Single Trial Authentication with Mental Password Writing

Sarah N. Abdulkader(✉), Ayman Atia, and Mostafa-Sami M. Mostafa

HCI-LAB, Department of Computer Science,
Faculty of Computers and Information-Helwan University, Cairo, Egypt
nabil.sarah@gmail.com, ayman@hci.fci.helwan.edu.eg,
mostafa.sami@fci.helwan.edu.eg

Abstract. This paper presents an authentication system that uses brain waves as a biometric discriminant trait. It utilizes Electroencephalogram (EEG) signals generated from mental writing of the user-owned password. Independent Component Analysis (ICA) and baseline correction has been used for preprocessing and noise removal. The effect of two types of features, multivariate autoregressive (MVAR) model parameters and power spectral density (PSD) features, have been studied for this activity. Performance results based on single trial analysis have revealed that imagined password writing can reach average Half Total Error Rate (HTER) of 5 % for PSD features vs 3 % obtained with MVAR coefficients. The experiments have shown that mental password writing can be used for increasing the user acceptance for enrollment conditions while maintaining high performance results.

Keywords: EEG · BCI verification · Biometric authentication · Mental writing

1 Introduction

Technological revolution that characterizes this era has brought a lot of facilities and comfort to different aspects of human lives. It allows fast information exchange in the form of rapid mail delivery systems, distant communication and overseas transactions. These advantages come at the expense of increasing vulnerability of data secrecy. They cause the growing need for advanced authentication mechanisms. Approving or declining the claimed identity of the user is the responsibility of these mechanisms. There are three fundamental techniques used in authentication mechanisms, which are knowledge based, object based, and biometrics based authentication as stated in [1].

Knowledge based authentication requires the owning of some information exclusive to the user. It includes passwords and personal identification numbers. Different kinds of attacks can take this technique down like shoulder surfing and user carelessness. Some of the weakness associated with passwords can be overcome with object based authentication. In this technique, user possesses physical objects which are given for later identity confirmation as cards or tokens. They cannot be shared with the same freedom as exchanging the passwords. However, this category can still be broken with card-theft.

Biometrics based authentication, which is concerned with the measurement of physical characteristics or personal traits, fights the stealing vulnerability associated with the

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 3–12, 2015.
DOI: 10.1007/978-3-319-20376-8_1

previously mentioned types. Biometric characteristics can be divided into two broad categories: physiological and behavioral.

Physiological biometrics depend on the physical features of the human body while behavioral biometrics or behaviometrics depend on the action-based features like gait recognition, hand gestures, keystroke dynamics and voice recognition.

A relatively recent discriminative trait, called Electrophysiology, has been used in behaviometrics authentication. It reflects electrical properties and voltage changes of biological system in response to ongoing activities. There are several electrophysiological readings that show great opportunities as biometrics. They have specific names, referring to the origin of the bioelectrical signals, such as Electrocardiography (ECG) for signals originated from the heart, Electrocorticography (ECoG) for signals originated from the cerebral cortex, and Electroencephalography (EEG) for signals originated from the brain as mentioned in [2].

This paper presents a new mental authentication activity and investigates how well it meets various biometrics evaluation factors. The next section highlights different activities for personal identifications and authentications applied in previous researches along with the used assessment criteria.

2 Related Work

EEG is used to study the differences in brain voltage. They reflect the occurrence of motor or mental activities in various Brain Computer Interface (BCI) applications. The brain responses to certain actions have been used to verify the claimed identity even for people with various disabilities or to convey secret messages through the identification process as implied by Su et al. in [3]. They have designed an identification system with the ability to detect a covert warning expressed as a clenching-teeth muscle activity. The system, that uses power spectral density as features and LDA and KNN classifiers, has obtained an identification accuracy of 90 % versus 93.7 % obtained in a non-warning identification system.

2.1 Personal Identification and Authentication

Several researchers have investigated the use of brain signals in personal identification and verification systems for different motivating actions. Visual evoked potential and graphical stimulation have been widely used in a variety of forms like employing face stimulation via presenting either self-face or non-self-face images, as anticipated by Yeom and his colleagues in [4, 5]. They first have chosen the highly distinctive channels and time components related to each user. Then they utilize the averaged ERP signals over multiple trials in order to compute the corresponding features. They have reached a mean accuracy of 86.1 %. While Ravi [6] and Zúquete [7] have presented black and white pictures from Snodgrass and Vanderwart picture set to 70 individuals. Ravi has achieved an identification accuracy of 95.25 % using 40 Hz EEG oscillations. While Zúquete et al. have been concerned with reducing the consumption of electrodes. The performance of two classifiers, K-NN and SVDD, has been compared and their best attained results for eight electrodes are 95.1 % and 98.5 % respectively.

Ashby et al. in [8] have utilized mental based actions like baseline measurement, limb movement, counting, and rotation to authenticate five subjects. It operates low cost EEG headset from the Emotiv Company to collect 14 channel signals, thus increasing the price-based collectability of the system. They have reached an average accuracy 98.78 % using one-versus-all SVM classifier while discriminating five types of features. On the other hand, Hema and his colleagues [9] pay special attention to the uniqueness of reading and multiplication mental responses. They have extracted PSD features from EEG Beta waves and applied them to feed forward neural classifier. The performance of identifying six subjects has reached an average accuracy of 97.5 %. PSD features of mental spelling and reading activities from different subjects have been classified using feed forward neural networks in [10]. The identification system has gained performance accuracy of 78.6 % based on single trial analysis compared to 90.4 % of multiple trials averaging.

Marcel et al. in [11] has involved the mental generation of words in person authentication. The first letter, chosen randomly, is the same across all subjects. They have proposed a statistical framework based on Gaussian Mixture Models and Maximum a Posteriori model adaptation on word generation as well as motor imagery EEG signal. It has resulted in HTER ranging from 6.6 % to 20.5 % for motor imagery versus 12.1 % to 26.1 % for word generation for various number of gaussians in the mixture in a single day.

In an attempt to combine knowledge based and biometrics authentication, Svogor and Kisasondi [12] have discussed the idea of merging the user's mental state with his own password. The password is divided into smaller elements called pels. The user determines the mental state associated with each element.

2.2 Biometrics Evaluation Factors

The biometrics based authentication systems are evaluated against validation factors like those revealed in [13]. They can be categorized, as shown in Fig. 1, into general, system-related, and user-related factors. General factors include the essential characteristics of the authenticating trait like universality, uniqueness, and permanence. Universality verifies the existence of such trait in every human being, while uniqueness ensures its distinctiveness per individual. Permanence or constancy validates the time-invariance of the measured biological phenomena. The system-related factors guarantee the collectability and quantitative aspects along with the estimated system performance. Finally, user-related factors are concerned with the usability and user acceptance level.

In [7], Zúquete et al. criticize the application of visual stimulation in BCI authentication against general and system related factors. They argue that the universality requirement is not completely met for blind or people with severe visual damages but no evidence for uniqueness violation. According to their findings, constancy has been under certain doubts caused by the variability of the circumstances surrounding cognition activities. EEG recording should also be carefully managed to fulfill the collectability condition and enhance signal-to-noise ratio, especially with the low-power attribute of the EEG signals. Electrodes must be placed always in the same scalp location, but this issue is usually solved by using EEG helmets.

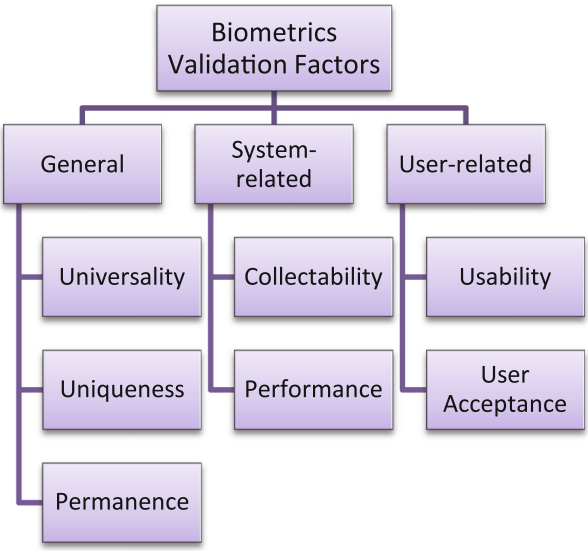

Fig. 1. Biometrics validation factors

According to Chuang et al. [14], the usability issues are related to two main reasons, one regarding EEG hardware, while the other is concerned with the mental tasks. For the recording hardware, less intrusive dry-contact electrode integrated in a wireless headset is preferred over free array of electrodes that must be carefully placed over the scalp. They have assessed mental task usability via a questionnaire filled by the participants in the authentication experiments. The evaluated tasks are closed-eyes breathing, imagined finger movement, sport motion, singing, tone-listening with eye reaction, counting specific color objects, and pass-thought.

The questionnaire has been interested in three factors, difficulty, bore, and the repeating intention. It has been claimed that among the performed tasks, movement imagination and pass-thought represent the most difficult tasks. The subjects have issues with imagining muscle actions without physical respond. Besides, bringing up specific feelings or events accompanying chosen pass-thought has proved hard to repeat on a consistent basis. Subjects have revealed that they consider finger movement as the most boring task. Breathing and counting colors are the highly recommended tasks for repetition. Although the promising usability results offered by breathing task, it is not suitable for sending secret messages opposite to pass, sport, song, and color related tasks. On the other hand, counting colors task faces a problem of recalling the secret attribute compared to the other four mental activities, as the subjects have no difficulty in recalling their personalized sport, song, and pass-thought choices.

In the following section, an authentication system with imagined password writing on a single trial basis is presented. It combines the memory recalling of the conventional password along with the specified mental writing action. This type of mental activities could help sending covert messages. The system enhances usability factors through exploitation of an easy to wear EEG recording headset. It also requires no previous

training for dealing with the system. Besides, the system demands only 3 to 4 min for samples' gathering process. The used dataset has been collected from six subjects in normal environmental conditions.

3 System Description

The recorded EEG signals of the participants, as shown in Fig. 2, pass through different phases of manipulation to perform the verification process. They are preprocessing, feature extraction and classification. The following subsections provide details for the involved algorithms in each phase.

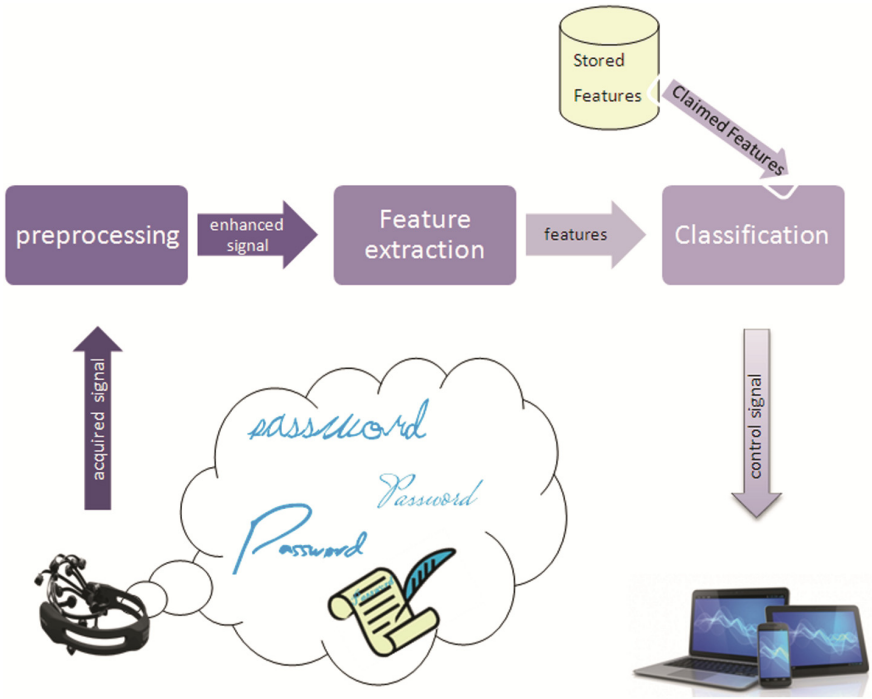

Fig. 2. Proposed BCI based authentication system

3.1 Preprocessing

The acquired signals from each subject have been modified by ICA. It is a statistical method for blind source separation [15, 16]. It performs spatial filtering for the supplied multidimensional signals to reduce artifacts, enhance SNR and facilitate EEG source localization [17]. In this system, the dimensionality of the output signals is the same as the input. Also, baseline correction has been utilized for this phase as described in [18].

3.2 Feature Extraction

Two types of mental password features have been studied, time analyzing features and spectral analyzing features. Multivariate autoregressive (MVAR) coefficients represent the temporal features. They contribute in modeling EEG multi-channel time series where the prediction for each value of one-channel signal relies not only on the previous values of the same time series but also on the previous values of the signals generated from other channels as well [19]. MVAR of order six has been used and estimated using Vieira-Morf method [20]. Spectral features are also involved in the current experiment. Power Spectral Density (PSD) has been computed using burg method with an autoregressive model of order six [21].

3.3 Classification

Support Vector Machine (SVM) has been used to take the final decision in the subject verification process. It exploits a discriminant hyperplane to identify classes. The selected hyperplane is the one that maximizes the distance between the nearest training points of different classes. This optimal hyperplane is described by the vectors, which lie on the margin that are called support vectors as discussed in [22]. The current subject is then authenticated if the supplied features belong to the same class as the features of claimed identity.

4 Experiments and Results

4.1 Dataset

In order to study the performance of the predescriped system, we have conducted an experiment involving six subjects. EEG signal has been recorded using an EMOTIV device [23] with fourteen channels. The channels, distributed according to international 10–20 system, are AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, AF4. During the training phase, the subjects are stimulated using an auditory cue. It instructs the user to recall his/her own password combining both knowledge and biometric based authentication. The password, composed of four digits, has been unified across the subjects to trace the effect of password stealing. The experiment consists of five runs each contains a session with 20 trials.

4.2 Performance Evaluation

The performance evaluation and enhancement is targeting the reduction of both error types: False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is measuring the percentage of the incorrectly authenticated subjects, while FRR is expressing the percentage of refusing the correct identities. In order to consider both errors, Half Total Error Rate (HTER) has been used. It is the average of both FAR and FRR [24].

4.3 Results

The results are obtained using a 10-fold cross-validation repeated over five runs with one-versus-all scheme for each subject. They illustrate that using MVAR model for feature extraction has achieved an error rate 44 %. It's lower than the outcome obtained using PSD features which is 45.08 % with only ICA spatial filtering employed in the preprocessing phase. When correcting baseline of the EEG signal, MVAR modeling parameters and PSD features have achieved reduced error rates of 3 % and 5 % respectively. The detailed results of each feature extraction method are viewed in Tables 1 and 2. The average results for each subject are shown in Fig. 3. ANOVA test has been conducted to trace the effect of baseline power correction on the authentication process. P-value was less than 0.05 for both MVAR model and PSD features. This p-value concludes that there is a noticeable influence of baseline power correction on classification results for both feature types.

Table 1. Authentication performance For MVAR coefficients after baseline correction

	R_1	R_2	R_3	R_4	R_5	Mean
S_1	0.1	0	0.025	0.025	0.025	0.035
S_2	0	0	0	0.075	0.025	0.02
S_3	0.05	0.1	0.1	0.075	0.1	0.085
S_4	0	0	0.025	0	0.025	0.01
S_5	0.025	0	0	0.025	0	0.01
S_6	0.025	0.025	0.025	0	0.025	0.02
Mean	0.033	0.020	0.029	0.033	0.033	0.03

Table 2. Authentication performance for PSD after baseline correction

	R_1	R_2	R_3	R_4	R_5	Mean
S_1	0.15	0.025	0.05	0.025	0	0.05
S_2	0.025	0	0	0.05	0.025	0.02
S_3	0.025	0.075	0.075	0.025	0.075	0.055
S_4	0.075	0.075	0.1	0.1	0.05	0.08
S_5	0.05	0	0	0.05	0.025	0.025
S_6	0.025	0.05	0.05	0.125	0.125	0.075
Mean	0.058	0.037	0.045	0.062	0.05	0.050

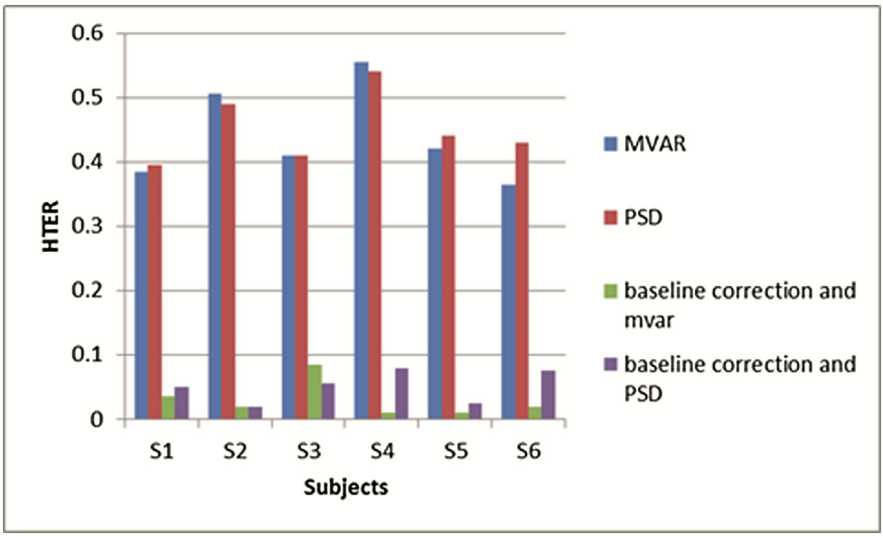

Fig. 3. System performance over five runs

The results have shown the efficiency of mental password writing activity in the authentication process for the same password. The proposed system gives better results than the mental word generation accomplished by Marcel et al. [11] for different words starting with the same letter. Their system has achieved HTER value that equals 6.6 % for motor imagery and 12.1 % for word generation. The effect of employing various passwords will be further examined in future work.

5 Conclusion

In this paper, an EEG based authentication system that utilizes mental password writing activity has been proposed. It aims at considering the user acceptance of enrollment conditions while attaining reasonable performance results. It uses ICA and baseline correction for preprocessing, PSD and MVAR coefficients for feature extraction, and SVM for classification. The final findings have shown that baseline correction has achieved a significant increase in the performance results. They have also revealed that time series modeling features and power spectral density features have offered comparable performance for this type of activity.

References

1. Shanmugapriya, D., Padmavathi, G.: A survey of biometric keystroke dynamics: approaches, security and challenges. arXiv preprint arXiv:0910.0817 (2009)

2. Riera, A., Dunne, S., Cester, I., Ruffini, G.: Electrophysiological biometrics: opportunities and risks. In: Mordini, E., Tzovaras, D. (eds.) Second Generation Biometrics: The Ethical, Legal and Social Context. The International Library of Ethics, Law and Technology, pp. 149–176. Springer, Netherlands (2012)
3. Su, F., Zhou, H., Feng, Z., Ma, J.: A biometric-based covert warning system using EEG. In: 2012 5th IAPR International Conference on Biometrics (ICB), pp. 342–347. IEEE (2012)
4. Yeom, S.-K., Suk, H.-I., Lee, S.-W.: Eeg-based person authentication using face stimuli. In: 2013 International Winter Workshop on Brain-Computer Interface (BCI), pp. 58–61. IEEE (2013)
5. Yeom, S.-K., Suk, H.-I., Lee, S.-W.: Person authentication from neural activity of face-specific visual self-representation. Pattern Recogn. **46**, 1159–1169 (2013)
6. Ravi, K., Palaniappan, R.: Leave-one-out authentication of persons using 40 Hz EEG oscillations. In: The International Conference on Computer as a Tool, 2005. EUROCON 2005, pp. 1386–1389. IEEE (2005)
7. Zúquete, A., Quintela, B., Cunha, J.P.S.: Biometric authentication using brain responses to visual stimuli. In: Proceedings of the International Conference on Bio-inspired Systems and Signal Processing, pp. 103–112 (2010)
8. Ashby, C., Bhatia, A., Tenore, F., Vogelstein, J.: Low-cost electroencephalogram (EEG) based authentication. In: 2011 5th International IEEE/EMBS Conference on Neural Engineering (NER), pp. 442–445. IEEE (2011)
9. Hema, C.R., Paulraj, M., Kaur, H.: Brain signatures: a modality for biometric authentication. In: International Conference on Electronic Design, 2008. ICED 2008, pp. 1–4. IEEE (2008)
10. Hema, C., Osman, A.A.: Single trial analysis on EEG signatures to identify individuals. In: 2010 6th International Colloquium on Signal Processing and Its Applications (CSPA), pp. 1–3. IEEE (2010)
11. Marcel, S., del Millán, J.R.: Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Trans. Pattern Anal. Mach. Intell. **29**, 743–752 (2007)
12. Svogor, I., Kisasondi, T.: Two factor authentication using EEG augmented passwords. In: Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces (ITI), pp. 373–378. IEEE (2012)
13. Wang, L., Geng, X., Global, I.: Behavioral Biometrics for Human Identification: Intelligent Applications. Medical Information Science Reference, New York (2010)
14. Chuang, J., Nguyen, H., Wang, C., Johnson, B.: I think, therefore i am: usability and security of authentication using brainwaves. In: Adams, A.A., Brenner, M., Smith, M. (eds.) FC 2013. LNCS, vol. 7862, pp. 1–16. Springer, Heidelberg (2013)
15. Hyvärinen, A., Karhunen, J., Oja, E.: Independent Component Analysis. Wiley, New York (2004)
16. Stone, J.V.: Independent Component Analysis. Wiley Online Library (2004)
17. Allison, B.Z., Dunne, S., Leeb, R.: Towards Practical Brain-Computer Interfaces: Bridging the Gap from Research to Real-World Applications. Springer, Heidelberg (2012)
18. Hu, L., Xiao, P., Zhang, Z., Mouraux, A., Iannetti, G.: Single-trial time–frequency analysis of electrocortical signals: baseline correction and beyond. NeuroImage. **84**, 876–887 (2014)
19. He, C., Lv, X., Wang, Z.J.: Hashing the mAR coefficients from EEG data for person authentication. In: IEEE International Conference on Acoustics, Speech and Signal Processing, 2009. ICASSP 2009, pp. 1445–1448. IEEE (2009)
20. Schlögl, A., Supp, G.: Analyzing event-related EEG data with multivariate autoregressive parameters. Prog. Brain Res. **159**, 135–147 (2006)
21. Marple, S.L.: Digital Spectral Analysis: with Applications. Prentice-Hall, Englewood Cliffs (1987)

22. Jian-feng, H.: Comparison of different classifiers for biometric system based on EEG signals. In: 2010 Second International Conference on Information Technology and Computer Science (ITCS), pp. 288–291. IEEE (2010)
23. [Last Visit: 2014.07.08]. http://www.emotiv.com
24. Monroe, D.: Biometrics Metrics Report v3.0. http://www.usma.edu/ietd/docs/BiometricsMetricsReport.pdf