P300-BCI-Based Authentication System

Moonwon Yu
School of Computing
Korea Advanced Institute of Science and Technology
Daejeon, South Korea
moonwon.yu@cs.kaist.ac.kr

Netiwit Kaongoen
School of Computing
Korea Advanced Institute of Science and Technology
Daejeon, South Korea
netiwit.k@cs.kaist.ac.kr

Sungho Jo
School of Computing
Korea Advanced Institute of Science and Technology
Daejeon, South Korea
shjo@cs.kaist.ac.kr

Abstract—**An authentication system is the system that decides whether to accept or reject the claiming identity of a person. Biometric-based authentication utilizes the individuality in human physiological and behavioral characteristics to authorize a person. Brain-signal-based authentication system is relatively new comparing to other types of biometric data. In this paper, we proposed a novel method that applies P300-based Brain Computer Interface (BCI) technique to the authentication system. The main concept for P300-BCI-based authentication is that the Oddball paradigm eliciting P300 waves is secret to the attacker. The experiments were conducted to evaluate the proposed system. The trained P300 classification model has 0.831 accuracy rate. And the proposed authentication system has 0.325 False Rejection Rate (FRR), 0.00 False Acceptation Rate (FAR) for secret-unknown attack and 0.10 FAR for secret-known attack. This study has shown that P300 wave has good potential as a biometric for highly secured authentication system.**

Keywords-P300; Brain Computer Interface; Authentication System; EEG; Biometric

I. Introduction

An authentication system is the system that decides whether to accept or reject the claiming identity of a person. Let X be an unknown person and ID be the identity that X claims to be, the authentication system must accept this claim if X is the true owner, client, of identity ID. Otherwise, if X is not the true owner of identity ID, we call X the imposer and thus, the system must reject this claim of identity [1].We use authentication system in our daily life and the most common one is the password-based authentication system where the registered username is represented as the identity and password is the proof of identity if matching with what registered in the system database. This password-based authentication system is simple and efficiency, however, lacks of strong security system. Username and password can be acquired directly by observation (i.e. Shoulder Surfing Attack) and there is no way to positively link the usage of the system to the actual user. In other words, when a username and password is used with two or more people, the system has no way to know who the actual user is [2].

Biometric-based authentication system utilizes the individuality in human physiological or behavioral characteristics in order to authorize a person. It provides a much more reliable user authentication than the password-based authentication system [2]. The biometrics that have been used for authentication system includes fingerprint, palm print, hand geometry, iris, face, ear force field, heart signals, odor, and brain signal [1].

Using brain signal, specifically, electroencephalogram (EEG), as biometric for authentication system is relatively new comparing to other types of biometric. EEG-based authentication system have several advantages. First, brain is the human organ that is less likely to be damaged comparing to other biometrics. Second, brain signal is almost impossible to mimic since it is unique to each individual person. Third, it's less likely to steal or force a person to authorize the system as the brain activity is sensitive to stress and mood of the person [3]. Previous studies [1][3][4], share similar scheme for the EEG-based authentication system. Apart from the difference in details for the method, they begin by having the users registered in the authentication system record their EEG signal while performing some specific mental tasks such as solving mathematic problems in their head, imagining repetitive self-paced limb movements or saying some specific words repetitively in their head. The EEG signal is then processed and features are extracted to construct the vector biometric data specific for each user. When performing the authentication with the pair <ID, X>, brain data of X is obtained and the system calculates matching score of X's data with both client and imposer data. If the matching score between pair <X, Client> is more than the pair <X, Imposer> for some specific threshold, the authentication system accepts the claiming identity ID of X.

Although the EEG-based authentication system presented in previous studies provides high accuracy and low authentication error rate, it takes time for the user to train and collect the data for the database. Mental activities require effort from the user and might be difficult for some peop le to perform. The threshold for the difference in matching score is also needed to be adjusted for each individual or specific mental task. To counter these disadvantages, we proposed P300-BCI-based authentication system that utilize P300-based brain computer interface (BCI) method. P300 signal is an event related potential (ERP) component that elicits due to the low-probability-target in oddball paradigm. It provides fast response to the stimuli and require small amount of training and effort from the user [5]. With the properties of P300 signal, we expect the system to be easy and effortless for user to use in real life.

II. Proposed Method

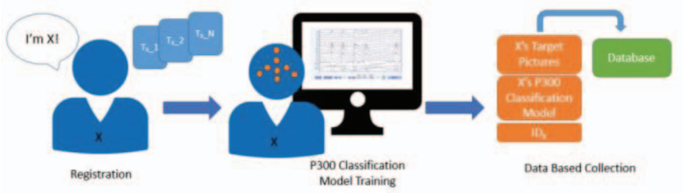
A. P300-based BCI

P300 is a positive ERP that occurs in the scalp-recorded EEG after a stimulus that is delivered under a specific set of circumstances. P300 latency may vary from 250 ms to 750 ms from onset of the stimulus and it is strongest in parietal area of human brain. The set of circumstances that elicit P300 ERP is known as Oddball paradigm in which a subject is presented with a series of 2-classes stimuli where the low-probability target stimuli are mixed with high-probability non-target stimuli. The low-probability target stimuli elicit a P300. The most common use of P300-based BCI is P300 speller, where the desired character works as the low-probability target stimuli thus P300 waves can be detected and the user is able to type words without using any kind of movement [5][6].

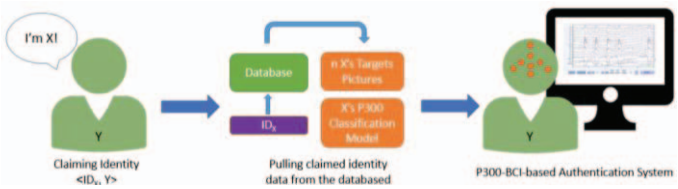
B. P300-BCI-Based Authentication System

The main idea for the proposed method, P300-BCI-based authentication system, is that the Oddball paradigm is secret only the client know. In other words, given the same sequence of stimuli to both client and imposers, only client will be able to distinguish the low-probability target stimuli from the high-probability non-target stimuli. In this paper, the stimuli are pictures of person and the low-probability targets are pictures of client's known people. Knowing this setting, client's P300 wave can be detected from watching a sequence of stimuli in Oddball paradigm and used as data to authorize the system. In contrast, the same sequence specifically made for the client would be perceived as just pictures of random person to the imposers and no P300 wave would elicit.

The scheme for the proposed system is shown in Figure 1 below. The system begins by having the user register to the system in which user has to provide the username (notated as ID_X for the user X) and N target pictures (Figure 1.a). The system then generates sequences containing pictures of random person randomly mixed with target pictures due to Oddball paradigm for users to perform P300 BCI. The user's EEG signal responded to each of stimuli is extracted, preprocessed and used to train the two-class (non-P300 response and P300 response) classification model using supervised machine learning technique. Finally, user's target pictures, trained P300 classification model along with the registered ID are saved to the system database.



(a)


I'm X!
Y
Database
ID_X
n X's Targets Pictures
X's P300 Classification Model
Y
Claiming Identity <ID_X, Y>
Pulling claimed identity data from the databased
P300-BCI-based Authentication System

(b)

Figure 1. The scheme for P300-BCI-based Authentication system: (a) Registration scheme, (b) Utilization scheme

Figure 1.b shows the scheme when a person uses authentication system. Given an identity-unknown person, Y, with the claiming identity, ID_X, the system will pull the client X's target pictures and P300 classification model from the database to construct the P300-BCI authentication system. If Y is indeed the client, P300 signals can be detected and the system will accept Y as X, the true owner of identity ID_X.

III. Experiment

A. Experimental Setup

The user is asked to sit comfortably in front of the PC monitor during the trails of P300-BCI-based authentication experiment. One trail of the experiment starts with a black screen with a white fixation point in the center that lasts for 5 s. One trial consists of 5 blocks containing randomly-generated stimuli sequence separating by the same black screen for 2 s. In each block, user observes a randomly-generated sequence of 10 picture stimuli in which 8 stimuli are pictures of random person and 2 stimuli are target pictures randomly drawn from client's database. Each picture is shown in the screen one at a time, last for 100 ms following by a black screen (without fixation point) that last for 100 ms, i.e. the interstimulus interval (ISI) is 200 ms. Every picture including the black screen is 300x400 in size.

There are four parts of the experiment: P300 classification model training part, authentication system testing part, unknown-attacking part, and known-attacking part. The training part is necessary to train the classification model to detect the P300 wave. The testing part is performed to test the accuracy and efficiency of the authentication system. The unknown-attacking part is done by having each subject randomly choose one of other subject's identity, and perform the authentication system. Last, the known-attacking part has same procedure as the unknown-attacking part, however, the attackers were able to learn and memorizes all of target pictures (the secret) and try to authorize himself as the true owner of the claiming identity. All parts of the experiment are performed for 10 trials per each subject.

B. Subjects

Four healthy male subjects (age 24 ±2 years) voluntarily participated in our experiment. All of the subjects were free of any neurological disorders and eye problems, and had never experienced any kind of brain-signal-based authentication system.

C. Data Acquisition

EEG data was recorded using OpenBCI 32bit board kit [7] in 8 channels including Fz, Cz, Pz, P3, P4, Oz, PO7 and PO8 according to the International 10-20 system (Figure 2). All 8 EEG channels are referenced to the right earlobe and grounded to the right mastoid. The sampling rate of EEG was 250 Hz. During the experiment, EEG epoch of length 800 ms starting from the stimulus onset time are cut to represent the brain activity response to each stimulus. Noted that in each EEG epoch, the last 600 ms data is overlapped with the data epoch of the next EEG epoch from subsequent stimuli.

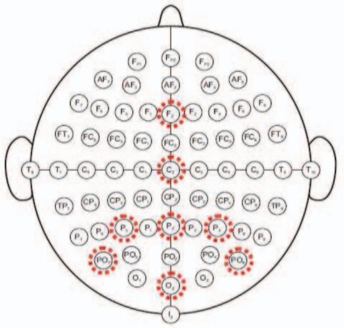


Figure 2. The EEG node positions used in the proposed system

D. Data Preprocessing

EEG epochs are underwent the following preprocessing methods before further data processing and analysis.

1) Filtering. EEG data are filtered using 6th ordered Butterworth bandpass filter. The cut-off frequency was set to 1.0-12.0 Hz.

2) Decimation. EEG data in each epoch is decimated with the factor of 15 to reduce the size of feature vector.

3) Winsorising. Winsorisation is performed to remove the effects of outliers in EEG data for better signal quality. In this system, the 10th and 90th percentile were computed for each EEG channel. Then the values lying below or higher than 10th and 90th are replaced by the 10th and 90th percentile value, respectively.

4) Standardization. EEG data from each channel is standardized to have zero mean and standard deviation equal to 1.

5) Feature vector construction. Finally, the feature vector for each EEG data epoch are constructed by concatenating samples from each of 8 channels into one data vector. The label vector is also constructed to label each EEG data epoch with [-1, 1] value to indicate whether the EEG epoch is the response for non-target stimuli or target stimuli (P300 wave response), respectively.

E. P300 Classification Method

The P300 classification models were trained using Fisher's Linear Discriminant Analysis (FLDA) [6][8]. The training data set was constructed from the data recording from the Training part of the experiment. The training data consists of the total 500 EEG epochs. The algorithm was fully automatic, i.e. no user intervention was required to adjust the parameters.

In this experiment, we performed the P300-BCI-based authentication system in two different methods. In the first method, classifier outputs from only one block of P300 BCI was used to determine whether to accept or reject the claim. If averaged classifier outputs between 8 non-target EEG epochs and 2 target EEG epochs indicate its correct class, the system will accept the claim. In the second method, the classifier outputs were averaged separately for all target and non-target EEG epochs in 5 blocks of one trial. If both averaged classifier output for both non-target and target EEG epochs indicates the correct class of the EEG epochs (i.e. P300 waves were elicited correctly), the authentication system accepts the claiming identity.

F. System Evaluation

The proposed P300-BCI-based authentication system was evaluated into two parts: performance of the P300 classification model and the performance of the authentication system. First, the P300 classification models trained from the data in Training part of the experiments were evaluated using 10-Fold Cross-Validation. Since cross-validation method gives different result values in each run, the algorithm was repeated for 10 times and we took the averaged result as the performance of trained P300 classification model.

The authentication system for both two methods were evaluated with two error rates: false rejection rate (FRR) and false acceptation rate (FAR). Both error rates are calculated using the following formula:

$$\text{FRR} = \text{\#Client incorrectly detected as Imposer/ \#trial} \tag{1}$$

$$\text{FAR} = \text{\#Imposer incorrectly detected as Client/ \#trial} \tag{2}$$

FRR was calculated using the data obtained from the testing part of the experiment. FAR was calculated for data obtained from both unknown-attacking and known-attacking part of the experiment. All system performances were averaged from all subjects to represent the final performance of the proposed system.

IV. Results and Discussion

Performance of the P300 classification model for each subject are summarized and shown in Table 1 below. From the results, the averaged accuracy of trained P300 classification model was 0.831 with the sensitivity and specificity equal to 0.570 and 0.897, respectively. The experiment part 2, 3 and 4 gave the performance of the authentication system. The performance for authentication system with method 1 and 2

TABLE I. EVALUATION RESULTS FOR P300 CLASSIFICATION MODEL

Evaluation Values	**Subjects**				**Average**
	S1	***S2***	***S3***	***S4***	
Accuracy	0.825	0.813	0.866	0.821	0.831
Sensitivity	0.554	0.507	0.700	0.519	0.570
Specificity	0.893	0.889	0.907	0.897	0.897

TABLE II. EVALUATION RESULTS FOR P300-BCI-BASED AUTHENTICATION SYSTEM WITH METHOD 1

Evaluation Values	**Subjects**				**Average**
	S1	***S2***	***S3***	***S4***	
FRR	0.66	0.78	0.68	0.64	0.69
FAR Unknown-Attack	0.04	0.04	0.08	0.04	0.05
FAR Known-Attack	0.04	0.10	0.08	0.14	0.09

TABLE III. EVALUATION RESULTS FOR P300-BCI-BASED AUTHENTICATION SYSTEM WITH METHOD 2

Evaluation Values	**Subjects**				**Average**
	S1	***S2***	***S3***	***S4***	
FRR	0.20	0.50	0.20	0.40	0.325
FAR Unknown-Attack	0.00	0.00	0.00	0.00	0.00
FAR Known-Attack	0.20	0.00	0.20	0.00	0.10

are shown in Table 2, and Table 3, respectively. From the results, method 2 of the proposed system yields much better performance in both FRR and FRR. The averaged FRR from both method are 0.690 and 0.325 which are relatively high comparing to the methods presented in previous studies [1][3][4]. Considering the low value of sensitivity of the P300-BCI classification model, the system might not be able to correctly detect the P300 waves and causes the system to falsely reject the client. The most important performance measurement of the authentication system is FAR. From the results, we can see that FAR was 0.00 when using the method 2 for the authentication system. This indicate the good security that is the main priority to be concerned for authentication system. The 4th part of the experiment where the attacker was given time to memorize all the target pictures of the client was conducted to prove that P300 wave is suitable choice for biometric-based authentication system. The FAR for secret-known attack experiment was 0.09 and 0.10 for method 1 and method 2. Table IV shows the comparison between the result of the proposed system and previous studies, [1], [3] and the conventional password-based system. This result shows that the proposed method have much higher security comparing to the conventional password-based authentication system in which the attacker would be able to access the client system right away. This is due to the individuality of human's brain activity (P300 waves, to be specific). In addition to the numerical results, there were no subjects reporting the difficulty of the system. The training time needed to perform for the construction of P300 classification model was 2 minutes 30 seconds and authorizing time (1 trial) was 15 seconds which was fast and convenient for the user. These results shows that the proposed method was satisfactory to be used in real life.

The future work includes improving the P300 classification model so that it yields better FRR for the system. This could be done by trying different kinds of machine learning or signal processing techniques. Because brain signal is sensitive and can vary according to the mood and body condition of the subject, the generalized version of P300 classification model for a user may be needed to use in real case scenario. This could be done by obtaining the P300 signal from a person in different conditions and since our proposed system requires such a short training time (comparing to previous brain signal-based authentication system), this can be done easily. The EEG acquisition tool is also needed to be considered. The clinical-grade EEG recording machine would give the better signal quality that yield the better system performances.

TABLE IV. COMPARING RESULTS TO PREVIOUS STUDIES

Evaluation Values	**Proposed System**	**R. P. [1]**	**S. M. [3]**	**Password -Based**
FRR	0.325	0.002	0.085	**0.00**
FAR Unknown-Attack	**0.00**	**0.00**	0.06	**0.00**
FAR Known-Attack	**0.10**	X	X	1.00

V. CONCLUSION

In this paper, we proposed a biometric-based authentication system that use P300 waves eliciting due to the target stimuli in Oddball paradigm as the data. The performance results were satisfactory. It shows that P300 wave has good potential as a biometric and P300-BCI-based authentication system is a promising authentication system that, with some minor improvement, could be used as an authentication system in the place that requires high security.

ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education (2013R1A1A2009378)

REFERENCES

[1] Palaniappan, Ramaswamy. "Two-stage biometric authentication method using thought activity brain waves." *International Journal of Neural Systems* 18.01 (2008): 59-66.

[2] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Enhancing security and privacy in biometrics-based authentication systems." IBM systems Journal 40.3 (2001): 614-634.

[3] Marcel, Sebastien, and José R. Del Millan. "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 29.4 (2007): 743-752.

[4] Rajagopal, Abhejit, Anthony C. Nguyen, and Dennis M. Briggs. "NeuroPass: A secure neural password based on EEG.

[5] Wolpaw, Jonathan R., and Elizabeth Winter. Wolpaw. *Brain-computer Interfaces: Principles and Practice*. Oxford: Oxford UP, 2012. Print.

[6] Krusienski, Dean J., et al. "A comparison of classification techniques for the P300 Speller." *Journal of neural engineering* 3.4 (2006): 299.

[7] http://www.OpenBCI.com

[8] Krusienski, Dean J., et al. "A comparison of classification techniques for the P300 Speller." *Journal of neural engineering* 3.4 (2006): 299.

[9] Selim, Abeer E., Manal Abdel Wahed, and Yasser M. Kadah. "Machine learning methodologies in P300 speller Brain-Computer Interface systems." *Radio Science Conference, 2009. NRSC 2009. National*. IEEE, 2009.