A Graphical Authentication System Controlled by Eye Movement

Zhanheng Li, Chenwei Xi, and Qiang Zhang and Xiujuan Zheng*
(College of Electrical Engineer and Information Technology, Sichuan University, Chengdu 610065, China)

Email: xiujuanzheng@scu.edu.cn

Abstract. Graphical password is a potential alternative to the traditional alphanumerical password due to its advantages of recognition and memory in the security system. Eye movement, a natural interaction modality, is a promising tool to replace the keyboard and the mouse in authentication. This paper proposes a graphical authentication system controlled by eye movement. In this keyboard-less authentication system, the user’s eye movements were recorded by eye-tracker as the control signal to generate recognition-based graphical passwords. The user test study has been conducted to verify the availability and effectiveness of this keyboard-less graphical authentication system. It’s also shown that the efficiency could be improved as the user getting familiar with this system.

1. Introduction

Human is often considered as the weakest link in a computer security system. Many security problems often derived from bad interactions between humans and systems. For human, the pictures are generally easier to recognize and remember than text [1] regardless the race, cultural, and educational backgrounds. In recent years, graphical password has been proposed as a potential alternative to the traditional alpha-numerical password for promoting more memorable passwords against guessing [2-3]. If the possible pictures used in graphical password system is sufficiently large, it will has the advantage for preventing knowledge-based guess and exhaustive search. Furthermore, if the password space can be customized by the users, a great contribution can be provided for the enhancing the password strength. Thus, it seems that the graphical passwords could has a better resistance to brute-force and dictionary attacks than text-based passwords. In light of these advantages, graphical password has been attracted more and more attentions in various authentication applications including workstation, web log-in systems, mobile devices as well as ATM machines [2]. However, the more pictures or details used for generating the graphical password, the larger image interfaces are required.

Eye movement is a natural human-computer interaction modality [5]. By using eye tracking technology, eye movement can be collected and analyzed to obtain the eye’s behavioral and attentional features. The eye’s behavioral features, such as fixation and saccades, were usually utilized in real time human-computer interaction. The eye movement can be treated as a directly control tool in the interaction. This technique has been used as a non-touchable mouse pointer for disables [6]. Eye movement is collected by an eye tracker and the eye’s features are hard to directly extract by human
observers. So that, eye movement is exactly suitable for using in authentication systems because of it high resistance to the shoulder surfing attacks.

Eye tracking technology has been explored to collect and measure eye movements precisely and conveniently. It could provide a new interaction mechanism to strengthen the existing graphical password schemes. Some researchers made attempts to develop eye-movement based graphical password systems by combining the advantages of graphical and eye movement together. Maeder et al. [7] and Hoanca et al. [8] has both proposed graphical password systems based on user’s gaze. Moreover, Dunphy et al. [9] implemented Passfaces (http://www.realuser.com) equipped by eye tracking to a real ATM password system.

This paper aimed to propose a graphical authentication system controlled by eye movement. In this authentication system, the merits of eye movement were fully utilized and integrated with a recognition-based graphical password scheme. Furthermore, the availability and effectiveness of this system was validated by a user test study.

2. Method

In this paper, the keyboard-less graphical authentication system was designed with eye tracker. Thus, the eye tracking technology and the design of graphical authentication system would be respectively introduced in this part.

2.1. Eye Tracking Technology

Eye tracking technology has been developed to study of the mechanisms and dynamics of eye rotation and used in researches on psychology, psycholinguistics, human factors engineering, et al. However, the goal of eye tracking is most often to estimate gaze direction. This could promote the application of eye tracking technology in the field of human-computer interaction. The video-based eye tracker, such as the solutions form Tobii Technology AB, is the most widely used current design that is commonly used cameras to focus eyes and record their movements. When using video-based eye tracking technique, the center of the pupil and infrared/near-infrared non-collimated light can be implemented to create corneal reflections. The vector between the pupil center and the corneal reflections can be used to compute the point of regard on surface or the gaze direction. Before using the eye tracker, a calibration of the individual user is required [10].

For the features of eye movement, fixation is the eye movement to stabilize the retina over a stationary object of area of interest. Saccades are the discrete movements that quickly change the orientation of the eyes. Fixation shows the static characteristics of the human vision system, while saccades reflect the dynamic characteristics. The fixation-based (sometimes named as “gaze-based”) interaction and saccades-based interaction are two available modalities for human-computer interactions using eye tracking technology [5]. The fixation-based interaction was adopted for the design of graphical authentication system in this paper.

2.2. Graphical Authentication System

The graphical authentication system was designed based on graphical password mechanism equipped with eye tracking technology. A set of single-object pictures was used to generate the personal identification images (PIIs) of the graphical password. The recognition-based technique was used for authentication. The user was required to recognize and identify their preselected PIIs in the registration stages in order to be authenticated. In the porotype, there were 24 single-object images shown in the interface by 4×6 or 5×5 tiles (as shown in Fig. 1), in order to avoid large image interface and reduce the risk of shoulder surfing attacks. These pictures would be randomly sorted for each 5 seconds. The time interval was defined as a refresh frame. While using eye tracking, the user is asked to fixate on the prescribed pictures among the decoy ones for authentication. In this process, the user’s fixation were extracted and utilized as a pointing device, like a mouse, by using Tobii EyeX controller (Tobii Technology AB). The fixation used in this study was defined as the total duration and the average location of a series of fixations within the one picture. By fixating eyes for at least 4 seconds
at a certain picture, the user can activate the command for selecting this picture as a PII of graphical password. This process can be repeated for several refresh frames (usually 2~10 frames) until the system determined the picture selected by the user. An example is given in Fig. 2.

![Figure 1](image1.png)

**Figure 1.** The prototype of the graphical authentication system. (A) the interface for inputting passwords in registration stage; (B) the interface for inputting passwords in login stage.

![Figure 2](image2.png)

**Figure 2.** An example plot of extracted fixations for inputting one password in two refresh frames. (A) the first 5 second fresh frame; (B) the following 10 second fresh frame; (C) The selected personal identification image (spider).

To ensure the integrity of the authentication system, there are three main stages in the proposed graphical authentication system: registration, login and password reset. The user can created their own accounts through the stage of registration. The username and password can be both generated by
inputting PIIs via the interface shown in Fig. 1 (A). These information were then transformed into encrypted information and stored in a database. The graphical password can be rest in the stage of password reset. The framework of this system was developed using Microsoft Visual Studio 2012 and Access 2013.

2.3. User Test Study
The user test study has been conducted to verify the availability and effectiveness of the proposed graphical authentication system. Total six participants, 3 male and 3 female, were recruited for the test study. The ages of the participants ranged from 20 to 24 with an average of 22.5 years. Three of the participants had normal vision and the rest participants had corrected normal vision by wearing the glasses. All of the participants were experienced computer users. None of them had any previous experience with eye-tracking based graphical authentication.

The participant tested all three stages of authentication individually and repeated for five times. For the 5 trails, the participants were asked for performing every trail with an interval of ten minutes and completing whole test within 2 hours. In each trail, the participant sequentially tested the stages of registration, login and password reset. For equal comparisons, the lengths of username were both set as 2. That is, there were only two PIIs in one username or one graphical password. The time spent in every stage was recorded for each trail and each participant. Meanwhile, the error input of PII at login stage were also recorded for each participant.

Finally, the participants were ask for answering a questionnaire about the usability of graphical authentication system.

3. Results
The setup of the proposed graphical authentication system is demonstrated in Fig. 3. The Tobii EyeX controller was mounted at the bottom of a 21-inch monitor and connected with a computer (i7-4790 3.6GHz, 4G RAM) through USB3.0. The participant sat in front of the screen with his/her comfortable position. If needed, the participant can wear the glasses to have normal vision.

![Figure 3](http://www.tobii.com/)

Figure 3. The demonstration for the setup of the proposed graphical authentication system. (A) the installation of Tobii EyeX Controller in this study; (B) the position of the participant (reproduced from http://www.tobii.com/).

After given a brief introduction of the graphical authentication system, the participant began with a calibration for using Tobii EyeX controller, and then completed the three stages of registration, login and password reset. At the stage of registration, the participant generated a graphical username corresponding with a graphical password. The information of account was encrypted and saved in a
database. The process of registration is illuminated in Fig. 4. The process of password reset is similar with registration.

![Registration Process Image](image)

**Figure 4.** An illumination of the stage of registration.

The average time spent on every stage is calculated and illuminated in Table 1. The results show that the total time to complete one whole trail ranged from 145 to 180 seconds, and about 50% time was spent on the password reset stage. The login stage, which is most frequently used in authentication system, consumed the least time compared with the other two stages.

| participants | registration | login | password reset | total       |
|--------------|--------------|-------|----------------|-------------|
| P1           | 50.6 ± 5.3   | 28.0 ± 3.2 | 86.4 ± 6.3     | 165.0 ± 10.9 |
| P2           | 51.8 ± 4.1   | 29.6 ± 3.1 | 91.6 ± 6.6     | 173.0 ± 11.9 |
| P3           | 47.0 ± 4.4   | 24.2 ± 2.0 | 84.2 ± 3.4     | 155.4 ± 9.4  |
| P4           | 51.8 ± 4.0   | 28.8 ± 4.0 | 87.4 ± 6.2     | 168.0 ± 13.6 |
| P5           | 50.4 ± 4.0   | 25.0 ± 2.8 | 86.8 ± 5.3     | 162.2 ± 11.7 |
| P6           | 48.0 ± 3.7   | 24.6 ± 2.9 | 86.4 ± 5.5     | 159.0 ± 11.6 |

*The unit is second.

The time spent on every stages were recorded and compared for the five trails for all participants. The results are illuminated in Fig. 5. From Fig. 5 (A)–(D), the apparent declines of the time spent on authentication could be observed with fluctuant standard deviations. The tendencies reflected by the results shows that all the participants spent more time for the first use no matter in which stage. The time would be decreased when the participants getting familiar with the authentication system. It could indicate that the length of time spent for each stage was highly correlated with the user’s experience of the graphical authentication system. Among five trails, one participant had two errors for PII inputting while two participants had one error. The rest three participants had no error during login. It is generally required additional time to remove and fix the error PIIIs, so that the time spent on the same stage would have a large standard deviation due to the errors. This is a reasonable explanation for the fluctuant standard deviations of the login time in Fig. 5 (B).
Figure 5. The changes of the average time spent on every stage of authentication. The standard deviations are given by error bars. (A) time spent on registration stage; (B) time spent on login stage; (C) time spent on password reset stage; (D) the total time for authentication.

All of the participants succeeded in the authentication using eye tracking. From the questionnaire, all the participants pointed out that the eye movement based approaches required more operating time than click based approaches. Most of them showed the interests in this system and gave a positive affirmation of the usability. All participants expressed a willingness to use the graphical authentication system based on eye tracking in the future. However, the user test were still limited to give a comprehensive evaluation for the proposed authentication system. In the future work, the strategies of PII determination based on the fixations at the refresh frames could be further explored to improve the efficiency and usability of the proposed authentication system.

4. Conclusions
A prototype of the graphical authentication system controlled by eye movement has been developed and tested by 6 users. The results of user test study have validated the availability and effectiveness of the proposed graphical authentication system. The operating time would be decreased, when the users were getting familiar with the system especially the use of eye tracker. In a conclusion, this paper has proposed a potential solution for the shoulder-surfing resistant authentication system with keyboard-less real-time interactions.

5. Acknowledgment
The author would like to acknowledge an insightful discussion regarding eye tracking technology with Dr. Yun Zhang at the Eye Tracking Lab, Electronic Information and Engineering School, Xi’an Jiaotong University, China.

References
[1] R. N. Shepard, ‘Recognition memory for words, sentences, and pictures’, Journal of Verbal Learning and Verbal Behavior, 6: 156-163, 1967.
[2] X. Suo, Y. Zhu and G.S. Owen, “Graphical Passwords: A Survey”, 21st Annual Computer Security Applications Conference (ACSAC’05), Tucson, AZ, 2005, pp.463-472.
[3] K.V. Renaud, “Guidelines for designing graphical authentication mechanism interfaces”. Int. J. Inf. Comput. Secur., 3(1):60-85, 2009.
[4] D. Hong, S. Man, B. Hawes, and M. Mathews, “A password scheme strongly resistant to spyware,” Proceeding of International conference on security and management. Las Vegas, NV, 2004.

[5] Y. Zhang, X. Mou, “Survey on Eye Movement based Authentication Systems”, Proceeding of Chinese Conference on Computer Vision 2015, Xi'an China, Spet 2015, pp. 144-159.

[6] A. T. Duchowski, Eye Tracking Methodology: Theory and Practice. Secaucus, NJ, USA: Springer-Verlag New York, Inc, 2003, pp. 319.

[7] A. J. Maeder, C. B. Fookes, and S. Sridharan, “Gaze based user authentication for personal computer applications”, Proceedings of International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004. October 20-22, 2004, Hong Kong.

[8] B. Hoanca and K. Mock. Secure graphical password system for high traffic public areas. In ETRA '06: Proceedings of the 2006 symposium on Eye tracking research & applications, San Diego, California, Anonymous ACM, New York, NY, USA, 35-35.

[9] P. Dunphy, a. Fitch and P. Oliver, P. 2008. Gaze-Contingent Passwords at the ATM. In Prague, Czech Republic, September 2-3, pp, 50-62.

[10] D. W. Hansen, Q. Ji, “In the Eye of the Beholder: A Survey of Models for Eyes and Gaze”. IEEE Trans. Pattern Anal. Mach. Intell. 32 (3): 478–500, 2010.