2021 43rd Annual International Conference of the
IEEE Engineering in Medicine & Biology Society (EMBC)
Oct 31 - Nov 4, 2021. Virtual Conference

Secure typing via BCI system with encrypted feedback

Hang Yu[1], Yu Qi[2,*], Hanwen Wang[1], Gang Pan[1,3]

Abstract— Information transmission security is an important issue in many scenarios such as password input. Traditional approaches such as typing or voice input are prone to peep, leading to a risk of information leakage. Brain computer interface (BCI) can read information directly from the brain, which is confidential inherently, thus it may be an ideal way for secure information input. This paper proposes a novel BCI-based secure input approach with encrypted feedback. The encrypted feedback is specially designed to notify users and confuse peepers at the same time. We give the theoretical guarantee of accuracy and evaluate the system with both simulation and experiments. The results show that our method can transmit messages effectively.

I. INTRODUCTION

In modern society, the privacy of information transmission is incredibly important in many scenarios such as password input, banking, and military. Although efforts have been made on encryption of information transmission process, only few studies emphasized on security of input process [1] [2]. Traditional input approaches such as typewriting or voice input can be easily recorded or monitored, leading to a risk of information leakage.

One potential option for secure information input is to use a brain computer interface (BCI) based typewriter. BCI provides a direct information pathway between the brain and external devices [3] [4] [5]. Since BCI does not require explicit body activities to generate information, it has natural merits in confidentiality [6], and may be an ideal way for secure inputting. One problem in current BCI paradigms lies in that, it usually requires visual feedback of the input content which we want to hide [7] [8] [9]. Therefore, how to design a proper feedback for secure BCI input is an important issue.

We propose a BCI based secure input approach with an encrypted feedback method. The BCI typing system is a steady state visual evoked potential (SSVEP) based typewriter. In secure typing situation, the user focuses on the specific stimulus corresponding to the target characters, and then confirms the result by an audio feedback. The audio feedback paradigm is specially designed to contain sufficient information to inform the user while confuse other observers (we refer as 'peepers' below). Specifically, according to the asymmetric information theory, the proposed feedback approach contains multiple targets, including one input target and some confusing targets. The user can judge whether the input is correct by examining whether the input target is included in the feedback targets, while a peeper is difficult to discriminate the input target from the rest ones. The user scenario of the proposed system is illustrated in Fig. 1. We give the theoretical guarantee of accuracy and evaluate the system with both simulation and experiments. The results demonstrate that our method can transmit messages effectively.

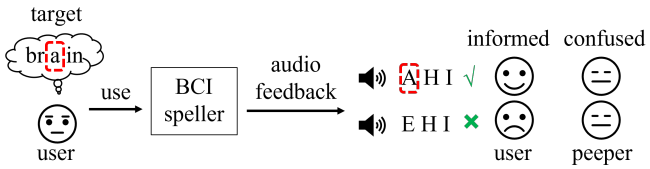


Fig. 1. The user scenario of the proposed system.

The rest of this paper is organized as follows. Section II introduces the speller system construction and performance evaluation criterions. Section III reports the experiment setting and results. Conclusions are drawn in Section IV.

II. METHODS

In this section, we firstly introduce the hardware of our spelling system. Then we illustrate the design of feedback. After that, we present the detection algorithm used in the system. Finally, we state the performance evaluation criterions. In this work, we use an SSVEP BCI speller for brain-based input. The framework of SSVEP-based BCI speller with audio feedback is shown in Fig. 2.

A. Speller System

1) Brain Signal acquisition: 20-channel electroencephalogram (EEG) device (DSI24, Neuracle Inc.) is used to record the subjects' brain responses at 300 Hz. Six electrodes (O1, O2, P3, P4, T5, T6) are selected to use

This work is supported by the Key Research and Development Program of Zhejiang Province in China (2020C03004), and partly supported by the grants from the National Key Research and Development Program of China (2018YFA0701400), and Natural Science Foundation of China (61906166 , U1909202), and the Zhejiang Lab (2019KE0AD01).

[1]Hang Yu, Hanwen Wang and Gang Pan are with the College of Computer Science and Technology, Zhejiang University, Hangzhou, China.

[2]Yu Qi is with the MOE Frontier Science Center for Brain Science and Brain-machine Integration and the College of Computer Science and Technology, Hangzhou, China.

[3]Gang Pan is with the First Affiliated Hospital, College of Medicine, Zhejiang University, Hangzhou, China, and Key Laboratory for Biomedical Engineering of Ministry of Education, Zhejiang University, Hangzhou, China.

*The corresponding authors is Yu Qi: qiyu@zju.edu.cn

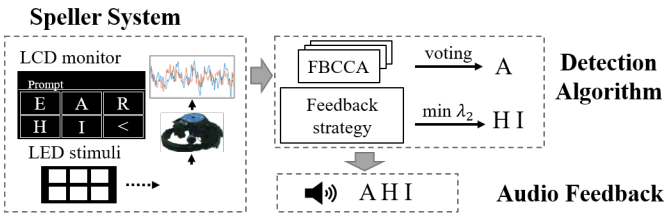
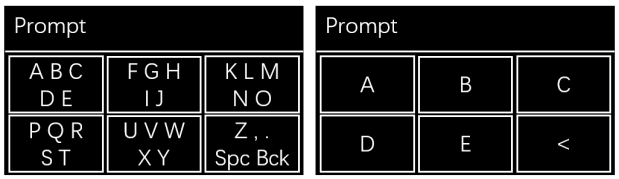


Fig. 2. The framework of SSVEP-based BCI speller with audio feedback.

in the following data acquisition. The reference electrode is placed at earlobes on both sides (A1, A2).

2) SSVEP Stimulus Device: The stimulus device contains two parts: an LED panel is used as stimulus; an LCD monitor is used as prompt.

In spelling experiments, an LCD monitor (E2416H, Dell) is used for the speller interface. Since the number of stimuli is less than the number of characters, we divide the interface into two levels: Level-1 contains all characters and some control symbols (Space, back); level-2 contains only 5 characters and a '<' control symbol for returning to level-1. The Prompt screen is shown in Fig. 3. The prompt program is developed under MATLAB using the Psychophysics Toolbox Version 3 (PTB-3).



(a) level-1 Screen (b) level-2 Screen

Fig. 3. The Prompt screen. (a) Level-1 screen contained all characters and two control symbols. (b) Level-2 screen contained 5 characters and a '<' symbol for returning to level-1. It should be noted that 5 characters may be a subset of one stimulus in level-1, or a probability-ranked set calculated by prompt program.

The stimulation matrix of the BCI speller is presented on a self-made LED panel with the size of 3×2 . The area of each stimulus is 2×2 cm square, and the distance between two neighboring stimuli is 2 cm. The frequency is $s \in \{7, 8, 9, 10, 11, 12\}$ Hz.

B. Feedback Strategy

Assuming that the user's stimulus detection accuracy P_{s_i} to stimulus $s \in \{s_1, s_2, ..., s_N\}$ is a fixed prior. The speller system generates feedback array e. P_e is the probability that target character appears in the feedback:

$$P_e = P_{e_{in}} + P_{e_{out}} \tag{1}$$

where e_{in} is the target character and in the feedback array, e_{out} is not the target but in the feedback array, which we call the 'confusing character'. According to the recognition result of a certain stimulus k, there are four situations:

1) recognize the stimulus correctly, feedback contains the target character.
2) recognize the stimulus incorrectly, feedback contains the target character.
3) recognize the stimulus correctly, feedback does not contain the target character.
4) recognize the stimulus incorrectly, feedback does not contain the target character.

In the above four situations, situation 3 is impossible, and the user can make correct judgments on 1 and 4. So an user's recognition accuracy P_k is,

$$P_k = \frac{P_{s_k} P_{e_{in}} + (1 - P_{s_k})(1 - P_e)}{P_{s_k} P_{e_{in}} + (1 - P_{s_k})(1 - P_e) + (1 - P_{s_k}) P_{e_{out}}} \tag{2}$$

Meanwhile, a peeper's recognition $\tilde{P}_k$ is,

$$\tilde{P}_k = \frac{1}{t+1} \tag{3}$$

where $t \in \{0, 1, 2, ..., N-1\}$ is the number of irrelevant stimulus characters.

Since there is only one target character, we assume,

$$\begin{aligned} P_{e_{in}} &= \lambda_1 \\ P_{e_{out}} &= \lambda_2 \cdot t \end{aligned} \tag{4}$$

where λ_1 and λ_2 are the statistical probability of occurrence of characters (λ_2 is the joint probability of all confusing characters, assuming that the probabilities of occurrence of characters are independent and fixed statistically).

Due to the small range of t, λ_2 can be calculated by maximizing the recognition difference ΔP between user's accuracy P_k and peeper's accuracy $\tilde{P}_k$,

$$\arg\max_{t,\lambda_2} (P_k - \tilde{P}_k) = \frac{t}{t+1} - \frac{\lambda_1 (1 - P_{s_k}) t}{2 P_{s_k} + \lambda_2 (1 - P_{s_k}) - 1} \tag{5}$$

As our goal is to find out the best feedback array under certain t. Our speller chooses the feedback array as,

$$\arg\min_{\lambda_2} \lambda_2 > \lambda_1 (t+1)^2 + 2 - \frac{1}{1 - P_{s_k}} \tag{6}$$

Equation (6) provides a recursive update rule: Given a certain t, the subject observes a target s_k, the speller computes the feedback array with the best λ_2 and updates itself. The feedback strategy workflow is shown in Fig. 4.

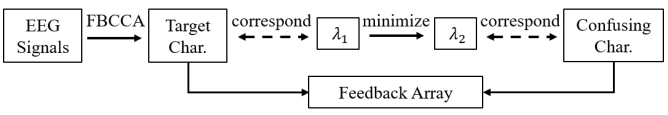


Fig. 4. The workflow of the feedback strategy.

C. Detection Algorithm

1) Data Preprocessing: In pre-test, data epochs are extracted from the flash period. Considering the latency, we set the data epoch length to 4 s. In spelling experiment, incoming data are separated into 2-second length epochs with a 0.2-second time step. A notch filter at 50 Hz is applied to remove power frequency interference. Then all epochs are band-pass-filtered from 4 Hz to 49 Hz with an infinite impulse response (IIR) filter.

2) Feature Extraction: In this paper, we use filter-bank canonical correlation analysis (FBCCA) algorithm to detect SSVEP signal [10].

FBCCA is an extended algorithm on standard canonical correlation analysis (CCA). It can extract target frequencies more efficiently by making use of harmonic SSVEP components to incorporate fundamental and harmonic frequency components. First, filter bank analysis with multiple filters performs sub-band decompositions. In this paper, zero-phase Chebyshev type I infinite impulse response (IIR) filters are used to extract sub-band components from original X. Second, the standard CCA is applied to each sub-band components separately, resulting in correlation values between the components and the reference Y. Finally, target identification is calculated as a weighted sum of square of the correlation values $\rho_k^1, \rho_k^2, ...\rho_k^N$ corresponding to all sub-band components:

$$\tilde{\rho}_k = \sum_{n=1}^{N} w(n) \cdot (\rho_k^n)^2 \tag{7}$$

where n is the index of the sub-band. And the weights $w(n)$ for the sub-band components are defined as follows:

$$w(n) = n^{-a} + b, n \in [1\ N] \tag{8}$$

where a and b are constants. According to the previous study [10], we used $a = 1.25$ and $b = 0.25$.

Since the asynchronous system does not contain timestamps or event triggers, a threshold of correlation values is introduced to distinguish the valid data. Besides, a voting mechanism is included in the program to reduce false feedback. In this study, the threshold value of each subject is unique, and will be fine-tuned during the experiments. The vote number we used is 3. Therefore, the system only sends a control command after receiving three consecutive detection results that exceed the threshold.

D. Performance Evaluation Criterion

To evaluate the performance of our proposed method in simulations and experiments, recognition accuracy and ITR are calculated separately.

Recognition accuracy is calculated by Equation (2) and Equation (3).

Information transfer rate (ITR) has been widely used in evaluating BCIs. It is a comprehensive evaluation indicator as reflecting recognition latency, recognition accuracy and number of recognitions. The calculation of ITR is given as follows:

$$ITR = \frac{60}{T} \times (\log_2 N + P \log_2 P + (1-P) \log_2 \frac{1-P}{N-1}), \tag{9}$$

where T is the averaged response time, N is the number of targets, and P is the averaged classification accuracy, which is calculated and fixed from the offline test.

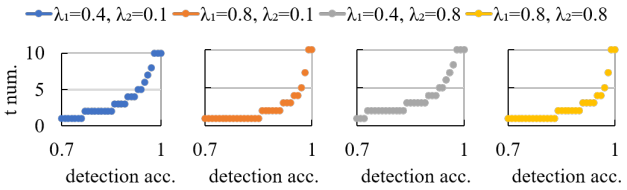


Fig. 5. The optimal feedback number t under different detection accruacy P_s through different λ. The range of t is [1, 10].

III. EXPERIMENT and RESULT

Both simulation and online experiment are carried out to evaluate the proposed approach. In simulation experiments, we test the theoretical input accuracy under various of conditions and select the optimal t. Online experiments report the input accuracy and speed in practical with four participants.

A. Simulation

The purpose of simulation is to find the best confusing character number t under different conditions. Due to the limited number of stimuli on LED panel, t ranges from $[1, 5]$. The selection of t depends on different parameters such as the input accuracy with SSVEP typewriter, number of stimuli. According to Equation 5, we estimate the peeper's recognition accuracy P_{peeper}, the user's recognition accuracy P_{user}, and the maximum accuracy difference ΔP between user's accuracy P_{user} and peeper's accuracy P_{peeper} through all valid t and different λ.

We first explore the best feedback number t. The maximum target number is assumed as 10. As detection accuracy P_s grows, the best t increases rapidly from 1 to all target number during 70% and 100% detection accuracies and is insensitive to the change of λ. The best feedback number of t under different P_s through different λ is shown in Fig. 5.

Then we investigate the recognition accuracy under different λ. The simulations show that, as t increased, P_{user} and P_{peeper} declined continuously, and ΔP will first increase and then decrease. The peak of ΔP is related to λ_1 and λ_2, and λ_2 has a greater impact on ΔP than λ_1. When $\lambda_1 = 0.8,\ \lambda_2 = 0.8$, the peak value is 48.48% at $t = 2$; and when $\lambda_1 = 0.4,\ \lambda_2 = 0.1$, the peak value is 60.19% at $t = 3$. Some typical simulations are shown in Fig. 6. Considering the stimuli number and simulation results, we test $t = 1, 2$ in following spelling experiments.

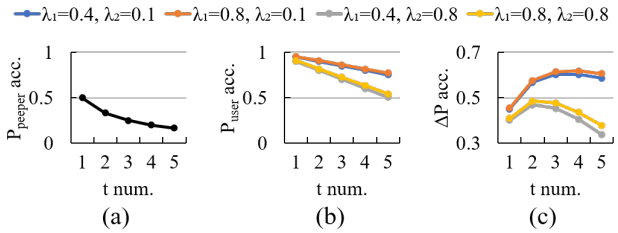


Fig. 6. The recognition accuracy under different λ. (a) the peeper's recognition accuracy P_{peeper} under different t; (b) the user's recognition accuracy P_{user} under different t and λ; (c) the recognition difference ΔP between user's accuracy P_{user} and peeper's accuracy P_{peeper} under different t and λ (Assuming $P_s = 0.9$).

We also simulate the probability of peepers deciphering. According to Equation 3, the accuracy of peeper's recognition is 4.88e-4 under typing 11 characters when $t = 1$ and decreases to 5.65e-11 when $t = 2$. The results show that it is difficult to guess what the subject has inputted from peepers' perspective.

B. Online Experiment

In online experiments, we first collect the SSVEP input accuracy for each subject as priors in pre-test, then we evaluate the spelling performance with the encrypted feedback in spelling experiment.

Four healthy subjects (3 males and 1 female, mean age: 27 years) participate in the whole experiment. All subjects have normal or corrected vision. At the beginning of the experiment, subjects are seated in front of the LED panel and LCD monitor at a distance about 60 cm. During the experiment, subjects are required to stay as still as possible. The whole study was conducted in compliance with relevant laws and institutional guidelines and approved by the Institutional Review Board of Zhejiang University (IRB2019001).

1) Pre-test: The purpose of pre-test is to obtain the subjects' detection accuracy for each SSVEP stimulus. Each test consists of ten blocks. Each block contains 6 trials corresponding to all 6 LED stimuli on panel. The subjects are asked to look at each stimulus one by one. In one trial, all stimuli flash at different frequencies 5 seconds, then blank for 2 seconds. There is no other visual cue during one block experiment, and subjects are asked to avoid eye blinks during the stimulation period.

The average detection accuracy across 6 targets is 93.75%. Among the subjects, the fourth subject shows the highest mean accuracy of 98.33%. All subjects show high accuracy in the pre-test. Detection accuracy for all subjects in pre-test are collected and fixed as priors for speller (see Table I).

2) Spelling Experiment: The spelling experiment requires subjects to type a word or sentence completely using BCIs. In each trial, we ask the subjects to input 'brain' in word and input 'how are you' in sentence. The prompt screen displays the characters correspond to the stimuli on the LED panel one-to-one. Subject looks at a specific stimulus, the system detects the recognition signal and sends the order to the speller. The speller computes the best feedback array by Equation (6), and then updates the prompt screen and outputs array in audio. If subject realizes that he has made a mistake or there is no character he wants on current screen, he can return to level-1 screen by targeting at '<' symbol.

All subjects achieve high accuracy in typing both word and sentence. We examine two situations: $t = 1$ and $t = 2$. The average ITR is 27.54 bits/min with one confusing character feedback in word typing, and 24.17 bits/min with two confusing characters feedback. In sentence typing, the average ITR is 21.76 bits/min and 18.98 bits/min with one and two confusing character numbers, respectively. The ITR is slightly higher on one character feedback than two characters whether typing a word or a sentence. The main cause is that the more characters there are, the longer feedback time will be required, resulting in a lower ITR. Under the same number of confusing characters, the ITR of typing words is higher than typing sentences, which is consistent with the result in [11]. The system spelling performance is shown in Table II.

TABLE I
Detection Accuracy in pre-test

Target	Sub1	Sub2	Sub3	Sub4	Avg. (%)
Target1(%)	100	90	100	100	97.5
Target2(%)	90	90	90	100	92.5
Target3(%)	100	90	90	100	95.0
Target4(%)	100	100	80	100	95.0
Target5(%)	90	80	80	90	85.0
Target6(%)	100	100	90	100	97.5
Avg. (%)	96.67	91.67	88.33	98.33	93.75

TABLE II
Spelling Experiment ITR Result

Confusing Char. Num.	Text	ITR (bits/min)				
		Sub1	Sub2	Sub3	Sub4	Avg.
t=1	word	26.39	33.27	15.38	45.14	27.54
	sentence	19.81	20.57	17.07	29.58	21.76
t=2	word	21.76	20.54	19.00	35.38	24.17
	sentence	20.80	17.06	15.70	22.38	18.98

IV. CONCLUSION

In this paper, we explore a new encrypted feedback method for SSVEP BCIs. To demonstrate the confidentiality of this method, we develop an SSVEP-based BCI speller with audio feedback and test the system on 4 subjects. The results show that the encrypted feedback method can provide a secure information transmission way with satisfactory ITR.

However, the proposed method has some limitations. One limitation lies in that the audio feedback usually takes a long time and hinders the input efficiency.

Besides, separate stimuli and prompts make user occasionally rushed during the input process. We will tackle to the problem by improving the friendliness of interface interaction.

Generally, the privacy merits of BCI are still not developed by commercial use. We hope this work could contribute to diverse feedback BCIs and inspire some new ideas.

References

[1] T. Iwata, K. Minematsu, J. Guo, and S. Morioka, "Cloc: authenticated encryption for short input," in International Workshop on Fast Software Encryption. Springer, 2014, pp. 149–167.

[2] Y. Liu, H. Huang, F. Xiao, R. Malekian, and W. Wang, "Classification and recognition of encrypted eeg data based on neural network," Journal of Information Security and Applications, vol. 54, p. 102567, 2020.

[3] M. A. Lebedev and M. A. Nicolelis, "Brain-machine interfaces: past, present and future," Trends in Neurosciences, vol. 29, no. 9, pp. 536–546, sep 2006. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0166223606001470

[4] H. Ji, B. Chen, N. M. Petro, Z. Yuan, N. Zheng, and A. Keil, "Functional source separation for eeg-fmri fusion: Application to steady-state visual evoked potentials," Frontiers in neurorobotics, vol. 13, p. 24, 2019.

[5] H. Wang, Y. Qi, H. Yu, Y. Wang, C. Liu, G. Hu, and G. Pan, "Rcit: An rsvp-based concealed information test framework using eeg signals," IEEE Transactions on Cognitive and Developmental Systems, 2021.

[6] G. Pfurtscheller, B. Z. Allison, G. Bauernfeind, C. Brunner, T. Solis Escalante, R. Scherer, T. O. Zander, G. Mueller-Putz, C. Neuper, and N. Birbaumer, "The hybrid bci," Frontiers in neuroscience, vol. 4, p. 3, 2010.

[7] M. Mahmood, D. Mzurikwao, Y.-S. Kim, Y. Lee, S. Mishra, R. Herbert, A. Duarte, C. S. Ang, and W.-H. Yeo, "Fully portable and wireless universal brain–machine interfaces enabled by flexible scalp electronics and deep learning algorithm," Nature Machine Intelligence, vol. 1, no. 9, pp. 412–422, 2019. [Online]. Available: http://dx.doi.org/10.1038/s42256-019-0091-7

[8] I. Volosyak, A. Moor, and A. Gräser, "A dictionary-driven SSVEP speller with a modified graphical user interface," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6691 LNCS, no. PART 1, pp. 353–361, 2011.

[9] X. Chen, Z. Chen, S. Gao, and X. Gao, "A high-itr ssvep-based bci speller," Brain-Computer Interfaces, vol. 1, no. 3-4, pp. 181–191, 2014.

[10] X. Chen, Y. Wang, S. Gao, T. P. Jung, and X. Gao, "Filter bank canonical correlation analysis for implementing a high-speed SSVEP-based brain-computer interface," Journal of Neural Engineering, vol. 12, no. 4, p. 46008, 2015. [Online]. Available: http://dx.doi.org/10.1088/1741-2560/12/4/046008

[11] A. Akce, J. J. Norton, and T. Bretl, "An SSVEP-based brain-computer interface for text spelling with adaptive queries that maximize information gain rates," IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 23, no. 5, pp. 857–866, 2015.