J Inf Process Syst, Vol.16, No.5, pp.1034~1047, October 2020
https://doi.org/10.3745/JIPS.03.0147

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Next-Generation Personal Authentication Scheme Based on EEG Signal and Deep Learning

Gi-Chul Yang*

Abstract

The personal authentication technique is an essential tool in this complex and modern digital information society. Traditionally, the most general mechanism of personal authentication was using alphanumeric passwords. However, passwords that are hard to guess or to break, are often hard to remember. There are demands for a technology capable of replacing the text-based password system. Graphical passwords can be an alternative, but it is vulnerable to shoulder-surfing attacks. This paper looks through a number of recently developed graphical password systems and introduces a personal authentication system using a machine learning technique with electroencephalography (EEG) signals as a new type of personal authentication system which is easier for a person to use and more difficult for others to steal than other preexisting authentication systems.

Keywords

Electroencephalography, Information Security, Machine Learning, Personal Authentication

1. Introduction

According to Wikipedia, “Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity” [1]. Personal authentication is the process of confirming the identity of a person and an essential tool for everybody in this modern information society. The importance of the security of various digital devices increases day-by-day.

Traditionally, the most general mechanism of authentication was alphanumeric passwords. Passwords are a convenient and efficient scheme of authentication, but they do have drawbacks. Passwords should be easy to remember, but hard to break. However, passwords that are hard to guess or to break, are often hard to remember. That is one of the big problems of text-based passwords.

Also, a user may have many accounts and each account requires a long password to strengthen security. However, long text-based passwords are hard to remember. Moreover, it is cumbersome to utilize different passwords for each account, so a user may employ the same password for many or all accounts. Using one password for multiple accounts is a very dangerous habit: a single compromised password could lead to a total loss of security. Hence, there is a trend to replace text-based password systems with other password systems. An emerging research topic on personal authentication focuses on developing a secure and user-friendly authentication system.

Manuscript received January 23, 2020; first revision April 8, 2020; accepted May 18, 2020.
Corresponding Author: Gi-Chul Yang (gcyang@mokpo.ac.kr)
* Dept. of Convergence Software, Mokpo National University, Mokpo, Korea (gcyang@mokpo.ac.kr)

Graphical passwords have begun to be used in authentication systems based on the fact that people can remember images better than text [1]. Graphical passwords can be an alternative to either of these systems. Graphical passwords have been developed to solve the problems described above. They use images rather than letters or numbers, so they are easier to remember than text-based passwords. Also, users can change their password whenever they want. However, graphical passwords, which are generally easy to remember, have the disadvantage of being easy to steal from others. Hence, they provide a poor defense against shoulder-surfing attacks, since others can remember graphics easily, too. Therefore, this paper introduces a reliable password system using brain-computer interface (BCI) as a new type of personal authentication system which is easy for users to use and is difficult for others to steal.

Since Berger [2] discovered brainwaves, electroencephalography (EEG) has long been used mainly in hospitals and laboratories to assess neurological disorders, to investigate brain function, and several studies [3–5] have explored the possibility of treatment. As the research progresses, it has developed into a research that can interpret the brain waves to read other people's thoughts and use them to adjust peripheral devices or communicate with others [6]. Recently, researches on the BCI have been actively conducted in various areas [7,8]. This paper introduces a password system based on EEG and deep learning techniques for personal authentication.

Using brainwaves as a password has the advantage that it is hard for others to steal. However, it is difficult to guarantee its reliability because of the technical limitations of current brainwave signal interpretation. Therefore, to guarantee the reliability of brainwave information, this study suggests developing a system using EEG based deep learning technique. This idea makes it possible to develop a reliable password system that utilizes the difficulty of stealing brain information.

The remainder of the paper is organized as follows. The following section briefly reviews some exemplars of recently developed graphical password schemes. Section 3 introduces EEG signals. Section 4 introduces a machine learning-based password system. Conclusion and future work are addressed in Section 5.

2. Recent Development of Graphical Password Systems

Research in the graphical password scheme, which increases both the security and usability, has accelerated over the years. The graphical password was first proposed by Blonder [9] and uses many preselected small regions in an image to compose a password, instead of alphanumeric codes. The user has to choose some of these regions as a password, and the user must click in each one of the chosen regions, in the correct order, to later login. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans remember pictures better than they do text; psychological studies support such an assumption, and images are recalled better than words [10,11]. Also, it is more difficult to break graphical passwords using the traditional attack methods, like brute force search, dictionary attack, and spyware [12,13].

These days, there are diverse schemes for graphical passwords [14-21]. A graphical password scheme Passfaces shows many human faces and requires the user to choose four faces as a password [22]. Passfaces can display only a small number of faces on each screen and yields password with very low entropy. The company Passlogix [23] implemented a graphical password scheme that uses an image that has predefined click objects. The number of click regions in this scheme is larger than that in Passfaces

but is still not enough. Thus, a password must belong, to be secure. A graphical password scheme PassPoints allows any image to be used and does not require artificial predefined click regions with well-marked boundaries [21]. Hence, the password space of PassPoints is larger than those of the previous graphical password schemes. The password space is the set of all possible passwords for a given password scheme, for a given set of parameters.

However, all graphical password schemes have some inherent weaknesses. Weidenbeck et al. [21] describe it as follows.

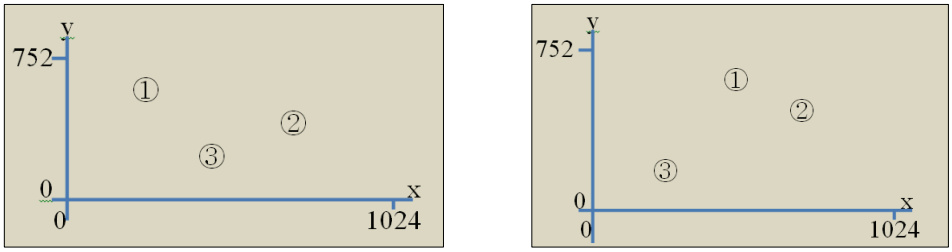
> "First, people with poor vision will have difficulties using graphical passwords. Second, people who have poor motor control and experience difficulties using pointing devices may not be able to use graphical passwords effectively. Third, people with various kinds of color blindness will see color differently. This may or may not affect their ability to use graphical passwords [21]."

A new graphical password scheme called PassPositions was recently introduced in [24]. PassPositions allows any image to be used and even works without any image. It is free from using images. Any image used in PassPositions is just a helpful item, not a necessary component of the scheme. Hence, PassPositions can avoid all the inherent weaknesses of the graphical schemes described above.

Graphical password schemes developed before PassPositions have used the absolute positions of click regions in a given image to construct a password. For the first time, PassPositions uses relative positions of the click regions, to construct a password [24]. With the relative positions, PassPositions brought many new advantages to the users. First of all, it is easy to construct a password in PassPositions. For handicapped persons and persons who have difficulties in pinpointing a small region in a graphical display, it was cumbersome to use graphical password schemes before PassPositions. PassPositions solves this problem. Secondly, like text-based passwords, most of the graphical passwords are vulnerable to shoulder surfing. PassPositions resists shoulder-surfing, by using different click regions for the same password at different times. Thirdly, compared to text-based passwords, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone, but this is not the case for PassPositions.

PassPositions-II is an improved version of PassPositions. PassPositions-II focuses on two aspects of "PassPositions": one is security, and the other is usability. From the security viewpoint, PassPositions can be improved, by expanding the password space. To find the relative position, PassPositions compares the position of the point just one-step before the current chosen point. So the first point's position is not used, when finding the relative position of the third chosen point, since the third point's position is compared only to the position of the second chosen point. PassPositions-II uses all the previous chosen points to find the relative position of the currently chosen point. Also, usability and reliability are improved in PassPositions-II, by allowing an area of tolerance [25]. PassPositions would recognize different sets of chosen points as the same password, regardless of whether the chosen points are in the same absolute location or not. This is because PassPositions can generate the same password (i.e., R-String) for different sets of chosen points. This characteristic of PassPositions can reduce the password space.

For example, PassPositions-II would recognize the two cases in Figs. 1 and 2 as different passwords, but PassPositions would not. PassPositions would generate the same R-String (RD, LD) for both Fig. 1(a) and 1(b), but PassPositions-II would generate the R-String (RD, LDLD) for Fig. 1(a), and R-String (RD, RDLD) for Fig. 1(b).



(a) (b)

Fig. 1. Three chosen points in PassPositions: (a) example 1 and (b) example 2.

PassSign is an efficient graphical password authentication system that employs a user's signature as a password. Unlike existing signature recognition systems, PassSign uses the relative position information (i.e., the information used for PassPositions) of the intersecting points in a signature [26]. Fig. 2 shows two signatures that are identified as different passwords by the PassSign system.

(a) (b)

Fig. 2. Two different password of PassSign [26]. (a) signature 1 and (b) signature 2.

PassSign has three main advantages. First, since the password is the user's signature, it is easy to remember and use. It is likewise difficult for others to steal. Also, PassSign is low-cost and easy to implement. Finally, the system can be efficiently installed and operated on mobile devices since PassSign is a light system.

T-TIME attempts authentication using only time information from graphical contact points, which are independent of the location of contact points on the device [27]. T-TIME has several steps to process the authentication as shown in Fig. 3.

The time difference is difficult to identify by observation. Applying T-TIME techniques in the PassPositions system makes it more resistant to shoulder-surfing attacks since an attacker would need to memorize both the touch locations and the time interval between them. Thus, T-TIME has a robust defense against shoulder-surfing attacks [27].

GTPass uses graphics and text simultaneously to utilize the advantages of graphical passwords and text-based passwords [28]. Images are used when registering their password, and numbers are used when logging in. Images are easier to memorize than text (including numbers) and numeric login provides a shorter login time than using image movement. It is an innovation that can solve many problems in existing password schemes.

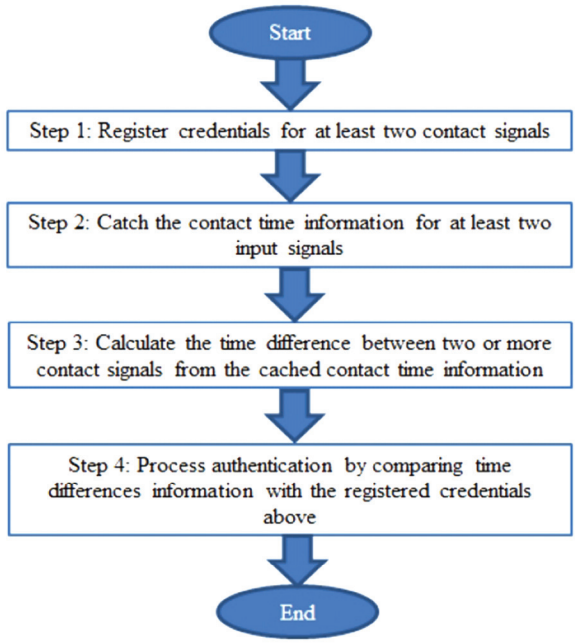
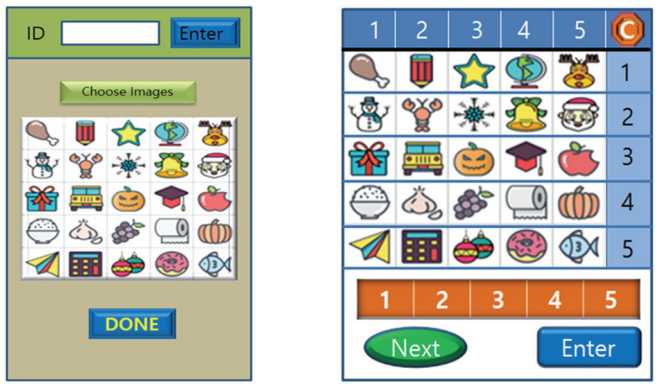


Fig. 3. Authentication processing steps of T-TIME. Adapted from [27].

The system interface of GTPass is shown in Fig. 4.

As we can see in Fig. 4, the user does not need to memorize the numbers. Images are the real password entities, but the numeric symbols are used to submit a password for login. This kind of password input scheme is the Transformed Input Scheme (TIS) of password input introduced in GTPass.



(a) (b)

Fig. 4. Interface of GTPass: (a) registering passwords and (b) log in.

It is generally difficult to compare different approaches because they vary in their selection of features. The wide range of previous approaches can be seen in the comprehensive survey by Biddle et al. [29] and there is a survey on graphical password systems developed in Korea [30]. Further complicating comparisons between different studies is the fact that authentication performance depends on the design and the method of experimentation used to evaluate usability. A universal set of test data does not exist to allow uniform comparisons of different schemes.

The ultimate goal should be to develop a graphical password authentication system that optimizes both security and usability. While the efforts to construct such an optimal graphical password authentication system are ongoing, the other approaches to achieve the ultimate goal of personal authentication are pursued. EEG was used for different purposes [31-34], but using the EEG signal can be one of other approaches to construct the ultimate personal authentication system and this paper introduces an EEG based personal authentication system with deep learning technique. Section 3 describes on EEG signals in some detail.

3. EEG Signals

Brainwave or EEG is a change in current due to the electrical current that flows when a signal is transmitted between neurons inside the brain. Investigations of the spontaneous electrical activity of the brain of an animal were reported before Hans Berger recorded the first human EEG in 1924. EEG related research was keep continued and scientists connected the brains of three people to experiment with the process of thought sharing recently [35]. Although medical use is one of the main applications of EEG, Recently, researches on the brain-computer interface have been actively conducted in various areas [7,8].

There are other methods such as positron emission tomography (PET), functional magnetic resonance imaging (fMRI), electrocorticography (ECoG), single-photon emission computed tomography (SPECT), and so on to study brain function. However, EEG possesses multiple advantages over some of these techniques despite the relatively poor spatial sensitivity of it; the advantages are on hardware costs, space-taking, temporal resolution, subject movement, exposure to radioligands, and so on including extremely un-invasiveness. While there are disadvantages such as the low spatial resolution on the scalp, difficult to identify specific locations in the brain, poorly measures neural activity that occurs lower layers of the brain (i.e., the cortex), and cumbersome to separate signal from noise.

The wavelength of the EEG from the human brain is a frequency of 0 to 30 Hz and has an amplitude of about 20 to 200 μV. The frequency range of the EEG is arbitrarily classified into a delta wave with a frequency of less than 4 Hz, a theta wave between 4 Hz and 7 Hz, an alpha wave between 8 Hz and 13 Hz, a beta wave between 13 Hz and 30 Hz, and above 30 Hz is called gamma wave. Example of alpha waves and beta waves are shown in Fig. 5.

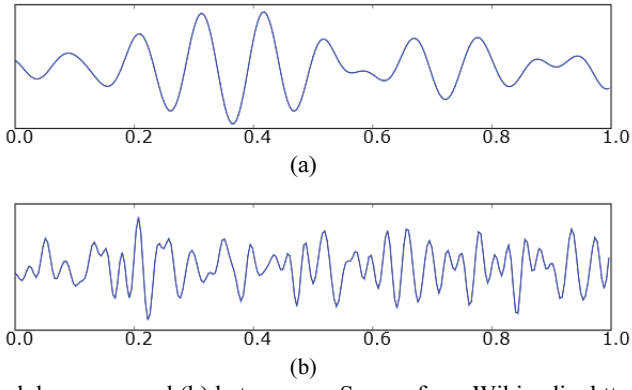


Fig. 5. Example of (a) alpha waves and (b) beta waves. Source from Wikipedia, http://en.wikipedia.org.

Alpha waves appear mainly in the occipital region and may extend to the parietal and posterior temporal lobes. posterior regions of the head, both sides, higher in amplitude on the dominant side. The alpha waves of the occipital lobe increase in amplitude when you close your eyes. It emerges with the closing of the eyes and with relaxation and attenuates with eye-opening or mental exertion. Beta waves occur primarily in the frontal lobe. Beta waves are mainly signaling in the frontal-central regions (both sides, symmetrical distribution, most evident frontally) with signals related to concentration. Beta waves activity is closely linked to motor behavior and is generally attenuated during active movements. Electromyogram (EMG) is similar in the frequency domain to the beta wave. Theta waves can appear in various areas of the brain. Theta wave occurring in the medial frontal cortex (found in locations not related to the task at hand) mainly during cognitive processing and increases with memory load. Theta waves measured at electrodes other than Fz or Pz are likely to consider as abnormal waves. Gamma waves are thought to be related to higher cognitive functions such as the integration of cognitions. Gamma waves are closely related to concentration and memory and are activated in the occipital lobe area (somatosensory cortex) when visual stimuli are meaningful.

A lot of research is currently being carried out for many purposes besides the conventional uses of clinical diagnosis and conventional cognitive neuroscience. Also, efforts are ongoing in order to make wearable EEG devices that are based upon creating low power wireless collection electronics and 'dry' electrodes which do not require a conductive gel to be used [36]. The characteristics of EEGs are described in Table 1.

Table 1. Characteristics of EEGs

EEG	Frequency domain (Hz)	Characteristics
Delta (δ) wave	0.2–3.99	Occurs when sleeping.
Theta (θ) wave	4–7.99	Occurs when falling asleep.
Alpha (α) wave	8–12.99	Occurs when you are stable.
SMR wave	12–15	Occurs when attention is focused. When the efficiency of work is optimal.
Beta (β) wave	13–30	Occurs when mental activity or nervous system is active. Occurs during activities such as anxiety and tension.
Gamma (γ) Wave	30 or higher	Occurs in extreme arousal and excitement.

4. EEG Based Machine Learning

The EEG password system should be able to measure a user's intention with a simple and inexpensive EEG device (i.e., dry EEG bioelectronic interfaces), so that a practical password system can be developed. Dry electrode signals depend upon mechanical contact. Therefore, it can be difficult getting a usable signal because of impedance between the skin and the electrode [37]. Therefore, analysis and classification of the accepted EEG signals are important to distinguish certain user's EEG signals among others. If we can distinguish each user's EEG signal correctly, we can use it as a password. The system proposed in this paper is working based on EEG signals and called PassEEG. PassEEG utilizes a deep learning technique to classify a user's EEG signal from others correctly.

PassEEG accepts EEG signals from a user and normalizes them to use it as personal information for authentication. After the normalization of the signal values, it needs to be classified. Different types of EEG signals shown in the previous section can be detected from a person, so multi-variable linear regression to classify a user by using multiple signals (e.g., alpha (α) wave, beta (β) wave, gamma (γ) wave) as input for a user. To design a multivariable linear regression, we need three things. Three things are hypothesis, cost function, and gradient descent algorithm. First, the hypothesis generates the predicted classified result, and the cost function evaluates the predicted classified result. Finally, gradient descent algorithm optimizes the cost.

For example, the hypothesis for 3-variable classification can be:

$$\mathrm{H}(x_1, x_2, x_3) = w_1 x_1 + w_2 x_2 + w_3 x_3 + b$$

Here, x_1, x_2, x_3 are the input variables and need to learn w_1, w_2, w_3, and b. In the case of n-variable classification the hypothesis for n-variables can be:

$$\mathrm{H}(x_1, x_2, x_3, \dots, x_n) = w_1 x_1 + w_2 x_2 + w_3 x_3 + \cdots + w_n x_n + b$$

The cost function for 3-variable classification can be:

$$cost(\mathrm{W}, \mathrm{b}) = \frac{1}{m}\sum_{I=1}^{m} (H\left({x_1}^{(i)}, {x_2}^{(i)}, {x_3}^{(i)}\right) - y^{(i)})^2$$

Here, $H\left({x_1}^{(i)}, {x_2}^{(i)}, {x_3}^{(i)}\right)$ is the predicted value generated by the hypothesis and $y^{(i)}$ is the true value we detected. We can get an optimized predicted value by minimizing predicted value through gradient descent algorithm. One problem here is that the predicted the value through the hypothesis can be any number and this problem can be solved by using a sigmoid function which is also called the logistic function. Multi-variable linear classification with logistic function is a logistic classification. Logistic classification can distinguish two groups, but it is not good enough for our purpose. Many users may use the personal authentication system PassEEG, so PassEEG should be able to distinguish one user among many users.

Therefore, we need to identify one user's EEG signal pattern out of many users' EEG signal patterns, so we need a multinomial classification. Multinomial classification can be implemented by using logistic regression. Logistic regressions use a logistic function shown below to confine the output value between 0 and 1.

$$f(x) = \frac{L}{1 + e^{-k(x - x_0)}}$$

where e is the natural logarithm base; x_0 is the x – the value of the sigmoid's midpoint; L is the curve's maximum value; and k is the logistic growth rate or steepness of the curve.

Logistic regression can separate two groups and we can separate many groups by using multiple logistic regressions. Hence, by using multiple logistic regressions we can perform a multinomial classification. Multiple logistic regressions can calculate easily by using matrix multiplication as an example below.

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \\ x_{41} & x_{42} & x_{43} \\ x_{51} & x_{52} & x_{53} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} x_{11}w_1 + x_{12}w_2 + x_{13}w_3 \\ x_{21}w_1 + x_{22}w_2 + x_{23}w_3 \\ x_{31}w_1 + x_{32}w_2 + x_{33}w_3 \\ x_{41}w_1 + x_{42}w_2 + x_{43}w_3 \\ x_{51}w_1 + x_{52}w_2 + x_{53}w_3 \end{pmatrix}$$

Multinomial classification can classify multiple categories as in Fig. 6.

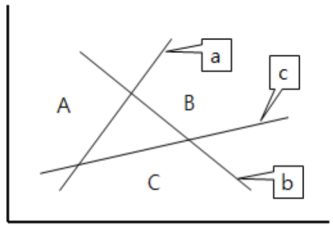


Fig. 6. Multinomial classification.

Category A is separated from other categories by line "a", and the line "b" separates category B from category A and C. Also, category C is separated from other categories by line "c". Each line is a logistic regression line. The output values of the logistic classifier for multinomial classification can be any score. These scores can be transferred into probabilities through the Softmax function. Specifically, in multinomial logistic regression and linear discriminant analysis, the input to the function is the result of ***K*** distinct linear functions, and the predicted probability for the *j*th class given a sample vector **x** and a weighting vector **w** is (from Wikipedia):

$$p(y = j|x) = \frac{e^{x^T w_j}}{\sum_{k=1}^{K} e^{x^T w_k}}$$

The cost function for the θ parameters can be defined as

$$J(\theta) = -\frac{1}{m}\left[\sum_{i=1}^{m} y^{(i)} \log h_\theta(x^{(i)}) + (1 - y^{(i)}) \log\left(1 - h_\theta(x^{(i)})\right)\right]$$

Use gradient descent by repeatedly update each parameter using a learning rate to minimize the logistic regression cost function.

$$\theta_j := \theta_j - \alpha \sum_{i=1}^{m} (h_\theta(x^{(i)}) - y^{(i)}) x_j{}^{(i)}$$

In the process of multinomial classification apply a one-hot encoding technique to select the final one category among many different categories. Next, store classified EEG signal values in the password storage along with the user ID to register a user's password. All the process for login is the same with the registration process but the last step. For login, the incoming classified EEG signals are compared with the signals stored in the password storage to identify a certain user. Fig. 7 is a brief diagram of the proposed system.

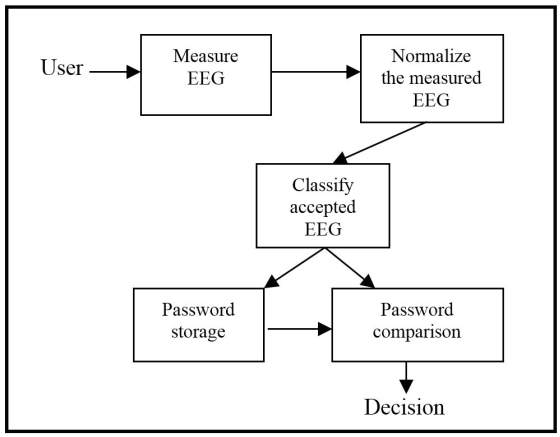


Fig. 7. System configuration of the proposed system.

The EEG-based password system is mainly divided into steps of generating and storing EEG signal values and classifying those values. To register the password, the user measures the EEG using the EEG device and classifies the measured signal according to a deep learning technique and stores it in the password database with the user ID. For password authentication, EEG is measured using an EEG device and classify an input password to compared with a password stored with the same ID to determine whether authenticate it or not.

The simple and easy registration and login process of PassEEG are described as follows.

Registration phase:

1) A user begins the creation of his/her profile by entering personal details and username.
2) Then, the user measures his/her EEG signal values using the EEG signal detection device.
3) Once the password is built, the registration phase is completed by the user.

Login phase:

1) First, the user enters their username.
2) The user measures his/her EEG signal values using the EEG signal detection device.
3) Login success once the current EEG signal values are the same as the stored EEG signal values of the user name.

The important point here is whether you can recognize the certain user's password. The EEG password system should be able to measure a user;s intention with a simple and inexpensive EEG device so that a practical password system can be constructed. In conventional scalp EEG, the recording is obtained by placing electrodes on the scalp with a conductive gel or paste. However, this kind of EEG recording scheme cannot be applied for general PassEEG. Currently, the dry EEG electrode is the best device for PassEEG. There are many advantages of dry electrodes such as no skin preparation, no electrolyte used, significantly reduced sensor size, and compatibility with EEG monitoring systems. But one big problem to use dry EEG electrode is low resolution. Fig. 8 shows an interface device for detecting EEG signals with dry electrodes.

Therefore, to guarantee reliable EEG measurement, we propose to use an incremental password stacking method to accept newly classified EEG password without making any conflict with existing

passwords. Among the deep learning technique, we recommend the multinomial classification with a one-hot encoding technique to accurately recognize a user's brain password.

Fig. 8. Dry EEG bioelectronic interface.

5. Conclusion

Digital security is one of the most significant social problems in our digital society. Among many different types of digital security areas, personal authentication is the area we are the most concerned. In current information society, individuals generally have multiple accounts and use digital devices. Personal authentication can play a significant role to keep our digital security. Hence we need better authentication schemes than the current password scheme. The most general mechanism of personal authentication today is the password system using an alphanumeric password.

Graphical password system is one of the alternatives that can replace the current alphanumeric password system. Graphics are better than text to remember, so easy to maintain multiple graphical passwords for different accounts. However, because of the easiness of remembrance makes the graphical password vulnerable to shoulder surfing attacks.

This paper proposed an EEG-based password system as a next-generation personal authentication system. EEG-based personal authentication system makes it difficult for an unauthorized person to steal a user's password by hiding the password input process to others. But it was unreliable to use in reality due to the limitation of current brain-computer interface technology. Dry electrodes should be used to build a practical EEG-based authentication system. However, the technical limitations of current brainwave signal interpretation using dry electrodes are an obstacle to produce a realistic EEG-based password system.

To overcome this problem, this paper proposed an EEG-based password system (i.e., PassEEG) that uses not only EEG signals but also a deep learning techniques. The proposed deep learning technique is a multinomial classification with one-hot encoding. Using EEG signals and deep learning technique together is a good combination that creates a very efficient and useful tool for grasping user's intention transparently. This paper focused on the idea of a new way of personal authentication. The experimental result will show in the next paper. The proposed solution indeed has a validation delay when compared with the other authentication approaches; however, the proposed system can be used in special environments (e.g., military system) at the moment before BCI technology is mature. This research result will provide an efficient way to build a practical personal authentication system based on the EEG signal. Also, this result can be used for various other applications and enhance the method of utilizing EEG signals.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) and funded by the Ministry of Education, Science, and Technology (No. 2017R1D1A1B04032968).

References

[1] Wikipedia, "Authentication," [Online]. Available: https://en.wikipedia.org/wiki/Authentication.

[2] H. Berger, "Uber das electrenkephalogramm des menschen," *Archiv fur Psychiatrie und Nervenkrankheiten,* vol. 87, no. 1, pp. 527-570, 1929.

[3] T. A. Travis, C. Y. Kondo, and J. R. Knott, "Alpha enhancement research: a review," *Biological Psychiatry*, vol. 10, no. 1, pp. 69-89, 1975.

[4] B. Rockstroh, T. Elbert, A. Canavan, W. Lutzenberger, and N. Birbaumer, *Slow Cortical Potentials and Behavior*, 2nd ed. Baltimore, MD: Urban & Schwarzenberg, 1989.

[5] M. B. Sterman, "Basic concepts and clinical findings in the treatment of seizure disorders with EEG operant conditioning," *Clinical Electroencephalography*, vol. 31, no. 1, pp. 45-55, 2000.

[6] H. J. Hwang, S. Kim, S. Choi, and C. H. Im, EEG-based brain-computer interfaces: a thorough literature survey, *International Journal of Human–Computer Interaction*, vol. 29, no. 12, pp. 814-826, 2013.

[7] H. J. Hwang, J. H. Lim, Y. J. Jung, H. Choi, S. W. Lee, and C. H. Im, "Development of an SSVEP-based BCI spelling system adopting a QWERTY-style LED keyboard," *Journal of Neuroscience Methods*, vol. 208, no. 1, pp. 59-65, 2012.

[8] I. Volosyak, "SSVEP-based Bremen-BCI interface--boosting information transfer rates," *Journal of Neural Engineering*, vol. 8, no. 3, 036020, 2011.

[9] G. Blonder, "Graphical passwords," U.S. Patent 5559961, Sep 24, 1996.

[10] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, no. 1, pp. 156-163, 1967.

[11] A. Paivio, T. B. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?," *Psychonomic Science,* vol. 11, no. 4, pp. 137-138, 1976.

[12] A. E. Dirik, N. Memon, and J. C. Birget, "Modeling user choice in the PassPoints graphical password scheme," in *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, 2007, pp. 20-28.

[13] D. Hong, S. Man, B. Hawes, and M. Mathews, "A graphical password scheme strongly resistant to spyware," in *Proceedings of the International Conference on Security and Management (SAM)*, Las Vegas, NV, 2004, pp. 94-100.

[14] R. Dhamija and A. Perrig, "Deja vu: a user study using images for authentication," in *Proceedings of the 9th USENIX Security Symposium*, Denver, CO, 2000, pp. 45-58.

[15] A. Perrig and D. Song, "Hash visualization: a new technique to improve real-world security," in *Proceedings of International Workshop on Cryptographic Techniques and E-Commerce*, Hong Kong, China, 1999, pp. 131-138.

[16] S. Akula and V. Devisetty, "Image based registration and authentication system," in *Proceedings of Midwest Instruction and Computing Symposium*, Morris, MN, 2004.

[17] D. Weinshall and S. Kirkpatrick, "Passwords you'll never forget, but can't recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*, Vienna, Austria, 2004, pp. 1399-1402.

[18] W. Jansen, "Authenticating mobile device users through image selection," in *The Internet Society: Advances in Learning, Commerce and Security*. Southampton, UK: WIT Press, 2004, pp. 184-192

[19] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proceedings of the 8th USENIX Security Symposium*, Washington, DC, 1999.

[20] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in *Information Security and Privacy*. Berlin: Springer, 1998, pp. 403-414.

[21] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies*, vol. 63, no. 1-2, pp. 102-127, 2005.

[22] S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? A field trial investigation," in *People and Computers XIV - Usability or Else*. London, UK: Springer, 2000, pp. 405-424.

[23] M. Boroditsky, "Passlogix password schemes," 2002 [Online]. Available: http://www.passlogix.com.

[24] G. C. Yang, "PassPositions: a secure and user-friendly graphical password scheme," in *Proceedings of 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, 2017, pp. 1-5.

[25] G. C. Yang and H. Oh, "Implementation of a graphical password authentication system 'PassPositions'," *Journal of Image and Graphics*, vol. 6, no. 2. pp. 117-121, 2018.

[26] G. C. Yang, "A new graphical password system using intersecting points in a signature," *International Journal of Engineering & Technology*, vol. 7, no. 4.39, pp. 61-64, 2018.

[27] G. C. Yang, "T-TIME: a password scheme based on touch signal generation time difference," *Journal of Advanced Information Technology and Convergence,* vol. 8, no. 2, pp.41-46, 2018.

[28] G. C. Yang, "A multimodal password system based on graphics and text," *Engineering Letters*, vol. 28, no. 2, pp. 300-305, 2020.

[29] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: learning from the first twelve years," *ACM Computing Surveys (CSSUR),* vol. 44, no. 4, article no. 19, 2012.

[30] G. C. Yang, "Development status and prospects of graphical password authentication system in Korea," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 11, pp. 5755-5772, 2019.

[31] T. M. Li, H. C. Chao, and J. Zhang, "Emotion classification based on brain wave: a survey," *Human-centric Computing and Information Sciences,* vol. 9, Article no. 42, 2019.

[32] N. H. Keum, T. Lee, J. B. Lee, and H. P. "Measuring the degree of content immersion in a non-experimental environment using a portable EEG device," *Journal of Information Processing Systems*, vol. 14, no. 4, pp. 1049-1061, 2018.

[33] T. Pedersen, C. Johansen, and A. Josang, "Behavioural computer science: an agenda for combining modelling of human and system behaviours," *Human-centric Computing and Information Sciences,* vol. 8, article no. 7, 2018.

[34] V. Suryani, S. Sulistyo, and W. Widyawan, "Two-phase security protection for the internet of things object," *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1431-1437, 2018.

[35] D. Nield, "Scientists have connected the brains of 3 people, enabling them to share thoughts," 2018 [Online]. Available: https://www.sciencealert.com/brain-to-brain-mind-connection-lets-three-people-share-thoughts.

[36] A. J. Casson, D. C. Yates, S. J. M. Smith, J. S. Duncan, and E. Rodriguez-Villegas, "Wearable electro-encephalography," *IEEE Engineering in Medicine and Biology Magazine*, vol. 29, no. 3, pp. 44-56, 2010.

[37] F. Wang, G. Li, J. Chen, Y. Duan, and D. Zhang, "Novel semi-dry electrodes for brain-computer interface applications," *Journal of Neural Engineering,* vol. 13, no. 4, article no. 046021, 2016.

Gi-Chul Yang **https://orcid.org/0000-0003-0929-3818**

He received his M.S. degree from the Department of Computer Science, the University of Iowa, USA in 1986 and Ph.D. degree in Computer Science and Telecommunications Program from the University of Missouri, USA in 1993. Currently, he is a Professor at Mokpo National University, where he has been working since September 1993. He was also a Director of Information & Computing Institute, School of Information Engineering and University Library at Mokpo National University. His research interests include artificial intelligence (AI) and human computer interaction (HCI). He was a Visiting Scholar at Heriot-Watt University and the University of Hamburg in 2002 and 2015, respectively. He collaborated with professors at Linkoping University, University of Zurich, University of Missouri, University of Auckland, and Drexel University. He is an author of several books (written in Korean) and was an editor of Springer's Transactions of Engineering Technologies.