Development of a multi-modal personal authentication interface

Sung-Phil Kim*, Jae-Hwan Kang*, Young Chang Jo† and Ian Oakley*
*Ulsan National Institute of Science and Technology, Ulsan, Republic of Korea
E-mail: spkim@unist.ac.kr Tel: +82-52-2172727
† Korea Electronics Technology Institute, SeongNam, Republic of Korea
E-mail: ycjo@keti.re.kr Tel: +82-31-789-7544

***Abstract*— Recent advances have brought biometric user interfaces such as fingerprint and iris to the users' daily lives. More advanced biometric techniques are on the verge of development and commercialization, with increasing levels of security. This paper presents recent work on the development of a multi-factor personal authentication system. The proposed system is based on unique cognitive responses of a user to predetermined stimuli. Biometric signals such as brain activity are used to measure cognitive responses. The approach to implement such a system and test authentication results are presented. Discussion includes the feasibility of the system as well as potential scenarios of using multi-factor authentication interfaces.**

I. INTRODUCTION

Multi-factor authentication refers to a security mechanism with more than one type of authentication scheme to provide strong security protocols [1]. Factors generally include possession (e.g. key), knowledge (e.g. password) and inherence (e.g. fingerprint) [2]. A significant amount of researches have demonstrated the utility of multi-factor authentication frameworks, such as the combinations of fingerprints and tokenized random numbers [3], dynamic handwriting signatures and passwords [4], or fingerprints, smart cards and passwords [5].

Among the factors, the knowledge factor is the most implicit and difficulty to hardcopy unless one's active expression of knowing information is fraudulently obtained by illegal users (e.g. typing PINs on the keyboard). However, the knowledge factor renders itself vulnerable to hacking due to its limits to the use of short but most random symbols (e.g. a password requirement of 6-15 characters of alphabets, numbers and special characters) [6]. These limitations are also related to intrinsic properties of the knowledge factor that the user should be able to memorize passwords to eliminate explicit storage but also always retrieve it correctly whenever necessary. A multi-factor authentication protocol can address this problem by mixing the knowledge factor with the biometrics so as to eliminate the need to remember symbolized passwords and instead generate biometric patterns unique to the knowledge that only the user has [7].

Yet, the traditional biometric techniques such as fingerprints, iris or palm vein image [8] may not be able to support the knowledge factor enough as they only produce static signals. Therefore, a password-free multi-factor authentication framework needs to leverage a dynamic biometric that can be inherent but also patterned by implicit knowledge. Recently developed biometrics such as electrocardiography (ECG) or electroencephalography (EEG) may serve as such a dynamic biometric [9-10] for the password-free multi-factor authentication. In particular, EEG-based biometrics are suitable for this purpose since EEG can represent underlying cognitive processes including memory retrieval. But it is also noteworthy that a password-free authentication protocol may need to provide known stimuli to the user to naturally evoke EEG responses without letting the user volitionally recall specific information.

The present study develops a multi-factor authentication protocol by designing a stimulus presentation paradigm and analyzing EEG responses to a special set of stimuli. In particular, we create sets of facial stimuli among which a face image known to the user is mixed or not. The presentation of these face image sets is expected to induce distinguishable EEG responses [11]. We also test an attacking scenario where an imposter might learn the face known to the user and attempt to pass the authentication protocol by generating EEG responses to that known face. We analyze EEG signals to find if there is any difference between EEG responses to learned faces and known faces.

II. METHODS

A. Participants

Twenty-nine undergraduate university students with normal or corrected-to-normal vision participated in the study (mean 22.44 ± 2.71 years old). Participants reported no history of neurological disorders and provided informed written consent prior to participation according to the pre-approval obtained from the Institutional Review board of the Ulsan National Institute of Science and Technology. Participants were divided into two groups: a "know" group of fourteen participants who had known the target faces in person, and a "learn" group of fifteen participants who had not known the target faces before but learned about the targets from the experimenter prior to the experiment.

B. *Stimuli and Experimental Procedure*

A set of twenty-eight color pictures of human faces were built. Four of them were known to the "know" group and determined as target faces. The task for participants was to identify the target face among many presented at the same time. A total of eight pictures randomly selected from the picture set were displayed on the computer monitor in a matrix form. This matrix had 3x3 cells with the eight pictures shown in each cell except for the center cell. The experiment consisted of 96 trials each of which belonged to either a "familiar" trial or an "unfamiliar" trial. In the familiar trial, one of the four target picture was randomly selected, mixed with other non-target pictures and shown in the matrix. Participants searched for the target picture and identified it using a numerical keypad (1~9 keys location-matched to the 3x3 cells on the monitor). If they did not find the target, they pressed the center key (i.e. 5). The unfamiliar trial was identical to the familiar one except that no target picture was presented. The correctness of the target identification was visually fed back to participants at the end of a trial.

The experiment was composed of four blocks that were divided by the duration of picture presentation: 1, 1.5, 2 or 2.5 s. There were 24 trials in each block. The ratio of the familiar and unfamiliar trials in each block was 1:1. EEG and eye tracking data of participants were recorded simultaneously over the entire experiment period. However, the present study only focused on EEG responses in participants. Figure 1 depicts the overall experimental paradigm.

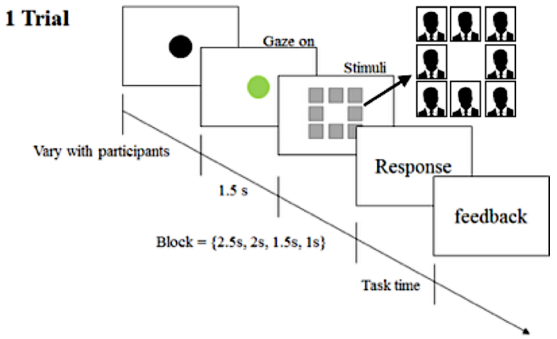

Fig. 1 The illustration of the overall experimental paradigm.

C. *EEG recordings*

Scalp EEG signals were recorded using 31-channel wet Ag/Cl electrodes (actiCHamp, Brain products GmbH, Gilching, Germany). EEG signals were amplified and filtered (band-pass 0.05-100 Hz, sampling rate 500 Hz). The position of the electrodes followed the 10/20 international system: FP1, FPz, FP2, F7, F3, Fz, F4, F8, FT9, FC5, FC1, FC2, FC6, FT10, T7, C3, Cz, C4, T8, CP5, CP1, CP2, CP6, P7, P3, Pz, P4, P8, O1, Oz, and O2 (Figure 2). An additional electrode was attached to the left mastoid as a ground. The EEG signals were referenced to the right mastoid. Electrode impedance was kept below 10 k.

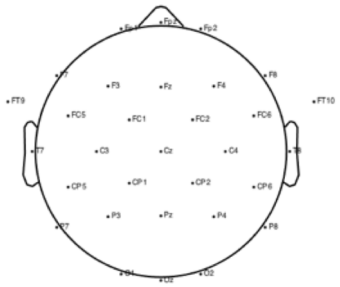

Fig. 2 The montage of the EEG electrode placement employed in this study.

D. *Data analysis*

The recorded EEG data were analyzed offline with MATLAB software. We first examined the quality of the data and excluded those of the participants where there was a loss of data, extraordinary behavior outcomes or substantial contamination by noise. Afterward, we analyzed the data of eighteen participants (nine in the "know' group and the other nine in the "learn" group). EEG data was bandpass filtered again with 0.1 Hz and 55 Hz for low-frequency and high-frequency cutoffs. Independent component analysis (ICA) was applied to the EEG data to minimize eye movement artefacts. Three channels of FP1, FPz and FP2 were excluded due to high noise from eye movements, leaving 28 channels to be further analyzed. Then the EEG signals were re-referenced by the common average reference (CAR) method [12]. The analysis epochs on EEG data were determined based on the task protocol. An epoch of EEG data was extracted from each trial -200 ms before and 800 ms after the onset of the longest fixation on the target picture in the cased of the familiar trials. For the unfamiliar trials, the onset was defined as the time the longest fixation (on one of the eight faces) started. The baseline for the event-related potential (ERP) analysis was set to be -200 ~ 0 ms time-locked to the onset. The EEG signals in each epoch was corrected to the baseline by subtracting the mean of EEG amplitudes within the baseline from the entire EEG signals. The ERPs for each block (i.e. different presentation durations), each trial type (i.e. familiar vs unfamiliar) and each participant were obtained by averaging the EEG signals over epochs.

III. RESULTS

We calculated the error rate of the identification of the target face picture for each participant where participants falsely identified a non-target face as the target or missed the target and hit the center key (i.e. indication of no target). The error rate was 11.9±4.7 % for the "know" group and 11.9±7.5 % for the "learn" group. There was no significant difference in the error rate between the "know" group and the "learn" group (two-sample t-test, $p > 0.05$). We also compared the error rate

between the blocks: the error rate was {18.3±10.9, 10.0±7.0, 10.0±5.6, and 9.5±9.0} % for the blocks with the presentation duration of {1, 1.5, 2, 2.5} s, respectively. There was a significant difference in the error rate between the blocks, showing that the error rate was higher in the block of the shortest presentation (i.e. 1s) than others (ANOVA, $p < 0.05$).

The ERP analysis revealed a specific response of positive deflections around 400 ms after onset. The positive component of ERPs in this period was known as late positive potentials (LPPs). LPPs were manifested over frontal areas in response to the target faces but not clear in response to the non-target faces. The statistical analysis revealed that LPPs at FC1 and F3 in response to the target faces were significantly larger in the "know" group than in the "learn" group ($p < 0.05$) even when both groups successfully identified the target faces (Figure 3).

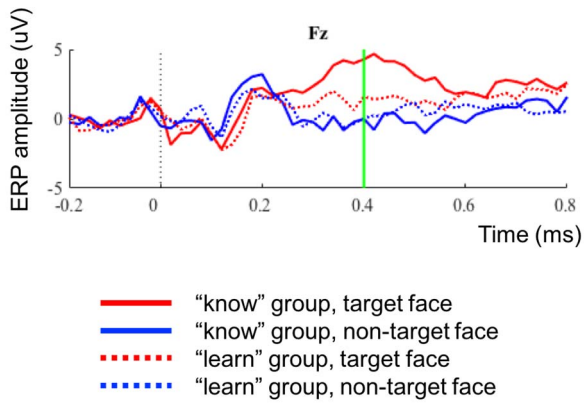

Fig. 3 ERP waveforms of the "know" group and the "learn" group for target face viewing and non-target face viewing trials. 0 s indicates the onset (see text).

In addition, we analyzed the spatial distribution of LPPs by a topological representation. The topography was developed using the LPP amplitudes at 400 ms after onset. It showed that LPPs were predominantly present over the bilateral frontal area (Figure 4).

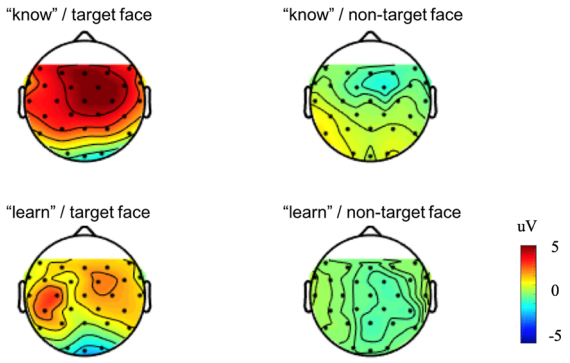

Fig. 4 The topography of the later positive potentials (LPPs) at 400 ms after the onset (see text). Red colors denote relatively larger amplitudes and blue ones denote smaller ones.

Note that little increases in ERP amplitudes were observed in response to the non-target faces. The ERPs here were also obtained from the correct trials only, eliminating potential effects of error potentials integrated in the waveform of ERPs [13].

IV. Discussion

No difference was found in the target face identification accuracy between the "know" and the "learn" groups. It implies that the "learn" group could accurately remember and identify the target person at will. Thus, behavioral performance based on target identification accuracy could be vulnerable to a possible attack by learning the information of the user.

However, this problem could be potentially addressed if an authentication scheme might be able to access the user's brain activity, as demonstrated in this study. Even when the imposter was aware which face the user was familiar with, the brain responses to the target face in the imposters were not as distinct as those in the genuine users. It suggests a feasibility that EEG-based biometrics combined with users' knowledge could fence a multi-level wall, with a lower level of screening for whether the test knowledge is accurately validated and a higher level of screening for whether brain activity induced by the test knowledge is clearly present.

Although the present study only investigated EEG-based biometrics, the eye gaze data collected during the experiment definitely deserve to a further analysis. It is expected that a number of fundamental properties of eye movements in the search for the target face may provide features distinct to the "know" group. If so, the eye gaze features as well as EEG responses shown in this study would collectively form an effective multi-factor authentication framework.

V. Conclusions

The present study investigates a feasibility that brain activity could discriminate an imposter from a genuine user when both were shown a target face. Our results showed that even both imposter and genuine user recognized the same target information to identify (i.e. face), their brain activities were rather different. Hence, an authentication system developed based on this finding would not allow an attack equipped with mere learning of the information the user knows. It is thus anticipated that a more natural and sophisticated personal authentication scheme will be made possible utilizing intrinsic brain mechanisms.

Acknowledgment

This work was supported by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (R0190-16-2054, "Development of Personal Identification Technology Based on Biomedical Signals to Avoid Identity Theft").

REFERENCES

[1] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *J. Comp. Security*, vol. 15, pp. 529-560, July 2007.

[2] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. D. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," *IEEE Trans. Parallel and Distri. Sys.*, vol. 22, pp. 1390-1397, Nov 2010.

[3] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenized random number," *Pattern Recognition.*, vol. 37, pp. 2245-2255, Nov 2004

[4] S. H. Khan, M. A. Akbar, F. Shahzad, M. Farooq, and Z. Kahn, "Secure biometric template generation for multi-factor authentication," *Pattern Recognition.*, vol. 48, pp. 458-472, Nov 2015

[5] C. I. Fan and Y. H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Info. Forensics and Security*, vol. 4, pp. 933-945, Sept. 2009.

[6] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *J. Comp. and Sys. Sci*., vol. 72, pp. 727-740, June 2006.

[7] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, "Multi-factor EEG-based user authentication," *Proc. Int'l Joint Conf. Neural Net*., pp. 4029-4034, Beijing, 2014.

[8] J. C. Lee, "A novel biometric system based on palm vein image," *Pattern Recognition Letters*, vol. 33, pp. 1520-1528, Sept. 2012.

[9] I. Odinaka, P. H. Lai, A. D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, "ECG biometric recognition: a comparative analysis," *IEEE Trans. Info. Forensics and Security*, vol. 7, pp. 1812-1824, Aug. 2012.

[10] E. Maiorana, D. La Rocca, and P. Campisi, "Eigenbrains and Eigentensorbrains: Parsimonious bases for EEG biometrics," Neurocomputing, vol. 171, pp. 638–648, 2016.

[11] S. K. Yeom, H. I. Suk, and S. W. Lee, "Person authentication from neural activity of face-specific visual self-representation," Pattern Recognition, vol. 46, pp. 1159-1169, 2013.

[12] J. Dien, "Issues in the application of the average reference: review, critiques, and recommendations," *Behav. Res. Methods, Inst. and Comp*., vol. 30, pp. 34-43, Mar. 1998.

[13] P. W. Ferrez and J. R. Millan, "Error-related EEG potentials generated during simulated brain-computer interaction," *IEEE Trans. Biomed. Eng*., vol. 55, pp. 923-929, Feb. 2008.