I Can Think Like You! Towards Reaction Spoofing Attack on Brainwave-based Authentication

Wei-Yang Chiu[1], Weizhi Meng[1,3](✉) and Wenjuan Li[2,3]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
[2] Department of Computing, Hong Kong Polytechnic University, China
[3] Institute of Artificial Intelligence and Blockchain, Guangzhou University, China
weme@dtu.dk

Abstract. In the coming period of Internet of Things (IoT), user authentication is one important and essential security mechanism to protect assets from unauthorized access. Textual passwords are the most widely adopted authentication method, but have well-known limitations in the aspects of both security and usability. As an alternative, biometric authentication has attracted much attention, which can verify users based on their biometric features. With the fast development of EEG (electro-encephalography) sensors in current headsets and personal devices, user authentication based on brainwaves becomes feasible. Due to its potential adoption, there is an increasing need to secure such emerging authentication method. In this work, we focus on a brainwave-based computer-screen unlock mechanism, which can validate users based on their brainwave signals when seeing different images. Then, we analyze the security of such brainwave-based scheme and identify a kind of reaction spoofing attack where an attacker can try to imitate the mental reaction (either familiar or unfamiliar) of a legitimate user. In the user study, we show the feasibility and viability of such attack.

Keywords: EEG, Biometric Authentication, Brainwave-based Unlock, Biometric Security, Reaction Spoofing Attack.

1 Introduction

The Internet of Things (IoT) is developing speedily and steadily, which allows various Internet-enabled devices and equipment to be connected with each other [30]. The Gartner report [9] predicted that the market of enterprise and automotive IoT will grow by around 21 percent and reach 5.8 billion endpoints by the end of 2020, compared with 2019. With so many endpoint devices, user authentication becomes a necessary and important security mechanism to protect assets from unauthorized access.

The traditional user authentication scheme is mainly based on either textual passwords or hardware tokens (e.g., smart cards, keys), which requires interrupting users to obtain their credentials. The system permits their access by

successfully verifying their credentials. Password-based systems are still popular and widely used nowadays due to the simplicity and efficiency. However, such kind of authentication scheme may not be considered as user-friendly and secure enough in practice [7]. For example, a password-based system relies heavily on the complexity of the password. That is, the more complex or longer the password, the more secure the system. While due to both the long-term memory limitation [39] and the multiple password interference issue [24], users are often difficult to remember such complex (or random) strings. In this case, users may choose simple passwords instead, which greatly degrade the system security.

To complement the traditional password-based authentication, biometric authentication receives much attention, which relies on the uniqueness of human's biological characteristics for authentication [21], such as face, hand, retina, fingerprint and so on. As compared with the traditional authentication scheme, the early adoption rate of biometric authentication is not high mainly due to the limitation of sensor accuracy and cost. With the recent advancement of technologies, sensors have become smaller, more accurate and more affordable. Biometrics as an authentication token are being considered in the market, i.e., many operating systems and platforms provide native support. For example, Microsoft introduces Windows Hello, an authentication method that allows users to take their fingerprints or face images as their credentials, and log into the system [11]. Google's Android platform provides the support for developers to combine their scheme with biometric authentication [12], and Apple's iOS platform also provides a similar library to support this [13].

More specifically, biometric authentication can be typically classified as either physiological authentication or behavioral authentication [21]. The former is based on the physical features for user authentication, like face, fingerprint, iris, palmprint, but the main limitation is that these features are constrained resources and cannot be changed. Table 1 shows some popular physiological features. If we considered each characteristic as a single set of passwords, we have a set of non-renewable passwords no greater than the number of 15.

Table 1. Utilizable sets of token of popular physiological authentication.

Biometrics Method	**Attributes Counts**
Face	1
Fingerprints	10
Iris	2
Palmprints	2

With the advancement in bio-sensor technologies, brainwave research based on EEG (electro-encephalography) becomes very popular in recent years. Brainwave, a kind of complicated signal of the active brain, represents every single action or intent humans make. It gives a possibility to investigate the connection between specific brainwaves and actions. The Brain-Computer Interfaces (BCI)

have been applied in some certain domains like healthcare [38] and security [8]. For brainwave-based authentication, EEG sensors can capture the brainwave signals and the system can verify the signal patterns for user authentication. For instance, Marcel and Millan [20] focused on user identification using brainwaves and introduced a statistical framework based on Gaussian mixture models and maximum a posteriori model adaptation. Chuang et al. [6] studied the brainwave authentication and achieved an error rate of around 1% by setting a threshold for each user when they complete custom tasks.

Contributions. In practical usage, brainwave-based authentication also suffers from some challenges. One is that the authentication accuracy may be fluctuant due to high signal similarity of users [20]. While this issue can be mitigated when users perform a particular task. Then Becker et al. [2] tried to identify security issues of brainwave-based authentication by designing a comprehensive framework, but their work did not introduce any findings. With the increasing popularity of brainwave-based authentication, its security receives more attention. Motivated by this issue, the purpose of our work is to investigate the security of a particular brainwave-based authentication method, namely brainwave-based screen unlock. The contributions can be summarized as below.

- We advocate that the accuracy of brainwave-based authentication can be enhanced by given users a particular task, and introduce a brainwave-based computer-screen unlock mechanism that can validate users based on their mental reaction to the displayed image.
- We then analyze such brainwave-based mechanism and introduce a kind of attack called *reaction spoofing attack*, where an attacker is able to unlock the screen by imitating the reaction of a legitimate user.
- In our user study with 37 participants, the results demonstrate the feasibility and viability of *reaction spoofing attack*.

The remaining parts of this paper are organized as follows. In Section 2, we review some related research studies about brainwave-based user authentication and screen unlock schemes. Section 3 describes the brainwave-based screen unlock mechanism and introduces our identified attack. Section 4 describes our experimental settings, analyzes the study results and discusses some challenges. We conclude our work in Section 5.

2 Related Work

2.1 Brainwave and User Authentication

The human brain is the complex and central organ of the human nervous system, which contains billions of nerve cells (namely neurons). Emotions and behaviours are the communication between neurons in the brain. Generally, the brain can include three major parts: the cerebrum, the brainstem and the cerebellum. The cerebrum is the largest part of the human brain, which connects the brainstem and the spinal cord.

Brainwaves are believed to be generated through synchronised electrical pulses from neurons. Our brainwaves can change according to our activities and feelings. People would feel tired when slower brainwaves are dominant, while the higher brainwaves would make people wired. Currently, we can capture brainwave signals using various headset-like devices. For instance, users can mount brainwave-sensing headset like Neurosky [32] and meditation made headband like Muse [29]. Some studies have shown that a computer system was able to identify a person's "brainprint" with nearly 100 percent accuracy [36]. Motivated by this trend, many research studies started focusing on applying brainwaves for user authentication.

As we know, traditional authentication schemes like password-based authentication often require interrupting or prompting the user to manually input or provide credentials, which may require more external equipment hooked on the device. Instead, the use of brainwaves does not need any physical interactions that can provide a transparent authentication process. As compared with some biometrics like fingerprint, brainwave signals are beleived to be more difficult to copy and replay [2]. Moreover, brainwaves can be changed and revoked based on the authentication methods. For example, a person's brainwave signals can be different under particular tasks [41].

In addition, the traditional authentication scheme only checks the legitimacy of a user at the moment of user login. After that, the system would not require further authentication. Hence the scheme can only protect the system at the moment of login, but cannot secure the system during the whole session. Similar to some other biometrics like keystroke dynamics [26] and touch dynamics [25], brainwaves can provide a continuous authentication process as well. The system can keep checking the brainwave signals during the whole session.

2.2 Brainwave-based Authentication

Similar to other biometrics, machine learning is an important tool for classifying brainwave signals. Many algorithms have been studied in EEG classification like kNN [40], Neural Network [4] and SVM [35]. For instance, Liew et al. [17] focused on EEG signals and explored the use of Fuzzy-Rough Nearest Neighbour (FRNN) classifier for EEG authentication. They extracted visual evoked potentials (VEPs) brainwaves data from the lateral and midline electrodes to elicit training and testing datasets. Based on the features like mean, cross-correlation and coherence, their algorithm could achieve an authentication rate of around 90%. To handle the issue of limited training data, they further introduced an Incremental Fuzzy-Rough Nearest Neighbour (IncFRNN) algorithm to reform the personalized knowledge granules via insertion and deletion of a participating object [18]. The algorithm of IncFRNN could reach an accuracy rate of around 96%, based on the similarity measures and predefined window size.

Marcel and Millan [20] used a statistical framework for personal EEG authentication based on Gaussian mixture models. By considering participants' reactions towards imagination movements and words consideration, their method could achieve an authentication rate of 93%. Tran et al. [35] focused on EEG

data and introduced an SVM binary classification method to improve the performance of the minority class in imbalanced datasets. By exploring participants' reactions towards the motor imagery of hand, foot and tongue, their improved SVM could reach an accuracy rate of 96.10%. Chiu et al. [5] also focused on studying the link between experienced events and brainwave reaction, and established an authentication system based on such reactions. With an SVM classifier and 20 participants, their system could achieve an accuracy rate of almost 100%, which validated the results in [36].

Zhou et al. [41] explored the feasibility of extracting long-term memory ability from users' brainwaves and identified the bio-features in the brainwaves. In their settings, their SVM classifier could reach an authentication rate of 90%. Pham et al [33] advocated that EEG could enhance the existing authentication mechanisms, and introduced an approach of using EEG to authenticate users in a multilevel security systems. Users need to conduct motor imagery tasks while their EEG signals would be tested for authentication. Based on the Graz datasets 2008, their method could provide an accuracy rate of around 90%. They further introduced an algorithm of The Small Sphere Two Large Margins Support Vector Data Description (SS2LM-SVDD), in order to build an optimal hyper-sphere in feature space [34]. They then designed an improved multilevel security system by combining mental tasks, age and gender information, which could reach an accuracy rate of around 97%.

Altahat et al. [1] tried to identify the factors that may affect the robustness of EEG-based authentication. They explored some factors such as the enhancement threshold value, EEG frequency rhythms, mental task and the person identity on the selected EEG channels. Their results demonstrated that the idle mental task may provide the highest accuracy rates as compared with other mental tasks in the settings. They also showed that the combined frequency rhythms could provide better authentication performance than using a single rhythm. Wang et al. [37] then proposed a multi-modal biometrics system that can continuously verify the identity of current user by considering both face images and Electroencephalography (EEG) signals. For authentication, their system fused the matching scores from these two modalities, and an overall accuracy rate of 90% could be achieved. Abo-Zahhad et al. [28] introduced a multi-level biometric authentication by using Electro-Encephalo-Gram (EEG) signals and eye blinking Electro-Oculo-Gram (EOG) signals. They applied density based and canonical correlation analysis strategies, and used the autoregressive model for EEG signals during relaxation or visual stimulation. With 31 participants and Neursky Mindwave headset, their results showed an authentication rate of 99%.

The results from the above studies indicate the feasibility of building EEG-based user authentication, but also show that classifier performance is not stable based on concrete datasets. For instance, Lotte et al. [19] found that many classifiers like FRNN and Probabilistic Neural Network could be effective in classifying EEG signals from stimulation and reaction, but are not suitable for classifying all EEG signals. Some more related studies can refer to recent studies [10, 14, 27, 31] and a survey [3].

2.3 Screen Unlock Mechanism

To against unauthorized access on devices, designing unlocking schemes are a basic and efficient solution. Currently, Android unlock patterns [22, 23] are the most widely implemented unlock scheme on mobile devices, which requires users to input a correct pattern in a 3×3 grid.

There are many different unlock schemes in the research community. Izuta et al. [15] introduced a screen unlocking system based on an accelerometer and pressure sensor arrays mounted on a mobile phone. When a user takes the phone from the pocket, the system could authenticate the user's behavior. Their system could achieve a false acceptance rate of 0.43. Li et al. [16] proposed a method of verifying swiping behavior and designed SwipeVlock, a supervised unlocking mechanism on smartphones, which can authenticate users based on their way of swiping the phone screen with a background image. With 150 participants, their results showed that participants could perform well with a success rate of 98% during login and retention. However, unlock mechanisms would be compromised when the pattern is leaked. Hence there is a developing trend of combining unlock schemes with biometrics.

3 Brainwave-based Unlock Mechanism and Our Identified Attack

In this section, we introduce the brainwave-based unlock scheme and the identified reaction spoofing attack.

3.1 Brainwave-based Unlock Scheme

As discussed above, due to the unstable performance given by learning classifiers, we notice that brainwave-based authentication is often used to help control legitimate access to assets. In this work, we focus on brainwave-based authentication and its application in designing a screen unlock mechanism on common computers, based on previous work [41, 5].

Figure 1 shows the design of such screen unlock mechanism, which can verify users based on their mental reaction (either familiar or unfamiliar) towards the images shown on the screen. The image pool contains various images that are predefined by the system. An image example is depicted in Figure 1, which shows the desktop of a user's computer with an ordinary word processor running, a taskbar, a wallpaper, and several application icons. If the user presents a correct brainwave pattern, then the authentication is successful.

In practice, the system can display different images and check users' mental reactions (familiar or not) as compared with the recorded EEG pattern. In the literature, most studies follow such idea to design different authentication schemes. For instance, Chuang et al. [6] showed that the error rate could reach 1% when given a particular custom task to users, which is similar to the unlock scheme in this work.

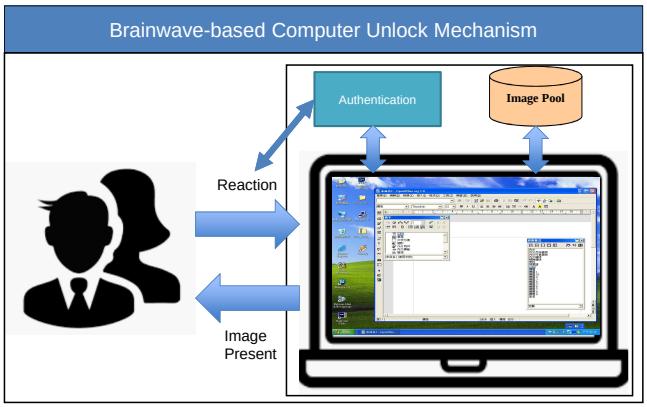

Fig. 1. The design of brainwave-based screen unlock mechanism

3.2 Our Identified Attack

In practical usage, we notice that many things may create a feeling of familiarity among different users, such as an iconic logo of a brand, an iconic design, and an iconic appearance of people. It is a phenomenon that would usually not cause any trouble, but it may bring a security concern to the brainwave-based authentication. This is because the mental reactions rely heavily on the experience and familiarities of a person. Then a question comes to the above brainwave-based screen unlock mechanism: what if the displayed image(s) is/are not only familiar to the legitimate user? For instance, different people may have the same feeling of familiarity regarding a smartphone with the same brand and model.

Survey. To investigate this issue, we perform a survey via Facebook platform with a total of 88 respondents regarding their familiarity level toward the image as shown in Figure 1. The responses are classified into five categories as below.

- I am not familiar with the image.
- I feel familiar because of the taskbar and titlebar.
- I feel familiar because of the wallpaper.
- I feel familiar because of the application icon.
- I feel familiar because of the word processor.

The survey result is summarized in Table 2. It is found that only four respondents were not familiar with the image, whereas up to 95.5% respondents were shown familiar with part(s) of the image. It is worth noting that some respondents can choose to be familiar with several parts of the image, like both wallpaper and application icon. The results validate that the screen unlock mechanism based on familiarity level may be vulnerable to some attacks.

Reaction Spoofing Attack. Motivated by the above observation, we figure out that an imposter has a good chance to imitate the mental reactions (either familiar or unfamiliar) of a legitimate user toward the displayed image(s), called *reaction spoofing attack*. The attack effectiveness is due to that classifiers cannot

Table 2. Questionnaire Result.

Familiarity Level	Number of Respondents
Not familiar	4
Familiar with Taskbar	37
Familiar with Wallpaper	35
Familiar with Word Processor	8
Familiar with Icons	16

Table 3. Environment Configuration

Hardware	**Attributes**	
Software	**Specification**	**Description**
Notebook	Acer TravelMate 4750	Collect Brainwave and Displaying Pictures to the participants
Desktop	Asus BM6AF	Receive the data from notebook and perform data classification
Brainwave Headset	BRI BR8-801	The brainwave headsets for participants.
Operating System	Microsoft Windows 10	
Program Platfom	Oracle Java 11	The program platform for displaying pictures, sending marks to the brainwave collector program
Brainwave Collector	BRI Brainwave Collector	The program extract the Brainwave headset's signal, also receive marks from our custom program
Classifier	libSVM	The main classifier for the experiment.

differentiate the people if they all show the same mental reactions toward the displayed image.

4 Evaluation

To explore the feasibility and performance of our identified attack, we perform a user study with a total number of 37 participants. The recruitment was performed via Emails and colleague recommendation.

4.1 Environmental Settings

All the participants are students from the same campus, who have an interest in our study. Before the experiment, we explained the study goal and how we collect and store the data. Table 3 summarizes the environmental settings. As a study, our brainwave-based screen unlock mechanism adopts support vector machine (SVM) as the classifier to verify users based on their familiarity level toward the displayed image(s). The selection is due to its popularity (see Table **??**) and the capability of handling high-dimensional data.

To ensure that all participants can generate the brainwave signals with a familiar feeling, we selected the iconic images from the university campus, such as library surroundings, department building, and administration building. The participants should wear the BRI brainwave headset (refer to Figure 2), which can capture their brainwave signals when they see the displayed images on the computer screen.

Fig. 2. The participant wearing headset while seeing the image(s)

In addition, with the purpose of collecting good-quality brainwave signals without the potential influence by image display, we adopted the following steps to display images, based on the previous studies [41, 5].

- A 15 seconds blank screen to attract participants and make them calm down.
- To display the images from the iconic building within the campus. Each image was displayed for 3 seconds, and there is a 3-second blank between any two images to prevent fatigue.
- To display the images with cold topics captured from the Internet, with the above same steps.

To preclude the potential influence caused by the screen display, we collected the brainwave signals by playing the image in the fullscreen mode. For data collection, the BRI headset stores the data in CSV format, with a special mark placed at the end of data records. These special marks are created based on the front image, whenever there is an event occurred. Fig. 3 shows an example, in our program, we send an ASCII character 'G' to the BRI Brainwave Collector if the program starts to display an image. When the program is about to close the display, we send an ASCII character 'C'. The practice of sending marks is important, which enables us to extract the accurate duration of image display with participants' brainwave signals. As the image is displayed in a fixed order, there is no need to send extra information to identify images.

As all the existing brainwave headsets are non-invasive, the environmental issues can affect the process of data collection, such as participant's skin conductivity, electric cords in the wall, and appliances nearby. The BRI Brainwave

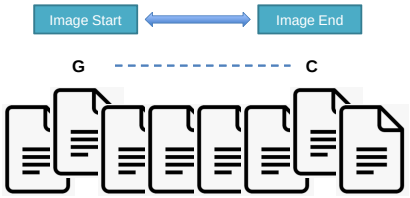

Fig. 3. An example of marks

Collector provides the built-in filter for alternating the current nearby electric cords. However, to minimize the unwanted effect like group shifting, instead of directly using the brainwave raw data, we retrieve only the delta value between records as the input data, based on the following equation [5].

$$\Delta_R = R_i - R_{i-1}1 \tag{1}$$

where R_i means the brainwave raw data at record i.

4.2 Study Results

To analyze the data and train the SVM classifier, we used 70% of the data for training and the rest for testing (with ten-fold cross validation).

With four participants. We first investigate the initial performance with four participants (namely CYU, RYC, WYN and YZW) as shown in Figure 4. It is found that SVM classifier has the tendency by classifying all participants as just one participant (e.g., YZW).

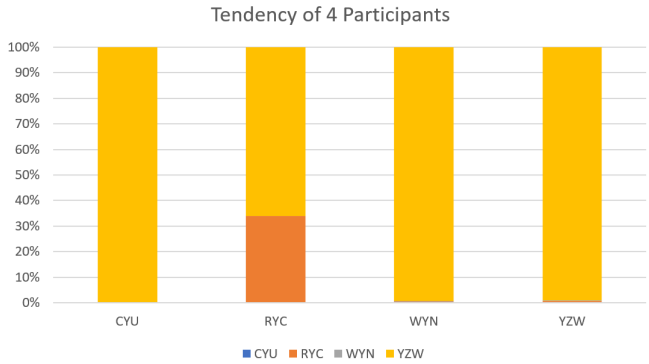

Fig. 4. User classification based on familiarity with 4 participants

To abstain any potential issues caused by the classifier itself, we also collected the participants' brainwave signals regarding unfamiliarity. Figure 5 shows that the SVM classifier has the capability of distinguishing both familiarity and

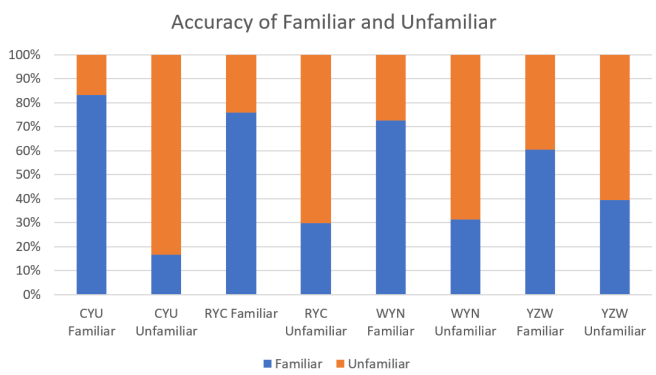

Fig. 5. Classification between familiarity and unfamiliarity by SVM

Table 4. The expected mental reaction for each image.

Image and Reaction				
Image 1	**Image 2**	**Image 3**	**Image 4**	**Image 5**
Familiar	Familiar	Unfamiliar	Familiar	Unfamiliar

unfamiliarity for each participant. Thus, the results indicate that our identified reaction spoofing attack is feasible, i.e., YZW can impersonate as the other three participants and unlock the screen.

With 37 participants. We then investigate the performance of our identified attack with the data from all participants. Table 4 summarizes the expected mental reaction for each image, with either familiarity or unfamiliarity.

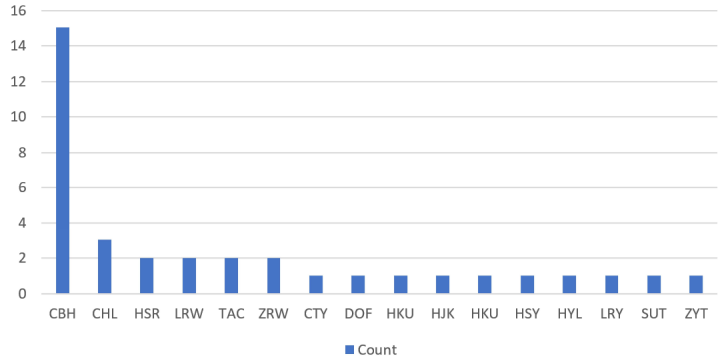

Fig. 6. Classification result with 37 participants

When all participants show the same feeling of either familiarity or unfamiliarity, Figure 6 depicts the classification result given by SVM. It is found that CBH has a possibility of above 50% to impersonate as others and then success-

fully unlock the computer screen. The observation indicates the practicability of our identified reaction spoofing attack in a real-world scenario.

4.3 Discussion

In the study, our results indicate that the (SVM) classifier is able to tell the familiarity and unfamiliarity, but cannot tell the difference between individuals if they have the same feeling of either familiar or unfamiliar, even if they show the same feeling according to a different thing (or image). Hence the brainwave-based screen unlock mechanism based on familiarity and unfamiliarity is not secure in practice, i.e., it would be vulnerable to our identified reaction spoofing attack, and some additional security mechanisms should be considered.

Due to the privacy concerns and the time consumption of collecting brainwave signals, most existing research studies often adopted around 20 or fewer participants. For example, there are 9 participants in [20], 15 participants in [6] and 18 participants (two datasets) in [35]. By contrast, in this work, we involved a total of 37 participants, which we considered is a good number. Indeed, how to involve more participants is an open challenge in the research of brainwave-based authentication. In our future work, we plan to involve more participants to validate our results.

5 Conclusion

With the rapid growth of IoT devices, brainwave-based authentication has received much attention, aiming to provide an enhanced user experience and protect assets from unauthorized access. However, we notice that such brainwave-based authentication may be vulnerable in practical usage. In this work, we focus on the brainwave-based computer-screen unlock mechanism and identify a kind of reaction spoofing attack, in which an imposter is able to unlock the screen by imitating the mental reaction (either familiar or unfamiliar) of a legitimate user. In the user study with 37 participants, our results demonstrate the feasibility and viability of such attack. Our work attempts to complement existing studies and stimulate more research on designing more secure brainwave-based authentication.

Acknowledgments. This work was partially supported by National Natural Science Foundation of China (No. 61802077).

References

1. S. Altahat, G. Chetty, D. Tran, W. Ma: Analysing the Robust EEG Channel Set for Person Authentication. ICONIP (4) 2015: 162-173 (2015)
2. K. Becker, P.A. Cabarcos, T. Habrich, C. Becker: Poster: Towards a Framework for Assessing Vulnerabilities of Brainwave Authentication Systems. *In: Proc. CCS*, pp. 2577-2579, 2019.

3. A.J. Bidgoly, H.J. Bidgoly, Z. Arezoumand, "A survey on methods and challenges in EEG based authentication," *Comput. Secur.* 93, pp. 101788, 2020.
4. C.H. Chen, C.Y. Chen: Optimal fusion of multimodal biometric authentication using wavelet probabilistic neural network. *In: Proc. ISCE*, pp. 55-56, 2013.
5. W. Chiu, K.-H. Yeh, A. Nakamura: Seeing Is Believing: Authenticating Users with What They See and Remember. ISPEC 2018: 391-403 (2018)
6. J.C.-I. Chuang, H. Nguyen, C. Wang, B. Johnson, "I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves," Financial Cryptography Workshops, pp. 1-16, 2013.
7. H. Crawford, "Understanding user preceptions of transparent authentication on a mobile device.," *Journal of Trust Management*, vol 1, no. 1, 2014.
8. R. Damasevicius, R. Maskeliunas, E. Kazanavicius, and M. Wozniak, "Combining cryptography with EEG biometrics," *Computational intelligence and neuroscience* 1867548:1-1867548:11, 2018.
9. Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. (accessed on 12 April 2020) `https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io`
10. E. Gupta, M. Agarwal, R. Sivakumar: Blink to Get In: Biometric Authentication for Mobile Devices using EEG Signals. ICC 2020: 1-6
11. "Biometric Facial Recognition - Windows Hello," Microsoft. (accessed on 21 April 2020) [Online]. Available: `https://www.microsoft.com/en-us/windows/windows-hello`
12. "Biometrics — Android Open Source Project," Google. (accessed on 24 April 2020) [Online]. Available: `https://source.android.com/security/biometric`
13. "Human Interface Guidelines - Apple Developer "Authentication - User Interaction - iOS - Apple Developer," Apple. (accessed on April 24, 2020) [Online]. Available: `https://developer.apple.com/design/human-interface-guidelines/ios/user-interaction/authentication/`
14. H. Huang, L. Hu, F. Xiao, A. Du, N. Ye, F. He: An EEG-Based Identity Authentication System with Audiovisual Paradigm in IoT. Sensors 19(7): 1664 (2019)
15. R. Izuta, K. Murao, T. Terada, T. Iso, H. Inamura, M. Tsukamoto: Screen Unlocking Method using Behavioral Characteristics when Taking Mobile Phone from Pocket. MoMM 2016: 110-114
16. W. Li, J. Tan, W. Meng, Y. Wang. A Swipe-based Unlocking Mechanism with Supervised Learning on Smartphones: Design and Evaluation. Journal of Network and Computer Applications, vol. 165, 102687, 2020.
17. S.H. Liew, Y.H. Choo, Y.F. Low, "Fuzzy-Rough Nearest Neighbour classifier for person authentication using EEG signals," *In: Proc. iFUZZY*, pp. 316-321, 2013.
18. S. Liew, Y.H. Choo, Z.I.M. Yusoh, Y.F. Low, "Incrementing FRNN model with simple heuristic update for brainwaves person authentication," *In: Proc. IECBES*, pp. 115-120, 2016.
19. F. Lotte, L. Bougrain, A. Cichocki, M. Clerc, M. Congedo, A. Rakotomamonjy, and F. Yger, "A review of classification algorithms for EEG-based brainCcomputer interfaces: a 10 year update," Journal of Neural Engineering, vol. 15, 031005, 2018.
20. S. Marcel, J.R. Millan, "Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation," *IEEE Trans. Pattern Anal. Mach. Intell.* 29(4): 743-752 (2007)
21. W. Meng, D.S. Wong, S. Furnell, and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1268-1293, 2015.

22. Meng, W.: Evaluating the Effect of Multi-Touch Behaviours on Android Unlock Patterns. Information and Computer Security, vol. 24, no. 3, pp. 277-287, Emerald (2016)
23. Meng, W., Li, W., Wong, D.S., Zhou, J.: TMGuard: A Touch Movement-based Security Mechanism for Screen Unlock Patterns on Smartphones. In: Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS), pp. 629-647 (2016)
24. W. Meng, W. Li, L.W. Hao, L. Jiang, J. Zhou: "A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords," *In: Proc. ACNS*, pp. 145-162, 2017.
25. W. Meng, Y. Wang, D.S. Wong, S. Wen, and Y. Xiang, "TouchWB: Touch Behavioral User Authentication Based on Web Browsing on Smartphones," *Journal of Network and Computer Applications*, vol. 117, pp. 1-9, 2018.
26. F. Monrose, A.D. Rubin: "Keystroke dynamics as a biometric for authentication," *Future Gener. Comput. Syst.* 16(4), pp. 351-359, 2000.
27. L.A. Moctezuma, M. Molinas: Event-related potential from EEG for a two-step Identity Authentication System. INDIN 2019: 392-399
28. M. Abo-Zahhad, S.M. Ahmed, S.N. Abbas: A new multi-level approach to EEG based human authentication using eye blinking. Pattern Recognit. Lett. 82: 216-225 (2016)
29. "Muse^{TM} - Meditation Made Easy with the Muse Headband," Muse (accessed on 24 April 2020) [Online]. Available: `https://choosemuse.com/`
30. M.B.M. Noor, W.H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Networks* 148: 283-294, 2019.
31. T. Nakamura, V. Goverdovsky, D.P. Mandic: In-Ear EEG Biometrics for Feasible and Readily Collectable Real-World Person Authentication. IEEE Trans. Inf. Forensics Secur. 13(3): 648-661 (2018)
32. "EEG-ECG-Biosensors," NeuroSky (accessed on 24 April 2020) [Online]. Available: `http://neurosky.com/`
33. T. Pham, W. Ma, D. Tran, P. Nguyen, D.Q. Phung: EEG-Based User Authentication in Multilevel Security Systems. ADMA (2) 2013: 513-523
34. T. Pham, W. Ma, D. Tran, P. Nguyen, D.Q. Phung: Multi-factor EEG-based user authentication. IJCNN 2014: 4029-4034 (2014)
35. N. Tran, D. Tran, S. Liu, L. Trinh, T. Pham: Improving SVM Classification on Imbalanced Datasets for EEG-Based Person Authentication. *In: Proc. CISIS-ICEUTE*, pp. 57-66, 2019.
36. Researchers can identify you by your brain waves with 100 percent accuracy. `https://www.sciencedaily.com/releases/2016/04/160418120608.htm`
37. M. Wang, H.A. Abbass, J. Hu: Continuous authentication using EEG and face images for trusted autonomous systems. PST 2016: 368-375 (2016)
38. J. Wolpaw and E.W. Wolpaw, Brain-Computer Interfaces: Principles and Practice. Oxford University Press, Oxford, UK, 2012.
39. J. Yan, A.F. Blackwell, R.J. Anderson, A. Grant: Password Memorability and Security: Empirical Results. *IEEE Secur. Priv.* 2(5): 25-31, 2004.
40. M.L. Yiu, E. Lo, D. Yung: Authentication of moving kNN queries. *In: Proc. ICDE*, pp. 565-576, 2011.
41. L. Zhou, C. Su, W, Chiu, K,-H, Yeh, "You Think, Therefore You Are: Transparent authentication system with brainwave-oriented bio-features for IoT Networks," *IEEE Transactions on Emerging Topics in Computing*, 2017.