Journal, Advances in Mathematical & Computational Sciences
Vol. 8 No. 3, September, 2020
www.mathematics-computationaljournal.info

Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD)
Southern University Baton Rouge, LA, USA

https://www.isteams.net/socialinformaticsjournal
DOI: dx.doi.org/10.22624/AIMS/MATHS/ V8N3P1
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

TrimT: A Graphical Password Authentication Scheme

Adebimpe, Lateef Adekunle
Department of Computer Science
Emmanuel Alayande College of Education
Oyo, Oyo State, Nigeria.
E-mail: dradebimpela@yahoo.com

ABSTRACT

Globally, the task of ensuring that unauthorized users are not given access into a secured system is being given necessary attention. As a result researchers have developed varieties of authentication methods. Alphanumeric password is the foremost and most common authentication method. Researches have shown that, it is difficult for users to remember strong and random alphanumeric password. Sequel to this, graphical password was introduced. Graphical password adopts visual interface. Human brain can remember visual images better than random characters [1]. Many graphical password methods have been proposed. After reviewing some of the existing graphical password methods, the outcome of the review indicated that login time of most of the graphical password methods is high. It is against this backdrop that this research principally focused on developing a new graphical password authentication method aiming at reducing login time.

Keywords: Graphical Password, Login time, Alphanumeric, Authentication.

Adebimpe, L.A. (2020): TrimT: A Graphical Password Authentication Scheme. Journal of Advances in Mathematical & Computational Sc. Vol.8, No. 3. Pp 1-12. DOI: dx.doi.org/10.22624/AIMS/MATHS/ V8N3P1. Available online at www.isteams.net/ mathematics-computationaljournal.

1. INTRODUCTION

Graphical password authentication uses visual objects (e.g. images, pictures, icons) to perform authentication. Users are required to reproduce previously drawn object or to identify previously registered objects [1]. To ensure strong authentication this process may be repeated for several rounds. The belief is that it will be difficult for adversaries to gain access. However, it is often result into increased login time. Researches have shown that login time is one of the major design and implementation issues of graphical password systems. Therefore, a new graphical password method is proposed in this research.

2. RELATED WORKS

De Angeli et al. proposed a graphical authentication method in 2002 [2]. During the registration procedure, a user is required to register several images. The user is required to remember the sequence of the registered images. During the authentication procedure, the user is required to identify and click the registered images in a particular sequence. According to the author, the scheme is easier to remember when compared with alphanumeric scheme.

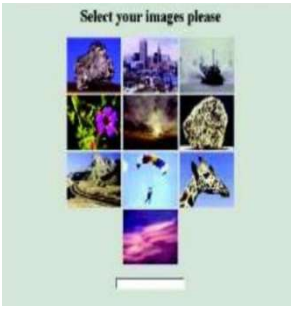

Figure 1: User interface of De Angeli et al's system (adopted from [2])

Sobrado and Birget proposed a method that used movable frame in 2002 [3]. During the registration procedure, a user is required to register four images. During the authentication process, the user is required to identify and arrange three of the registered images on a straight line to login. According to the author, this method can prevent shoulder-surfing attack.

Figure 2: User interface of Sobrado and Birget's system (adopted from [3])

Jansen et al proposed a graphical authentication method in 2003 [4]. During the registration procedure, a user is required to register certain images from thirty images shown on a 5 x 6 grid. The user is required to remember the sequence of the registered images. During the authentication procedure, the user is required to identify and click the registered images in a specific sequence. According to the authors, this system can prevent shoulder-surfing attack. However, the system is vulnerable to FOA attack.

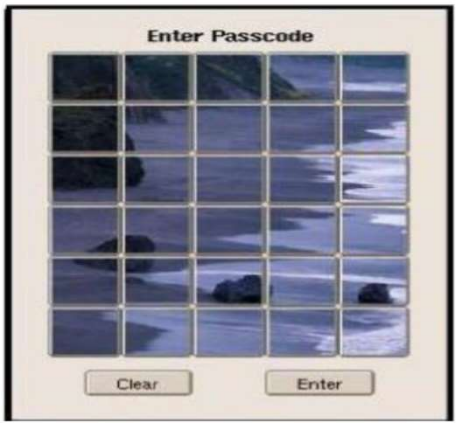

Figure 3: User interface of Jansen et al's system (Adopted from [4]).

Hayashi et al. proposed a graphical authentication method in 2008 [5]. During the registration procedure, a user is required to register several images. After that, the system distort the images such that only user is able to recognize the images. During the authentication procedure, the user is required to identify and click the registered images. According to the authors, this scheme can prevent shoulder-surfing attack since the distorted images are only meaningful to the user.

Figure 4: User interface of Hayashi et al's system (Adopted from [5]).

Bicakci et al. proposed an authentication method that used varieties of icons in 2009 [6]. During the registration procedure, a user is required to register several icons as password. The user is required to remember the sequence of the registered icons. During the authentication procedure, the user is required to identify and click the icons in a specific sequence. According to the author, this system is able to confuse attackers by using different decoy icons.

Figure 5: User interface of Bicakci et al's system (Adopted from [6]).

Stobert and Biddle proposed Object PassTile scheme in 2012 [7]. During the registration procedure, a user is required to register five images from the images shown in the 8 x 6 grid cells. During the authentication procedure, the user is required to identify and click the registered images in sequence. This method is vulnerable because attackers can easily capture the clicked images.

Figure 6: User interface of Stobert and Biddle's system (Adopted from [7]).

Por proposed a graphical authentication method in 2013 [8]. During the registration procedure, a user is required to register a minimum of eight images from the images shown in the 4 x 4 grid cells. During the authentication procedure, four or five of the registered images are shown in the challenge set. To login, the user is required to identify and click the registered images shown in sequence. According to the author, this method can confuse attacker since the user only click a subset of the registered images.

Shaikh et al proposed a method called NAPTune in 2015 [9]. During the registration procedure, a user is required to register six images. Each of these images is associated with a character. During the authentication procedure, the user is required to key in the characters associated with registered images in sequence. This method is vulnerable because attackers can capture the characters key in by the user and subsequently use it to login legitimately.

Figure 7: User interface of Shaikh et al's system (Adopted from [9]).

Assal et al. proposed an authentication method in 2016 [10]. During the registration procedure, a user is required to register five images from the images shown in the 8 x 6 grid cell. After that, the user needs to create a story around the registered images to aid memorability. During the authentication procedure, the user is required to identify and click the registered images in sequence to login. This method is vulnerable because attackers can easily capture the clicked images.

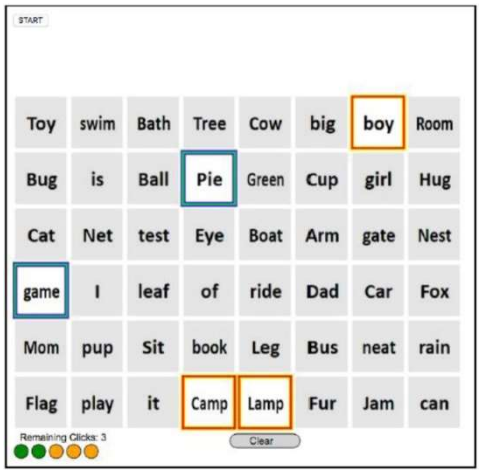

Figure 8: User interface of Assal et al's system (Adopted from [10]).

Yu et al. proposed a method called EvoPass in 2017 [11]. During the registration procedure, a user is required to register three images. After that, the system distort all the images to be displayed in the challenge set. During the authentication procedure, the user is required to identify and click the registered images. According to the authors, the scheme can prevent attack because the clicked images are meaningless to the attackers.

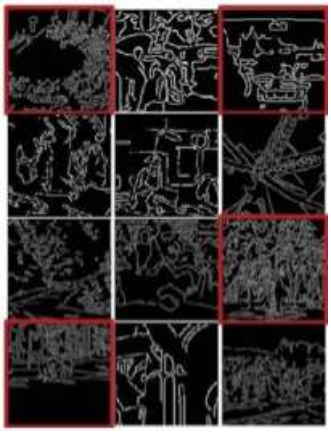

Figure 9: User interface of Yu et al's system (Adopted from [11]).

Maximilian et al. proposed an authentication method that used varieties of icons in 2017 [12]. During the registration procedure, a user is required to register four icons. The user is required to remember the sequence of the registered icons. During authentication, the user is required to identify and click the icons in a specific sequence. This method is vulnerable because attackers can easily capture the clicked images.

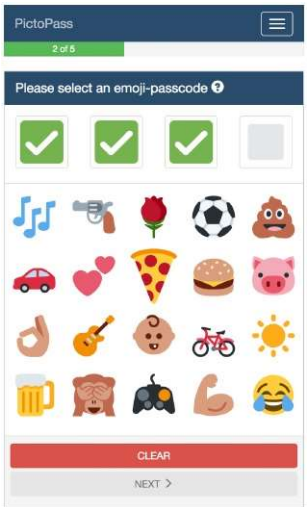

Figure 10: User interface of Shaikh et al's system (Adopted from [12]).

Adebimpe proposed an authentication method named DPass in 2019 [13]. During the registration procedure, a user is required to register one image from the images shown in the 4 x 4 grid cells. After that the user is required to register a four-digit figure. During the authentication procedure, a challenge set that consists of 4 x 4 grid is shown. To login, the user is required to mentally navigate from the current position of the registered image based on the value of the registered figure. The first digit determines forward movement.

The second digit determines backward movement. The third digit determines upward movement. The fourth digit determines downward movement. According to the author, this method can confuse attacker because it will be difficult for attackers to determine the registered image and the number of mental movement.

(a) (b)

Figure 11: User interface of Adebimpe's system (adopted from [13]). (a) Registration (b) Authentication

3. PROPOSED SYSTEM

The proposed system is divided into registration procedure and authentication procedure

3.1 Registration Procedure

During the registration process, a 5x5 grid is shown. The user is required to register several images from the images shown in the grid. After that the user is required to reconfirm the registered images.

Figure 12: Registration interface

3.2 Authentication Procedure

During the authentication procedure, a challenge set that consists of 5x5 grid is shown. A total of twenty five (25) images are randomly displayed in the 5x5 grid cells. To login, the user is required to click the row without a registered image. After that, the user is required to click next button.

Figure 13: Authentication Interface

4. EVALUATION

4.1 Participants

A total of 100 participants were invited to evaluate the effectiveness of the proposed method in terms of reducing login time. 67 participants were male and 33 were female. Each participant was tested separately.

4.2 Procedure

The user study was carried out in three sessions. The initial session (day 1), the second session (7days) and the third session (30days). In the initial session, participants were trained on how to use the proposed system. After that, the participants were instructed to create an individual account to login. The login time was recorded by the system. In the follow-up sessions (7 days session and 30 days session), participants were asked to log into proposed system and the login time was recorded by the system.

4.3 Results

As shown in the table 1 below, the minimum time taken by the participants for a successful login is 2.0 seconds. 4.0 seconds is the maximum time taken by the participants for a successful login. The average login time taken by the participants is 2.3 seconds.

Table 1: Statistics of successful login time

item	time (seconds)
Minimum	2.0
Maximum	4.0
Mean	2.3

5. DISCUSSION

Table 2 shows the login time comparison between the selected graphical password methods and the proposed method. The proposed method has the shortest login time 2.0 seconds followed by Por et al. system [17] 3.0 seconds and ColorLogin [15] 3.4 seconds. In term of mean login time, the proposed method has the shortest login time 2.3 seconds followed by Por et al. system [17] 9.67 seconds, then Salman et al. system [19] 22.33 seconds.

Table 2: Login time Comparison

Method	Min login time (seconds)	Max login time (seconds)	Mean login time (seconds)
CHC [14]	24.08	150.42	71.66
ColorLogin [15]	3.4	11.3	No specify
Ho et al. [16]	16.1	184.2	53.5
Por et al. [17]	3.0	28.0	9.67
PassMatrix [18]	No specify	No specify	31.31
Salman et al. [19]	22.0	29.75	22.33
DPass [13]	22.0	29.75	22.33
Proposed method	2.0	4.0	2.3

6. FUTURE WORKS

This research only focus on reducing login time, other usability factors are not covered in this research work. Consequently, the future work should consider other usability factors as well as design and implementation issues of graphical password authentication.

REFERENCES

[1] Por, L.Y., Adebimpe, L.A., Idris, M.Y.I., Khaw, C.S., & Ku, C.S. (2019). LocPass: A Graphical Password Method to Prevent Shoulder-Surfing. *Symmetry*, 11(10), 1252.

[2] De Angeli, A., Coutts, M., Coventry, L., Johnson, G. (2002). VIP: A visual approach to user authentication. *Proceedings of the Working Conference on Advanced Visual Interfaces*, pp. 316-323.

[3] Sobrado, L. (2002). Graphical passwords. *The Rutgers Scholar, an electronic Bulletin for undergraduate research*.

[4] Jansen, W., Gavrila, S.I., Korolev, V., Ayers, R. P., & Swanstrom, R. (2003). Picture password: a visual login technique for mobile devices. *UMBC Student Collection*.

[5] Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008, July). Use your illusion: secure authentication usable anywhere. In *Proceedings of the 4th symposium on Usable privacy and security* (pp. 35-45).

[6] Bicakci, K., Atalay, N.B., Yuceel, M., Gurbaslar, H., & Erdeniz, B. (2009, July). Towards usable solutions to graphical password hotspot problem. In *2009 33rd Annual IEEE International Computer Software and Applications Conference* (Vol. 2, pp. 318-323). IEEE.

[7] Stobert, E., & Biddle, R. (2012, December). Visual end-user security. In *2012 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)* (pp. 233-234). IEEE.

[8] Por, L.Y. (2013). Frequency of occurrence analysis attack and its countermeasure. *Int. Arab J. Inf. Technol.*, *10*(2), 189-197.

[9] Shaikh, J., Pawar, C.C., Jadhav, V.S. & Sindhu, M.R. (2015). User authentication using graphical system. *Progress in Science and Engineering Research Journal*, 17(3), 56-61.

[10] Assal, H., Imran, A., & Chiasson, S. (2018). An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction*, 18, 37-46.

[11] Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W. T., & Song, L. (2017). EvoPass: Evolvable Graphical Password against Shoulder-Surfing Attacks. *Computer & Security*, 70, 179-198.

[12] Maximilan, G., Dennis, D., & Markus, D. (2017). EmojiAuth: Quantifying the Security of Emoji-based Authentication. *USEC '17*, 26 February 2017, San Diego, CA, USA.

[13] Adebimpe, L.A. (2019). DPass: A Method for Preventing Shoulder-Surfing Attack. *Journal of Digital Innovations & Contemporary Resources in Science, Engineering & Technology*, 7(2), 105-114.

[14] Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces* (pp. 177-184). ACM.

[15] Gao, H., Liu, X., Wang, S., Liu, H., & Dai, R. (2009, December). Design and analysis of a graphical password scheme. In *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on* (pp. 675-678). IEEE.

[16] Ho, P.F., Kam, Y.H.S., Wee, M.C., Chong, Y.N., & Por, L.Y. (2014). Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information. *The Scientific World Journal*, *2014*.

[17] Por, L.Y., Ku, C.S., Islam, A., & Ang, T.F. (2017). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. *Frontiers of Computer Science*, 1-11.

[18] Sun, H.M., Chen, S.T., Yeh, J.H., & Cheng, C.Y. (2018). A shoulder surfing resistant graphical authentication system. IEEE Transactions on Dependable and Secure Computing. 15(2), 180-193.

[19] Salman, M., Li, Y., & Wang, J. (2019, July). A Graphical PIN Entry System with Shoulder Surfing Resistance. In *2019 IEEE 4th International Conference on Signal and Image Processing (ICSIP)* (pp. 203-207). IEEE.