Journal of Systems Science and Information
Jun., 2024, Vol. 12, No. 3, pp. 423–432
DOI: 10.21078/JSSI-2023-0113

A Secure Cryptographic System Based on Steady-State Visual Evoked Potential Brain-Computer Interface Technology

Xu XIAO
College of Life and Environmental Science, Minzu University of China, Beijing 100081*, China*
E-mail: *xiaoxu@muc.edu.cn*

Feiyang ZHANG
School of Instrumentation and Optoelectronic Engineering, Beihang University, Beijing 100191*, China*
E-mail: 1417*zfy@buaa.edu.cn*

Wenhan YIN
School of Instrumentation and Optoelectronic Engineering, Beihang University, Beijing 100191*, China*
E-mail: 1014656031@*qq.com*

Dezhi ZHENG*
Advanced Research Institute of Multidisciplinary Sciences, Beijing Institute of Technology, Beijing 100081*, China*
E-mail: *zhengdezhi@bit.edu.cn*

Abstract Addressing the vulnerability of contact-based keyboard password systems to disclosure, this paper proposes and validates the feasibility of a non-contact secure password system based on brain-computer interface (BCI) technology that detects steady-state visual evoked potential (SSVEP) signals. The system first lets a testee look at a digital stimulus source flashing at a specific frequency, and uses a wearable dry electrode sensor to collect the SSVEP signal. Secondly, a canonical correlation analysis method is applied to analyze the frequency of the stimulus source that the testee is looking at, and feeds back a code result through headphones. Finally, after all password codes are input, the system makes a judgment and provides visual feedback to the testee. Experiments were conducted to test the accuracy of the system, where twelve stimulus target frequencies between 10-16Hz were selected within the easily recognizable flicker frequency range of human brain, and each of them was tested for 12 times. The results demonstrate that this SSVEP-BCI-based system is feasible, achieving an average accuracy rate of 97.2%, and exhibits promising applications in various domains such as financial transactions and identity recognition.

Keywords brain computer interface; steady-state visual evoked potential; password system

Received July 24, 2023, accepted March 1, 2024
Supported by Innovative Talents Training Project in the Basic Educational Stage of Beijing ("Soaring Program" Instrument and Student Training in Aerospace Field, Under No. 631306)
* Corresponding author

1 Introduction

With the widespread popularization and development of internet technology applications, information security is becoming increasingly important. Password security is an important component of information security, and keyboard is one of the main devices for password input. At present, the main way to ensure the security of entering passwords on the keyboard is to install a password keyboard cover, which physically prevents passwords from being peeked at. However, even so, there are still many cases of passwords being peeked, which poses new demands for the research of password input systems. In recent years, Brain Computer Interface (BCI) technology has developed rapidly, and its wearable equipment has gradually become lightweight and more comfortable[1]. The recognition accuracy of electroencephalogram (EEG) signals has also been improved to reach a relatively higher level[2]. With BCI technologies, one can use his/her brain to input passwords instead of using fingers, which can further improve the concealment of password input.

In 1973, BCI technology was first proposed by Vidal[3]. The principle of BCI is to detect the electrical signals of the testee's brain reflex activity, analyze the testee's wishes represented by them, and then convert them into commands of the control system program to achieve the goal of understanding and realizing the testee's wishes through the electrical signals. In recent years, thanks to the rapid development of computer technology, biological sciences, and computing algorithms, BCI technology has developed rapidly and become much more applicable[4]. In terms of algorithms, with the continuous development of researchers, the classification accuracy of brain computer interfaces continues to improve. For example, in 2020, Jiang, et al.[5] proposed a new feature selection method for BCIs based on MI, which significantly improved the average classification accuracy by 10.14%. In 2021, the tensor based frequency features combination method and the strategy of using channel level recognition to improve classification performance for Motor Imagery EEG proposed by Pei, et al.[6, 7] improved classification accuracy by approximately 5% and 8.3%, respectively. In terms of applications, researchers have completed using BCI technology to move the cursor and input characters on a computer[8], control flight simulators[9], and replace lost body functions[10, 11]. Nowadays, learning algorithms have developed rapidly[12, 13] and can be applied to improve the accuracy of BCI signal recognition.

Among many BCI technologies, steady state visual evoked potential (SSVEP) Brain-computer interface technology is a branch of key research technology, and has developed rapidly in the past decade[14–21]. In terms of algorithm optimization in SSVEP, the unsupervised learning algorithm[9] using statistical learning methods was the main strategy of the SSVEP analysis algorithm in 2007. However, due to factors such as differences in experimental personnel and weak EEG signals, this algorithm is difficult to achieve excellent system performance. Then, the researchers proposed an algorithm based on supervised learning method[14, 17] to improve the accuracy of the algorithm. In 2018, Jiang, et al. proposed an algorithm for dynamically determining the time required for a single frequency recognition[18], which optimized system performance. These studies indicate that through the unremitting optimization of many researchers, the recognition accuracy of the SSVEP algorithm has gradually improved. In addition to optimizing recognition algorithms to improve accuracy, some domestic and foreign scholars are

also studying methods that can induce the generation of SSVEP signals with higher amplitude and more stability[19]. In terms of technological application, currently researchers have applied SSVEP technology to fields such as healthcare[16] (such as SSVEP controlled wheelchairs[14], spellers[8]), games (Perez Valero designed SSVEP based electronic games[20]), and improved the quality of life for patients with motion disorders such as amyotrophic lateral sclerosis[21], and disabled individuals[22]. However, Vansteensel, et al.[23] pointed out that there is still some way to go before SSVEP technology goes out of the laboratory and is used by the general public, but most researchers are optimistic about this. This indicates that there is still a lot of research gaps for the application of SSVEP technology.

Nowadays, many cracking methods for keyboard password input methods have been developed. For example, Zan[24] proposed a computer vision based password cracking scheme that can analyze the user's input password through video, even if the keyboard is blocked. Liu, et al.[25] proposed a method that can distinguish the position of a user typing on a keyboard using only the microphone of a mobile phone, with precision to the millimeter level. Wang, et al.[26] demonstrated the feasibility of determining passwords by analyzing hand movement trajectories collected by sensors. Therefore, the possibility of keyboard input passwords being cracked has increased, and there is a demand for new, contactless password input methods, which has a certain research gap.

The contributions of this article are as follows:

1. This article designs a non-contact secure password system framework based on SSVEP-BCI technology for special populations, proposing a new solution for identity authentication devices.

2. Experimental verification was conducted and it was found that the system is verified to be applicably feasible, with good signal recognition accuracy and has great application prospects in wearable devices based on BCI for special populations.

The remainder of this study is organized as follows. In Section 2, the principle of SSVEP and the EEG device to-be used in the experiment are introduced. The secure cryptographic system is developed in Section 3, including the system framework and the light source stimulation. in Section 4, experiments were conducted and the results were showed. Section 5 concludes this study.

2 Principle of SSVEP

Steady state visual evoked potential is a brain activity mode of BCI based on scalp EEG, as shown in Figure 1. When the human brain experiences periodic and continuous visual stimuli, a special potential change, SSVEP, is produced. It has a fundamental wave with the same frequency as the stimulus and a harmonic frequency distributed in multiples, mainly located in the visual area of the cerebral cortex in the form of electrical signals. If the testee is asked to look at a stimulus source that flickers at a special frequency, the obvious peak value of the SSVEP signal will be at the flicker frequency of the stimulus source and its harmonic wave, and the steady state will continue the entire stimulation process, and will not return to the resting state. By using the peak value, the frequency and phase difference of the stimulus source that the user is staring at can be determined. Then, through encoding analysis, the type of light

source that the subject is looking at can be determined, and the subject's intention can be understood and the predesigned function can be achieved. The following figure illustrates in detail the principle of SSVEP. The deviation of 0.072 from the peak value is a random error caused by the sensor and is within a controllable range (relative deviation is 0.9%).

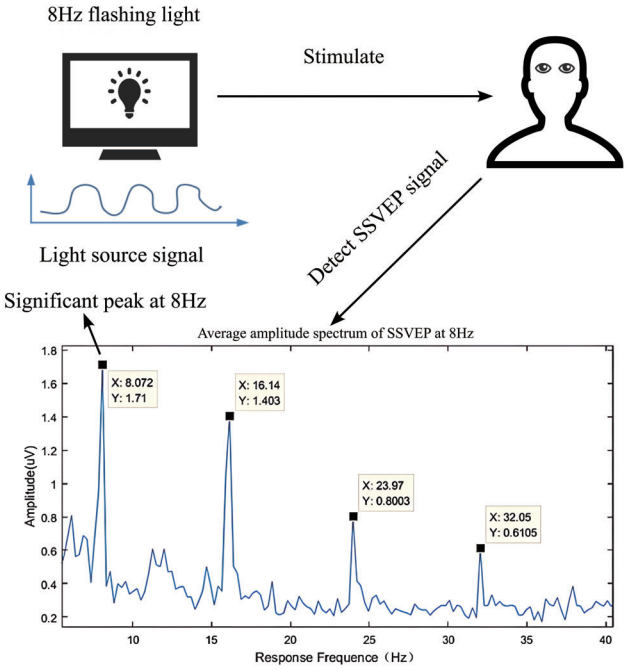


Figure 1 Schematic diagram of SSVEP

2.1 EEG Sensor

The method for collecting EEG signals in this system is to use electrodes in contact with the scalp, which has high time resolution and low cost. In the selection of EEG acquisition equipment, due to the cumbersome preparation steps of wet electrodes, which seriously affect the efficiency of the experiment, this system adopts the self-developed dry electrode as the EEG acquisition equipment[1], as shown in Figure 2.

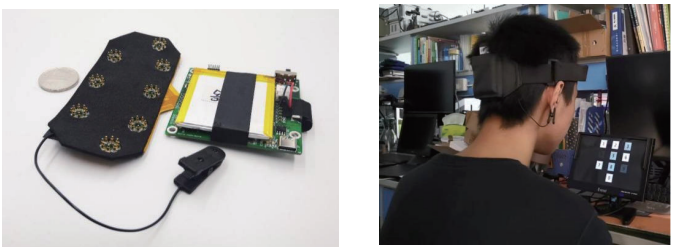


Figure 2 EEG sensor equipment

2.2 Data Acquisition and Bluetooth Transmission Device

The components of EEG signals collected from the scalp are relatively disorderly, with not only weak SSVEP but also interference caused by other physiological signals, which puts

high requirements on the performance of signal acquisition equipment. The signal acquisition equipment used in this system mainly consists of a core circuit board, a lithium battery, and a bluetooth transceiver module. In order to reduce power frequency noise, before the signal enters the core processor, the signal is first filtered out through a 50Hz notch filter to improve the signal-to-noise ratio of the collected signal.

3 Design of the Secure Cryptographic System

3.1 System Framework

This article aims to improve the traditional keyboard input password system, so its input method is similar to the traditional method, but its input method and information feedback method are different. The system innovatively utilizes SSVEP-BCI technology and headphone feedback for password input systems. To protect password privacy, the entered password must be invisible to the outside world. Therefore, this testing system uses bluetooth headphones to play voice feedback to provide user operation prompts. Firstly, after the subject starts the password input program and wears the corresponding device, the system enters password input mode. Secondly, when the subject is staring at the screen, the system will detect and analyze SSVEP, enter the password, and the earphone will inform the user of the password they just entered. Finally, when the participants confirm that the password input is completed, the system will perform a password correctness check and inform the user of the password judgment result. In addition, when the accuracy of the testing system meets the accuracy requirements, the earphone voice feedback method can be cancelled. Figure 3 is the input control logic diagram of the password system.

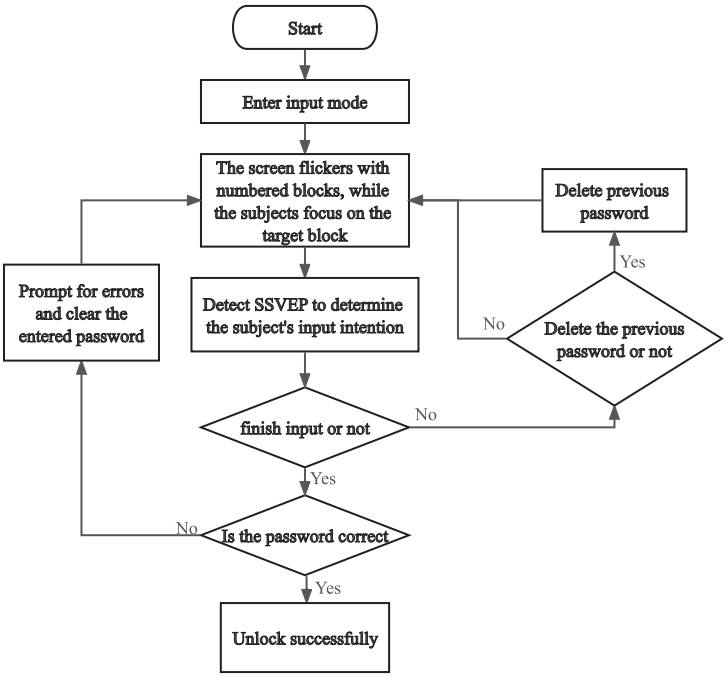


Figure 3 General flowchart of SSVEP based password input system

3.2 Design of Light Source Stimulation

This system has designed a simple password input interface to verify the feasibility and recognition accuracy of the design framework, as shown in Figure 4. The password input screen contains block icons with the numbers 0∼9, "Delete", and "Confirm", all of which are flickering stimuli with different frequencies. After the subject looks at a rectangular digital icon for a period of time, the EEG sensing device detects the SSVEP signal, and then uses the canonical correlation analysis method[2] to input the multi-channel EEG time domain signal X and k groups of standard sine and cosine signal groups $Y = [y_1, y_2, \cdots, y_k]^{\mathrm{T}}$ into the CCA algorithm to output the maximum correlation coefficient ρ, and then identify the frequency accordingly. Finally, according to the SSVEP signal coding table, judge the number the subject looks at, and generate a password input. Each time a password is generated, the system will play it through voice playback and add an • sign in the password input box, in order to provide feedback on the input, and prompt the subject to enter the next password. After the password input is completed, the subject looks at the "Confirm" box, and the system determines whether the password is correct.

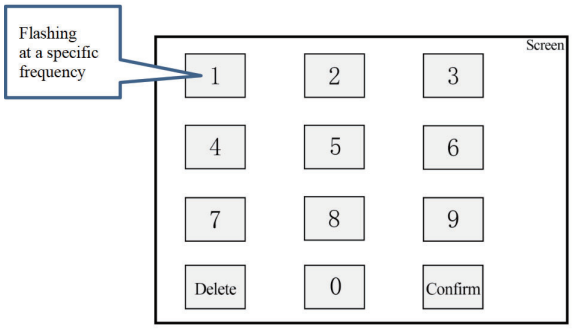
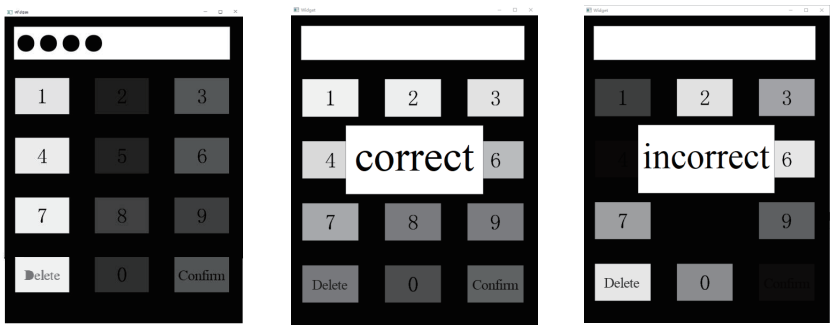


Figure 4 Design of the main page of the password input screen



(a) Input interface (b) Correct interface (c) Incorrect interface

Figure 5 Screenshot of the secure cryptographic system

4 Experiments

This system was implemented using C++ programming language, and ran in a PC computer installed with Window 10 OS system, a set of EEG sensor, and a Bluetooth headset.

4.1 Implementation of Control Code

After the program starts, first call the Widget, Ui_Widget and other classes, which contain functions related to image generation and many parameters, including image path, coordinates, flicker frequency, transparency, etc. These images will continue to flicker as stimuli that trigger SSVEP. After reading the data, the system will calculate the number of refreshes per second according to the refresh rate of the screen device, and start the timer. Every time the timer reaches the set refresh time, the program will update the transparency of the image. Due to the different flash cycles of different image settings, the image will flicker at different frequencies. When the program detects SSVEP, it will call the SSVEP analysis algorithm to analyze it, determine the expected password for the user, play the voice of the number, and save it with QString. After confirming that the password input has been completed, the program will compare the entered password with the pre-set password to see if they are consistent. If the two passwords are completely consistent, a "Password Correct" voice will be played to prompt that the password is correct, and the entered password will be cleared; If the passwords of the two are inconsistent, play the "Password Incorrect" voice, prompt for password incorrect, and clear the entered password. Figure 6 shows the program operation flowchart of this system design.

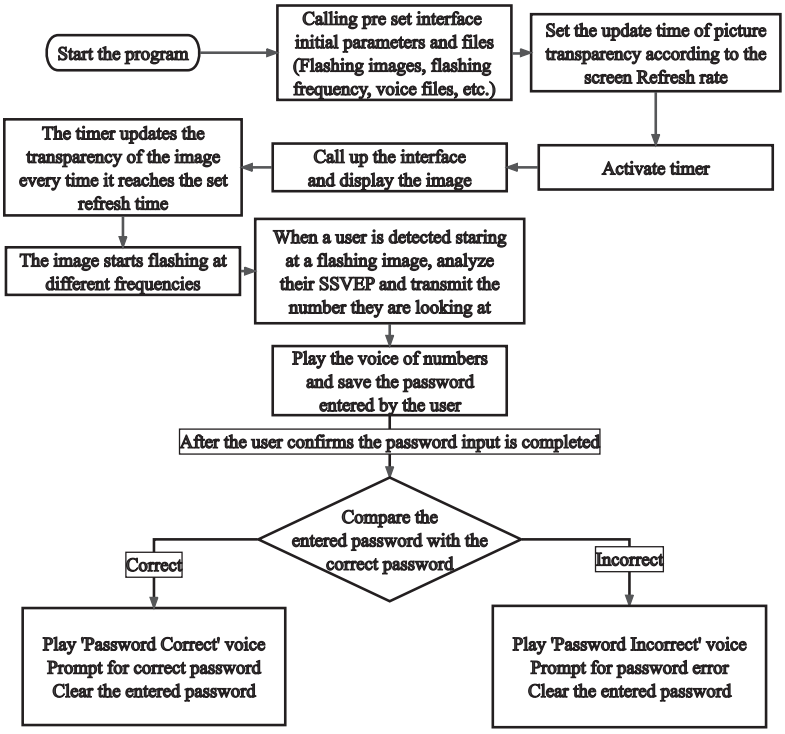


Figure 6 Program operation flowchart of the password system

4.2 Experimental Results and Analysis

The testing system sets the frequency of the stimulus light source to a normal frequency range that is easily recognizable by the human brain, ranging from 10 Hz to 16 Hz. Each acquisition time is 3 seconds. The accuracy of each button is tested in a random order, and each button is repeated 12 times. The data obtained is shown in Table 1. As for subject #1, it can be seen that out of the 12 buttons, 8 buttons have a 100% accuracy rate, and 4 buttons have errors once, with a accuracy rate of 91.7%. The average accuracy rate has reached 97.2%. For subject #2, 10 out of 12 buttons achieved an accuracy of 100%, while the average accuracy reached 97.9%. Considering the impact of human errors, such as subjects' distraction, the average accuracy of the secure system has reached a relative high level. The phase difference of the signal source in this experiment is set to 0, and it is not involved in identifying the role of SSVEP encoding. It should be pointed out that due to the narrow flicker frequency range that easily induces the generation of SSVEP, the corresponding number of recognizable codes is relatively small. When applied to complex cryptosystems including numbers, uppercase and lowercase letters, and special symbols, the combination of frequency domain and phase difference can meet the needs of large numbers of codes.

Table 1 Accuracy of the SSVEP-BCI secure system

Target	Stimulation target frequency	Phase difference	Test times	Correct times		Accuracy	
				Subject # 1	Subject # 2	Subject # 1	Subject # 2
Key 1	10.3 Hz	0	12	12	12	100%	100%
Key 2	10.8 Hz	0	12	12	12	100%	100%
Key 3	11.3 Hz	0	12	12	10	100%	83.33%
Key 4	11.8 Hz	0	12	11	12	91.70%	100%
Key 5	12.3 Hz	0	12	12	12	100%	100%
Key 6	12.8 Hz	0	12	11	12	91.70%	100%
Key 7	13.3 Hz	0	12	12	12	100%	100%
Key 8	13.8 Hz	0	12	12	12	100%	100%
Key 9	14.3 Hz	0	12	11	12	91.70%	100%
Key 0	14.8 Hz	0	12	12	12	100%	100%
Delete key	15.3 Hz	0	12	12	11	100%	91.7%
Confirm key	15.8 Hz	0	12	11	12	91.70%	100%
				Average accuracy		97.2%	97.9%

5 Conclusion

This article proposed a non-contact password input system using a brain computer interface technology. By detecting and analyzing the steady state visual evoked potential of the brain, the system enables users to complete password input just by looking at the screen without contacting. After massive experiments of testing and verification, the results showed that the system

is feasible, and the signal recognition accuracy is high, reaching 97.2% and 97.9%, respectively. Moreover, if strengthened by early training and personalized system settings, there is still much room for the accuracy improvement of the SSVEP signal recognition. In the future, this system has the application prospect in the fields of financial privacy protection, confidential scenario authentication and other industries that need high security level of password input. Moreover, this secure system can also be combined with Augmented Reality (AR) glasses to achieve more privacy and secure applications. It should be pointed out that the SSVEP signal recognition has a relatively long response time, which is related to algorithm design, device signal-to-noise ratio, and the proficiency of the human brain in cryptographic systems. Improving device performance and signal-to-noise ratio is also the future research direction.

References

[1] Na R, Zheng D, Sun Y, et al. A wearable low-power collaborative sensing system for high-quality SSVEP-BCI signal acquisition. IEEE Internet of Things Journal, 2022, 9(10): 7273–7285.

[2] Na R, Hu C, Zheng D, et al. Research on the adaptive brain computer interface technology of synthesizing frequency response characteristics and weight coefficient. Chinese Journal of Scientific Instrument, 2020, 41(5): 154–163.

[3] Vidal J J. Toward direct brain-computer communication. Annual review of Biophysics and Bioengineering, 1973, 2: 157–180.

[4] Jamil N, Belkacem N A, Ouhbi S, et al. Noninvasive electroencephalography equipment for assistive, adaptive, and rehabilitative brain-computer interfaces: A systematic literature review. Sensors, 2021, 21: 4754.

[5] Jiang J, Wang C, Wu J, et al. Temporal combination pattern optimization based on feature selection method for motor imagery BCIs. Frontiers in Human Neuroscience, 2020, 14: 231.

[6] Pei Y, Luo Z, Zhao H, et al. A tensor-based frequency features combination method for brain-computer interfaces. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 2021, 30: 465–475.

[7] Pei Y, Luo Z, Yan Y, et al. Data augmentation: Using channel-level recombination to improve classification performance for motor imagery EEG. Frontiers in Human Neuroscience, 2021, 15: 645952.

[8] Chen X, Wang Y, Nakanishi M, et al. High-speed spelling with a noninvasive brain-computer interface. Proceedings of the National Academy of Sciences, 2015, 112(44): E6058–E6067.

[9] Li C X, Meng Q C, E Y Y, et al. A review of brain-computer information interaction technology. Computer Knowledge and Technology, 2019, 15(3): 184–185.

[10] Chen X, Yang C, Chen Q, et al. Hot topics review of brain-computer interface in 2019–2020. Science & Technology Review, 2021, 39(19): 56–65.

[11] Chen X, Huang X, Wang Y, et al. Combination of augmented reality based brain-computer interface and computer vision for high-level control of a robotic arm. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 2020, 28(12): 3140–3147.

[12] Si H W, Tan G Z, Li D Y, et al. GACS: Generative adversarial imitation learning based on control sharing. Journal of Systems Science and Information, 2023, 11(1): 78–93.

[13] Yang H, Li J. SimCLIC: A simple framework for contrastive learning of image classification. Journal of Systems Science and Information, 2023, 11(2): 204–218.

[14] Zhang Y, Xia M, Chen K, et al. Progresses and prospects on frequency recognition methods for steady-state visual evoked potential. Journal of Biomedical Engineering, 2022, 39(1): 192–197.

[15] Na R, Hu C, Sun Y, et al. An embedded lightweight SSVEP-BCI electric wheelchair with hybrid stimulator. Digital Signal Process, 2021, 116(2021): 103101.

[16] Chen X, Chen Q, Liu B, et al. Application of brain-computer interface technology based on EEG in medical field. Artificial Intelligence View, 2021, 25(6): 6–14.

[17] Jiao Y, Zhang Y, Wang Y, et al. A novel multilayer correlation maximization model for improving CCA-based frequency recognition in SSVEP brain-computer interface. International Journal of Neural Systems, 2018, 28(4): 1750039.

[18] Jiang J, Yin E, Wang C, et al. Incorporation of dynamic stopping strategy into the high-speed SSVEP-based BCIs. Journal of Neural Engineering, 2018, 15(4): 046025.

[19] Han C, Xu G, Jiang Y, et al. Stereoscopic motion perception research based on steady-state visual motion evoked potential. 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Berlin, Germany, 2019: 3067–3070.

[20] Perez-Valero E, Lopez-Gordo M A, Vaquero-Blasco M A. An attention-driven video game based on steady-state motion visual evoked potentials. Expert Systems, 2021, 38(4): e12682.

[21] Li L, Chen X, Sui L. Induction of steady-state motion visual evoked potential and its application in brain-computer interface. Journal of University of Shanghai for Science and Technology, 2022, 44(1): 27–33.

[22] Chen L, Chen P, Zhao S, et al. Adaptive asynchronous control system of robotic arm based on augmented reality-assisted brain-computer interface. Journal of Neural Engineering, 2021, 18(6): 066005.

[23] Vansteensel J M, Kristo G, Aarnoutse J E, et al. The brain-computer interface researcher's questionnaire: From research to application. Brain-Computer Interfaces, 2017, 4(4): 236–247.

[24] Zan X. Resarch on a lock screen PIN cracking method based on computer vision. Xi'an: Xidian University, 2023.

[25] Liu J, Wang Y, Kar G, et al. Snooping keystrokes with mm-level audio ranging on a single phone. Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, 2015: 142–154.

[26] Wang C, Guo X, Wang Y, et al. Friend or foe? Your wearable devices reveal your personal pin. Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, 2016: 189–200.