SHOULDER SURFING RESISTANT TEXT BASED GRAPHICAL PASSWORD SCHEMES USING COLOR

Nurul Kholisatul Ulya[1], Lukito Edi Nugroho[2], Dani Adhipta[3]

Universitas Gadjah Mada, Department of Electrical Engineering and Information Technology
Grafika Street 2, Yogyakarta 55281 Indonesia

lisaulya@gmail.com[1], lukito@ugm.ac.id[2], dani@ugm.ac.id[3]

Abstract

Password is important information to access or enter a system. Alphanumeric is a text-based password system that is commonly used. Unfortunately, many users make a weak password that is easy to guess and vulnerable to various attacks such as brute-force, dictionary attack, guessing attack and others. To create a strong password is suggested to have a lot of variety and long, but it will be difficult to remember by the user. Graphical password is an alternative method that gives usability for the user. Based on psychological research, people are generally easy to remember or recognize an images, shapes and colors rather than text. This reinforces the researchers to develop this method. The main problem of graphical password is vulnerable to shoulder surfing. In this paper will be proposed scheme as graphical password text based that are resistant to shoulder surfing attacks using color.

Keywords: graphical password, shoulder surfing resistant, text, color

Presenting Author's biography

Nurul Kholisatul Ulya. She received computer's degree in Informatic Enginering from University of Muhammadiyah Surakarta in 2012. Now she is a student master's degree of Department Electric Enginering and Information Technology from Gadjah Mada University. Her research interests in computer networking and computer security.

1. Introduction

Authentication is an important topic in information security to protect user's privacy. There are various authentication schemes developed by researchers. Alphanumerical password is the most common method for user authentication. The password must be easy to remember and should be secure [1]. However, alphanumerical password also has its problems; it is vulnerable to shoulder surfing password, have low entropy that makes them susceptible to dictionary attack, in some cases they are often too difficult to remember, and the user tends to set a weak password such as username, full name or birth date[2][3] [4][5]. Because this limitation of the traditional authentication, alternative solutions, such as biometric, have been used. In this paper, we will focus on another alternative option by using picture as a password.

Graphical password have been proposed as a possible alternative to text- based schemes, motivated by the fact that humans can recognize pictures better than text. Psychological studies support this assumption. Generally, pictures are easier to be remembered than text, the graphical password may have big password space; thus, this will be better resistant to dictionary attacks. Despite these advantages, there is a growing interest in graphical password [2][5]. Graphical password techniques can be classified into two categories, recognition based and recall based. In recognition-based, during registration phase a user selects of images as a password, and successful authentication is required to identify and recognize the previously selected images. Recall-based is categorized into two, pure recall-based and cued recall-based. The pure recall require user to reproduce something that he or she created during registration. In cued recall-base, user is provided with some hint to assist in recalling the previously generated password selected. The recognition is easier cognitive than recall.[6]

Shoulder surfing is the main drawback of graphical password. Shoulder surfing is a direct observation technique, such as looking over someone's shoulder to get password, PINs and other sensitive personal information. A number of graphical password solutions have been created but they offer little security against of shoulder surfing attacks. The researchers developed some hybrid schemes based on graphic and text. The main objective of this scheme is to achieve higher security with compromising user-friendliness and procure a considerable improvement in terms of system security [3][7][8].

2. Related Work

Shoulder surfing is the most vulnerable to graphical password. It is simply looking over someone's shoulder to get any useful data and information. Subrado and Birget[1] developed shoulder surfing resistant to the triangle, in this scheme user has to choose and remember passicons as a password. When logging in, user must to find three passicons displayed on the login screen and then click inside the invisible triangle created. To give high security and usability, convex hull click scheme is proposed as an improved version of triangle scheme. This scheme allows user to prove knowledge of the graphical password safely in an insecure location because user never need to click directly on their password. Haichang Gao et al [5] has proposed Color login. It is implemented in an interesting game way to decrease boring feeling of graphical authentication. This scheme is resistant to shoulder surfing attack but the required space is smaller than text-based password.

Most users are familiar with traditional textual password authentication scheme. Zao et al proposed a Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS)[9]. In this scheme, user has to find the textual password in invisible triangle area to get session password. D. Surya Devi et al [10] improved the pair-based by using text and color. To get session password, user must enter the intersection from row and column of his or her secret password. Yi-Lun Chen et al [11] proposed a simple text-based shoulder surfing resistant. During registration, user have to choose on color from 8 color assigned by the system. The system displays a circle composed of eight equally-sized sectors. Wei-Chi Ku et al [12] proposed the chameleon, which uses shape, text, and color to make a password. This scheme offers high security and to enhance usability, the researcher uses QWERTY keyboard.

3. The Proposed Scheme

Textual password is the most common method for authentication. However, it is vulnerable to many attack like dictionary attack, guessing attacks, and shoulder surfing. Graphical passwords have been introduced as an alternative to textual password even though this technique is vulnerable to shoulder surfing. To address this problem, a design has been created wherein text can be combined with pictures or color.

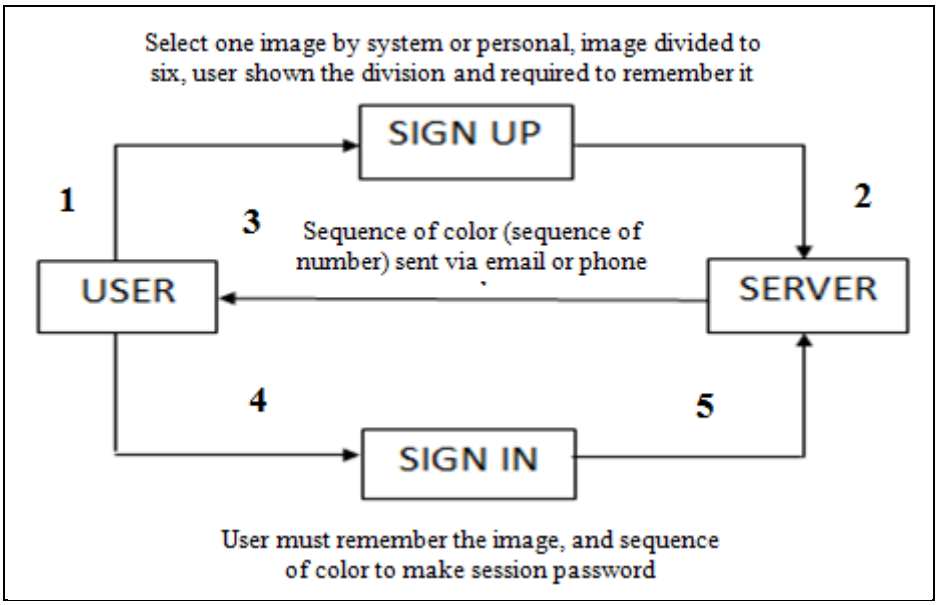

Fig 1. Architecture of Registration and Authentication

In this system, the text is created by using session passwords, which will be displayed on the randomized color grid containing uppercase, lowercase, numbers, and symbols arranged like QWERTY keyboard. This is development of [12] schemes, it is using mouse for its input. Based on [2], the keyboard input is better to prevent shoulder surfing; therefore, this proposed scheme will be developed by using keyboard input.

How the scheme works

The system is recognition-based graphical password. The operational framework of the design process will be discussed in two different phases:

1. Registration (Sign Up)

   In this stage, user types his or her user ID. Then he or she must choose one image (can be from system or personal). The image will be divided into six images, and the user will be shown the result of the division. After registration, the user will get the sequence of passcolor from number telephone or email. This will help to make the session password. This will be explained in Fig. 2.

2. Authentication (Sign In)

   The user enters user ID. Furthermore, the user must remember the image part of the image that has been selected. Password consists of 8 characters. The eight characters are divided into two parts, the four characters at the beginning and at the end that have the same color sequence. Four characters consist of three sequence characters passcolor and one character of non-passcolor or detractors color. The detractors color is raised from the position and color of the selected image. This will be shown in Fig. 1. For example, the image in position 3rd and the color is red. So, the detractors are in third place by selecting characters on the red grid.

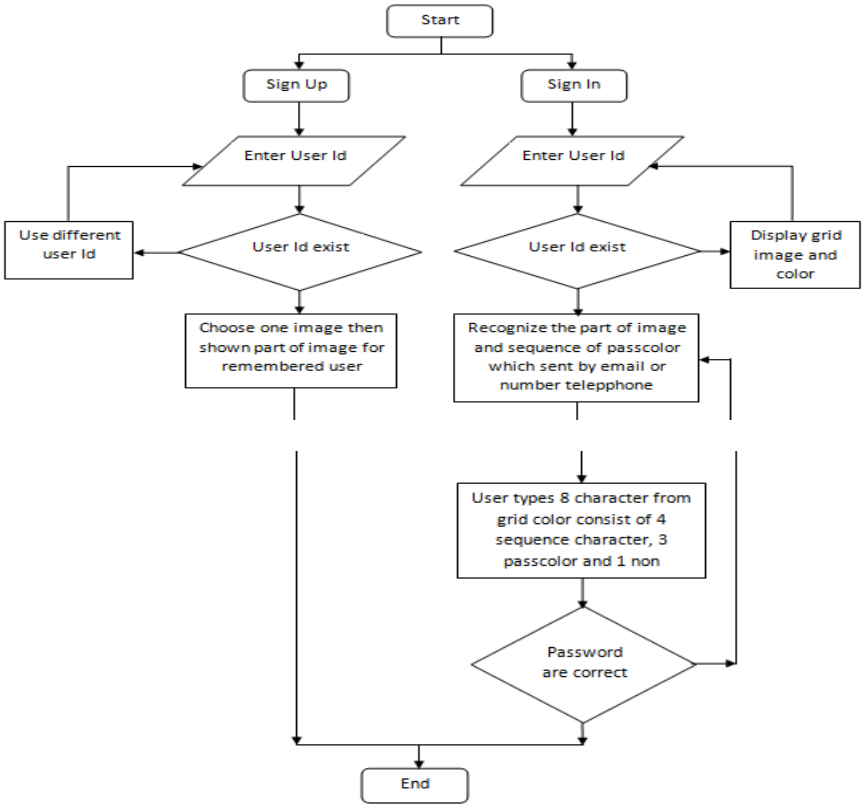

Fig 2. Flowchart of Registration and Aunthentication

The systems use both graphical password and text password. The use of text is to eliminate the problem of shoulder surfing 1]. In addition, it is beneficial to keep the image password. Each login, the part of image will be randomized so that it will be different every login. Login screen is divided into two, there are part of image with abbreviation of colors and QWERTY keyboard characters to make session password. Firstly, part of image is taken from one image that is selected previously. Before dividing it into six parts, the image is changed to grey for the prevention of social engineering by verbal communication. The six parts of images are randomized on every login. The means of R, G, B, and so on are abbreviation of colors like R for Red, G for Green, B for Blue, and so forth. Secondly, QWERTY keyboard characters consist of 26 uppercase, 26 lowercase, 10 digit, and 28 symbol.

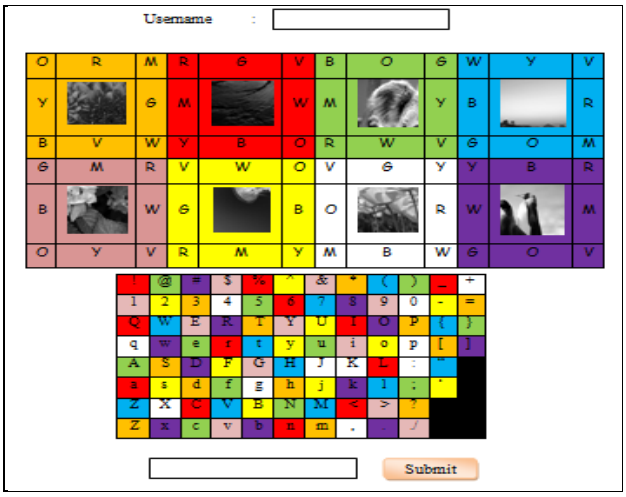

Fig 3. An example of login screen

4. Analysis

Password Space

System security generally depends on having sufficiently large password space. Password security is usually measured by the size of password space. The total number of all possible passwords with length L is 90^L . There for the password space of the proposed scheme is shown in Eq.(1)

$$\sum_{L=8}^{16} 90 \hat{} L \approx 1{,}85x10^{31} \quad (1)$$

Resistant of attacks

Shoulder surfing: the technique is resistant to shoulder surfing because the text password can be changed on every login.

Dictionary attack: in this attack, an attacker uses a set of dictionary word and authenticates it by trying one word after another. This will be difficult because the password can be changed every time.

Social engineering: this attack uses the weak side of human, which will be requested any information about password. Graphical password information to attacker would be difficult to detect the real picture, because instead of the original image, only part of that image will be displayed.

Guessing attack: many users tent to select the password based on their personal information . in this attack, the attacker will tries to guess the password by trying the main password possibilities. The possibility of breaking password is small, because use session password. In addition, the detractors on display graphical password and writing the text password is unpredictable.

Usability

The character like QWERTY keyboard is familiar to most users. In addition, the users does not need much memory because they are required to remember part of one selected image on registration and sequence of color to make session password.

5. Conclusion and Future work

Graphical Password is more secure and can be remembered or recalled easily. The recognition based graphical password is good in memorability that will allow users to remember and recognize the passwords successfully. The main drawback of graphical password is its vulnerability to shoulder surfing. In this paper, the method combined the image and color to arise usability of authentication. The operation of the system is easy for users who are familiar with textual password and QWERTY keyboard. The design provides high security and usability for user. This design is in its early stage and need to be explored and analyzed further with the real user.

References

[1] and J. . B. S. Wiedenbeck, J. Waters, L.Sobrado, "Design and evaluation of a shoulder surfing resistant graphical password scheme," *Proceding Work. Conf. Adv. Vis. Interfaces*, pp. 177–184, 2006.

[2] F. Tari, a Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," *Proc. Second Symp. …*, p. 56, 2006.

[3] A. H. Lashkari, S. Farmand, D. O. Bin Zakaria, and D. R. Saleh, "Shoulder Surfing attack in graphical password authentication," vol. 6, no. 2, p. 10, 2009.

[4] N. S. Joshi, "Session Passwords Using Grids and Colors for Web Applications and PDA," vol. 3, no. 5, pp. 248–253, 2013.

[5] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," *2009 4th Int. Conf. Innov. Comput. Inf. Control. ICICIC 2009*, pp. 675–678, 2009.

[6] M. R. Albayati and A. H. Lashkari, "A New Graphical Password Based on Decoy Image Portions (GP-DIP)," pp. 295–298, 2014.

[7] J. Thirupathi, "A Comprehensive Survey on Graphical Passwords and shoulder surfing resistant technique analysis," vol. 2, no. 4, pp. 1130–1136, 2015.

[8] P. H. Mokal and R. N. Devikar, "A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes," vol. 3, no. 4, pp. 747–750, 2014.

[9] H. Zhao and X. Li, "S3PAS : A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme."

[10] S. Prabhu and V. Shah, "Authentication Using Session Based Passwords," *Procedia Comput. Sci.*, vol. 45, pp. 460–464, 2015.

[11] Y. Chen, W. Ku, Y. Yeh, and D. Liao, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme," pp. 161–164, 2013.

[12] W. Ku, D. Liao, C. Chang, and P. Qiu, "An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme," pp. 204–208, 2014.