 3, then the subject is said to be genuine and will be accepted. Or else he is considered as an imposter. The authentication procedure is be briefly explained here.

Out of the 10 input stimuli, a correlation index is computed for each stimuli, to predict the genuineness of claimed subject. For audio stimuli, only gamma band is considered for correlation index whereas average of correlation values of alpha and beta bands are used in visual stimulus. Accordingly a series of comparison of the estimated correlation indices with stimulus-specific threshold values are performed at Check 1 to 5 as depicted in Fig. 3.

- In Check 1, if match count of self-voice stimuli (MCSV) ≥2 out of the 3 stimuli given && match count in self-face stimuli (MCSF) ≥2 out of the 3 stimuli given && match count in unfamiliar and familiar voice stimuli (MCUF) ≥2 out of the 4 stimuli given, the subject is accepted. If No, go to Check-2 stage.
- In Check-2, find whether MCSF is ≥2. If No, got to Check-4. If Yes, Check-3 is performed to evaluate if the average correlation value of self-face trials is > 0.6. If Yes, the subject is accepted. If Check-3 is not satisfied, Check-5 is performed.
- In Check-4, the following matching is done. If MCSF<2 && MCSV >1, then claimant is accepted. Otherwise, he is rejected.
- In Check-5, if MCSF≥2 && MCSV≥1, then claimant is accepted. Otherwise, he is rejected.

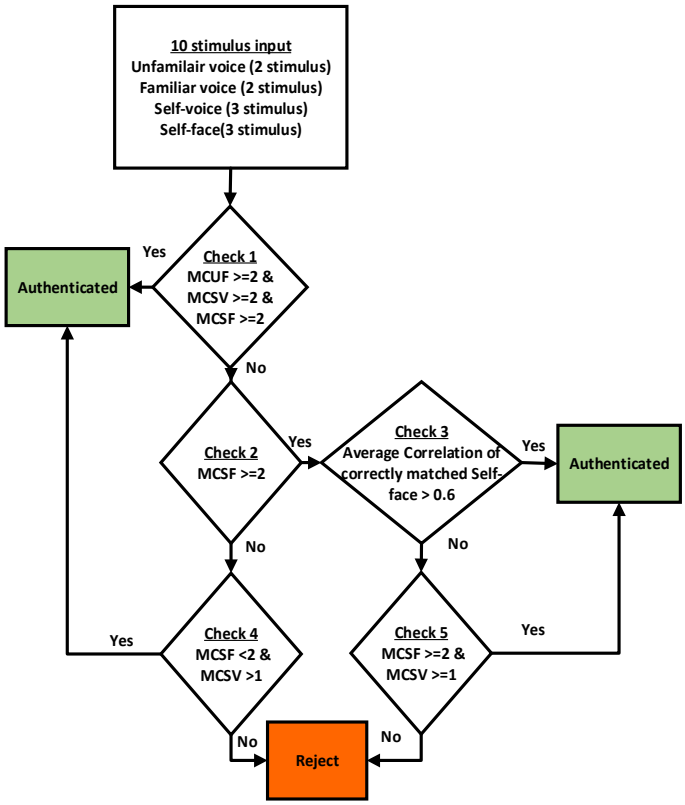

Fig. 3 The detailed data flow diagram for authentication. MCUF represents match count in unfamiliar and familiar voice stimuli. MCSV indicates match count in self-voice stimuli. MCSF is the match count in self-face stimuli.

The defined comparison stages in authentication using mentioned correlation thresholds and match counts (MCSV, MCSF and MCUF) values are chosen based on extensive offline data analysis of 5 subjects. The shown criterion and values are the same for all subjects.

III. EXPERIMENTAL SET-UP

As mentioned earlier, EEG signals are recorded by Emotiv Epoc neuroheadset. Five subjects (3 males and 2 females with an average age of 27±6.50 years) have participated in the

offline and online experiments. All of the subjects are right-handed. No subjects had any history of neurological or psychiatric disorders, substance abuse, or other serious medical conditions. In order to do online authentication experiment employing visual and audio stimulus, the correlation thresholds of various stimuli for each subject are pre-estimated by carrying out offline experiment and data analysis.

A. Calibration experiment

During the course of offline experiment for calibrating threshold values, both visual and audio stimuli (self, familiar and unfamiliar) have been presented to the subject in 2 separate sessions, and EEG signals are stored for analysis. The visual session consists of 10 self-face images, 10 face images of familiar (some relative or friend) and 10 unfamiliar face images in random order. Each single trial lasts for 10 sec, with preparation period of 2 sec, stimulus presentation for 6 sec and rest period of around 2 sec. During audio session, subjects are made to hear self-voice, familiar voice, unfamiliar voice (with same phrase spoken). The phrase for this is chosen as "A B C D E". There are 8 trials for each stimulus (self-voice, familiar voice and unfamiliar voice) for every subject.

For both visual and audio stimuli, all 4 bands (theta, alpha, beta, and gamma) are chosen for comparison and evaluation to check consistency in terms of correlation between trials. The average of cross-correlation values between trials in each stimulus type for all the 5 subjects are separately computed and their average value is taken as threshold for that specific stimulus type for each band. From offline analysis, threshold value of correlation between self-voice/face, familiar voice/face and unfamiliar voice/face have been computed for all subjects in each band. From the offline analysis, the threshold values are assigned as 0.52 in unfamiliar voice correlation, 0.54 for familiar voice, 0.60 for self-voice and 0.55 for self-face for all subjects. As it is found that, consistency of better correlation values are more in self-face, self-voice, familiar voice and unfamiliar voice across all subjects, we have chosen these stimuli in the design of online paradigm.

B. Online Experiment

Initial Preparation (10 sec)	**Trial preparation time (2 sec)**	**Stimuli (face/ voice) (6 sec)**	**Rest (2 sec)**	**….**

Fig. 4 Timing protocol for online experiment.

The online experiment consists of presentation of 7 auditory stimuli and 3 visual stimuli. The experiment starts with an initial preparation period of 10 seconds to avoid any sort of delay in data transmission from Emotiv Epoc due to weak connections. The timing protocol for a single trial is elaborately depicted in Fig. 4. The stimulus persists for a period of 6 sec preceded by a preparation phase of 2 sec and followed by rest time of 2 sec. After presenting 10 stimuli, the system predicts whether the claimant is client or imposter based on the procedure explained in Section II.B.

IV. RESULTS AND DISCUSSIONS

The observations and results obtained during the offline and online experiments have been presented here. Fig. 5 shows the response of subject-2 for self-face, familiar and unfamiliar images for channels P7 and O2 in offline analysis. The time segment giving best discrimination between 3 types of stimuli are shown in the graph. It is noted that during the response to self-face stimuli the amplitude of EEG signal is higher compared to familiar/unfamiliar stimuli for all subjects. Channels P7 and O2 are selected in the graph to show the response in parietal and occipital regions of brain towards stimuli. This observation was mostly consistent among all subjects.

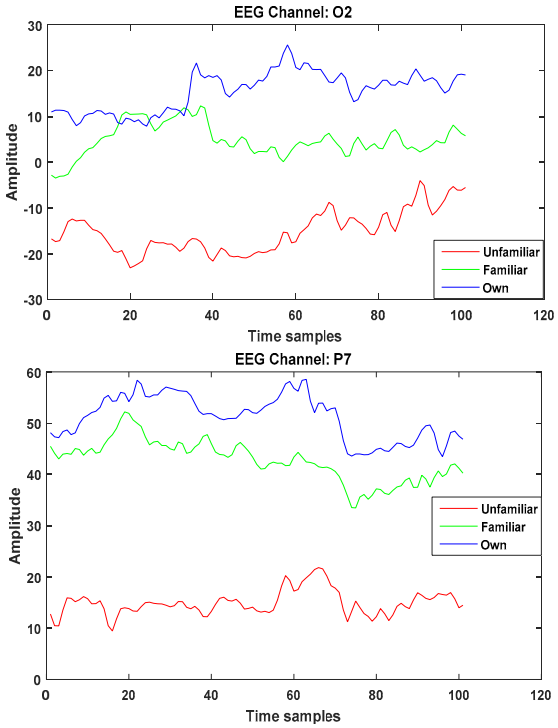

Fig. 5 EEG response towards face stimuli for Subject-2.

Fig. 6 shows EEG signal corresponding to the audio stimuli (self, familiar and unfamiliar) for subject-4 in channel F3 and O1 in offline analysis. Signal amplitudes in response to self-voice is found to be lower than familiar and higher than unfamiliar voices. Channels and segments showing good discrimination between various stimuli are plotted in the graph.

As the correlation values are the main decision making factor in authentication process, we show the correlation values of theta, alpha, beta and gamma bands of EEG for different subjects, for self-face and self-voice trials in Fig. 7 and 8 respectively. It is found that in both stimuli type, theta band is not much informative. The alpha and beta band correlation values are better in visual stimuli whereas gamma

band correlation is the best in audio stimulus experiment. Based on the observation, we have used only gamma band while processing audio stimuli whereas average of alpha and beta band correlation is taken for visual stimuli in online authentication.

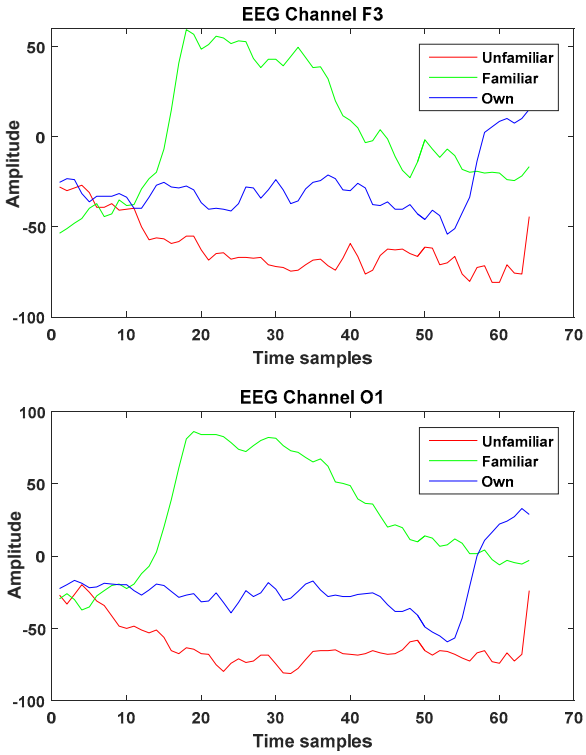

Fig. 6 EEG response towards different voice stimuli for Subject-4 in channels F3 and O1.

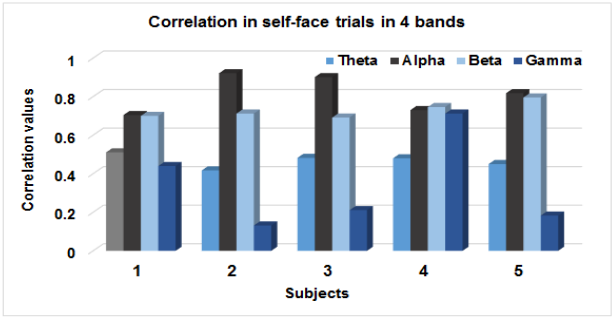

Fig. 7 Correlation in self-face trials for 5 subjects.

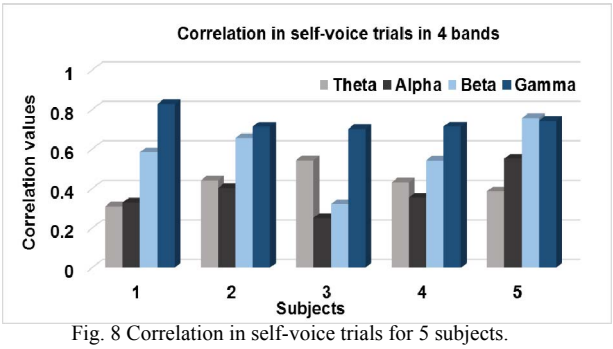

Fig. 8 Correlation in self-voice trials for 5 subjects.

During the online analysis, when a subject inputs his EEG signal to the authentication system, feature vectors composed of PSD values are computed and compared with the template vectors in respective bands for the specific stimulus type for all the 10 stimuli. Based on the authentication procedure explained in Section II.B, subjects are accepted as genuine clients or rejected as imposters. Fig. 9 and 10 shows the average correlation values obtained in the correctly matched self-face trials and self-voice trials respectively obtained for 5 subjects in the online authentication.

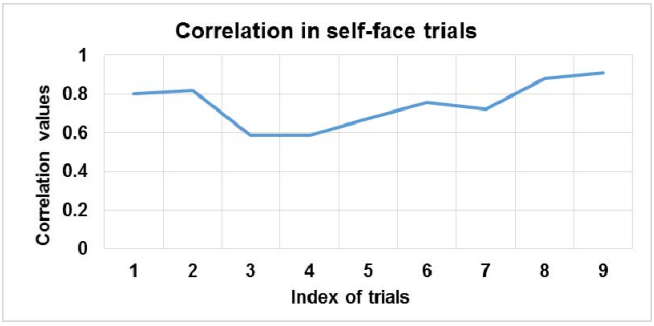

Fig. 9 Average correlation of alpha and beta for self-face stimulus in client matching cases.

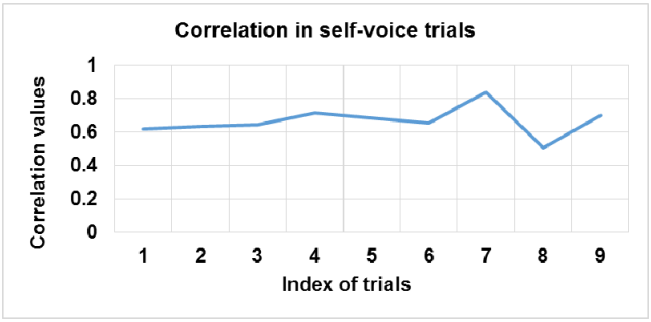

Fig. 10 Correlation of gamma for self-voice stimulus in client matching cases.

Table I Online authentication results

Subjects	FAR	FRR	Recognition Accuracy
Subject 1	12.5 %	25 %	81.25 %
Subject 2	15.38 %	16.67 %	83.97 %
Subject 3	0 %	33.3 %	83.35 %
Subject 4	25 %	25 5%	75 %
Subject 5	16.67 %	33.3 %	75.1 %
Mean	**13.91 %**	**26.66 %**	**79.73 %**

The online authentication results are tabulated in Table 1. In online authentication experiments, we have performed an average of 3 client trials and 3 imposter trials for every subject. The average FAR is 13.91% whereas FRR is 26.66%. The accuracy is computed in line with the study of [19] which uses self-face and non-self-faces for biometric authentication. The work in [19] reports an average accuracy of 86% among 10 subjects in offline analysis whereas our online system offers 79.73%. The obtained results are promising, but further investigation is necessary to fine tune the system parameters and improve the recognition performance. The proposed

system has to be tested in a bigger population over longer period of time in near future to precisely validate the results.

V. CONCLUSION

In this paper, an online EEG based biometric authentication system using both visual and audio stimuli is presented. In the proposed system, subject's EEG patterns in response to a set of visual and audio stimuli consisting of self, familiar or unfamiliar faces/voices are evaluated, using PSD features of alpha, beta and gamma bands. For audio stimuli, gamma band PSD is utilized whereas average of alpha and beta band PSD values are in visual mode to generate template vector for each subject. During online authentication, the stored templates are then matched with the respective test feature vectors collected. Five subjects have participated in the online authentication study. Based on the experimental analysis, it is found that the proposed system can offer an accuracy of 79.73% with a FAR of 13.91% and FRR of 26.66% among 5 subjects. The obtained results are promising, but future investigation is necessary to validate the stability and performance accuracy of the proposed methodology in bigger populations.

REFERENCES

[1] Fraschini Matteo, Arjan Hillebrand, Matteo Demuru, Luca Didaci and Gian Luca Marcialis, "An EEG-Based Biometric System Using Eigenvector Centrality in Resting State Brain Networks," *IEEE Signal Processing Letters*, vol. 22, no. 6 , pp. 666-670, 2015.

[2] Dai, Yixiang, Xue Wang, Xuanping Li, and Yuqi Tan. "Sparse EEG compressive sensing for web-enabled person identification." *Measurement*, vol. 74 , pp.11-20, October 2015.

[3] Wayman, J., Jain, A., Maltoni, D., Maio, D. (eds.): Biometric Systems: Technology, Design and Performance Evaluation. *Springer-Verlag* (2004).

[4] Duta, N., Jain, A.K., Mardia, K.V. "Matching of palmprints", *Pattern Recognition Letters*, vol. 23, no. 4 pp. 477-485, 2002.

[5] Jain, A.K., Ross, A., Pankanti, S. "A prototype hand geometry-based verification system", *Proceedings of 2nd International Conference on Audio and Video-Based Biometric Person Identification*, vol. 1 , pp. 166-171, 1999.

[6] Daugman, J.: Recognizing persons by their iris patterns. In Jain, A.K., Bolle, R., Pankanti, S. (eds.): Biometrics: Personal Identification in Networked Society. *Kluwer Academic*, 1999.

[7] Samal, A. and Iyengar, P. "Automatic recognition and analysis of human faces and facial expressions: a survey", *Pattern Recognition*, vol. 25, no. pp.65-77, 1992.

[8] Hurley, D. Nixon, M. and Carter, J. "Force field feature extraction for ear biometrics", *Computer Vision and Image Understanding*, vol. 98, no. 3 pp.491-512, 2005.

[9] Biel L., Pettersson O., Philipson L. and Wide P., "ECG analysis: a new approach in human identification," *IEEE Transactions on Instrumentation and Measurement*, vol. 50, No. 3, pp. 808-812, 2001.

[10] Korotkaya Z.: Biometric Person Authentication: Odor, 2003. http://www.it.lut.fi/ kurssit/03-04/010970000/seminars/Korotkaya.pdf.

[11] Matsumoto T., Matsumoto H., Yamada K. and Hoshino, S., "Impact of artificial gummy fingers on fingerprint systems," *In prInternational Society for Optics and Photonics*, Electronic Imaging, pp. 275–289, 2002.

[12] Galbally J. and Satta R., "Three-dimensional and two-and-a-halfdimensional face recognition spoofing using three-dimensional printed models," *IET Biometrics*, 2015.

[13] 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.

[14] Kavitha P. Thomas, Cuntai Guan, C. T. Lau, Vinod. A. P and K. K. Ang, "Adaptive Tracking of Discriminative Frequency Components in EEG for a Robust Brain-Computer Interface," *Journal of Neural Eng.,* vol. 8, no: 3, pp. 1-15, 2011.

[15] http://www.emotiv.com

[16] E. Niedermeyer, F.H. Lopes da Silva (Eds.), "Electroencephalography: Basic Principles, Clinical Applications, and Related Fields," Williams & Wilkins, Baltimore, 1993.

[17] DelPozo-Banos M., Travieso C. M., Weidemann C. T. and Alonso J. B., "EEG biometric identification: a thorough exploration of the time-frequency domain," *Journal of neural engineering*, Sep 23;12(5):056019, 2015.

[18] Yeom Seul Ki, Heung Suk and Seong Whan Lee, "EEG-based person authentication using face stimuli," *International Winter Workshop on Brain-Computer Interface BCI 2013*, February 2013.

[19] Yeom Seul-Ki, Heung Suk and Seong-Whan Lee, "Person authentication from neural activity of face-specific visual self-representation," *Pattern Recognition*, vol. 46, no. 4 pp. 1159-1169, 2013.

[20] Mahesh K., Smitha K.G. and A. P. Vinod, "Voice familiarity detection using EEG-based Brain-Computer Interface," *IEEE International Conference on Systems, Man and Cybernetics (SMC 2016)*, Budapest, Hungary, October 2016.