ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse08842019.pdf
https://doi.org/10.30534/ijatcse/2019/08842019

Towards Usability Evaluation of Jumbled PassSteps

Jerome P. Songcuan[1], Dr. Ariel M. Sison[2], Dr. Ruji P. Medina[3]
[1]Technological Institute of the Philippines, Philippines, jerome.songcuan@dmmmsu-sluc.com
[2]Emilio Aguinaldo College, Philippines, ariel.sison@eac.edu.ph
[3] Technological Institute of the Philippines, Philippines, ruji.medina@tip.edu.ph

ABSTRACT
Authentication plays a crucial role in information security by which several mechanisms are widely used to protect services from attacks. Graphical password is the most popular mechanism and frequently assert the advantage that they are significantly more secure. However, most graphical passwords are susceptible to shoulder surfing attack. To overcome this problem, this study proposed a hotspot guessing attack resistant graphical password authentication scheme based on the modified PassMatrix method. The modification involves replacing the single discretized image of the PassMatrix method into several independent images and applying a random grid traversal method. The proposed Jumbled PassSteps was evaluated in terms of its usability. Experimental results showed that the users were able to remember their graphical passwords successfully as the memorability percentage reached 100.00% and 90.90% in the first and second session respectively. Further, users achieved an average registration time of 29.96 seconds and carried out two log-in attempts with an average time of 46.03 seconds and 63.43 seconds.

Key words: graphical password, Jumbled PassSteps, PassMatrix, usability.

1. INTRODUCTION

A secured user authentication system is vital nowadays in light of the increasing amount of sensitive information available. A technique which is based on graphical password authentication is now getting huge attentions from various business organizations. This password authentication scheme offers a good trade-off between security [1], [2] and password memorability. In fact, studies have revealed that graphical passwords are a better choice to text-based passwords from the memorability and usability perspective [3]-[7].

Graphical password authentication schemes utilize pictures as passwords rather than complex set of characters. Researchers have identified that pictures are more easily remembered than recalling alphanumeric characters for the reason that pictures permits for a greater depth of cognitive processing [8]-[12]. Moreover, pictures basically possess more features than what individual letters and numbers have, thus facilitating retrieval as well. This type of authentication scheme is widely used in some applications such as in social media, online commerce, and banking.

In spite of the fact that graphical schemes offer a more memorable passwords, these should also meet other usability needs such as the time taken in the registration and authentication for widespread adoption. Users have to choose an image from a collection of images when registering and the users have to scan many images to pick several pass images for authentication purposes. These processes must be quick to be considered as efficient graphical password authentication scheme.

There have been various studies on the usability assessment of user authentication systems using a graphical password. Reference [13] compared the memorability of an alphanumeric password to four graphical passcodes. All of the graphical schemes found to be more memorable than the alphanumeric scheme. Same result was found by [14] in which most participants verbally remembered the password. Hence, the performance of the graphical schemes in terms of memorability is satisfactory compared to alphanumeric scheme, for which no participant was able to enter his or her password correctly or verbally remember it three weeks later.

The study of [15] implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its usability. The usability perspective was measured by the amount of time users spent in each PassMatrix phase: registration and authentication. From the experimental result, the proposed system showed better resistance to shoulder surfing attacks while maintaining usability. A usability was also investigated in terms of memorability and efficiency (i.e. registration and authentication time) of multiple image passwords in PHAS [16]. The results demonstrated that the memorability of multiple passwords in PHAS is better than in existing Graphical authentication systems (GASs). Although the registration time took longer, authentication time for successful attempts is either equivalent to or less than the time reported for previous GASs.

A usable Graphical Password Authentication Scheme was proposed [17]. ChoCD, a hybrid graphical scheme, combined the method of "Click-based", "Choise-based", and "Draw-based". It was found that ChoCD is easy to use and provides higher level of memorability. In addition, [18] improved password memorability while not inconveniencing the users. The findings demonstrate that authenticating passwords three times can definitely increase password memorability.

Although the previous studies have achieved high user performance in terms of usability, there are nevertheless several issues which may affect the usability. The limitations of usability include issues such as passwords being too hard to remember after a period of time, taking more time to log in on the registered account, and the complex of authentication method for users without proper education and practice.

2. OBJECTIVES OF THE STUDY

Since the development and security evaluation of Jumbled PassSteps scheme were done in our previous study [10], this paper aims to measure its usability in terms of:

a. Memorability,
b. Registration Speed, and
c. Authentication Speed

3. PROPOSED JUMBLED PASSSTEPS

In this work, we proposed Jumbled PassSteps which is also known as a hostpot guessing attack resistant graphical password authentication scheme based on the modified PassMatrix method. This intends to address PassMatrix's vulnerability to hotspot guessing attacks. The modification involves replacement of the discretized pass-images with several independent pass-images and application of a random grid traversal method.

3.1. Replacing Single Discretized Image into Several Independent Images

Figure 1 shows the proposed Jumbled PassSteps' registration process. At this phase, the user creates an account containing a username and a password. Several independent images in a 5x5 grid are used instead of a single image. From this set of images, the user will choose images as pass-images. Then, the image discretization step from the existing PassMatrix method is removed to avoid hotspot guessing attack. A random number ranging from 1 to the total number of columns in the grid will be presented to the user. This will be assigned as the original number of steps which will be utilized when performing the grid traversal during authentication phase. Thereafter, the username, chosen pass-images, decoy images, and the random number will be stored in the database. This completes the registration phase.

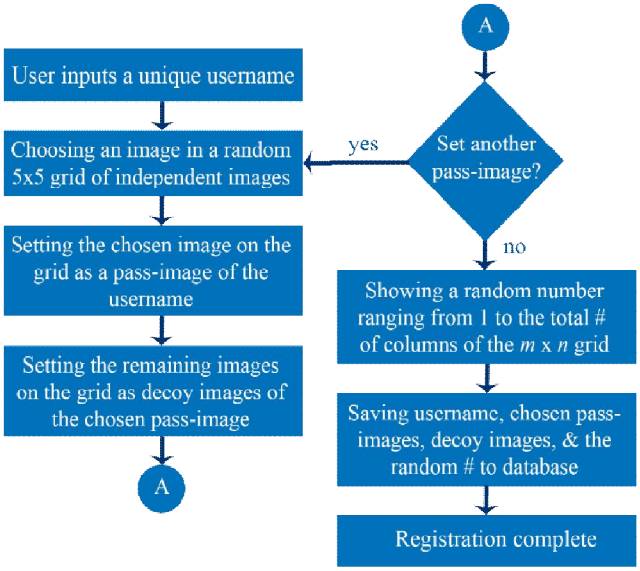

Figure 1: Process of Registration Phase in Jumbled PassSteps

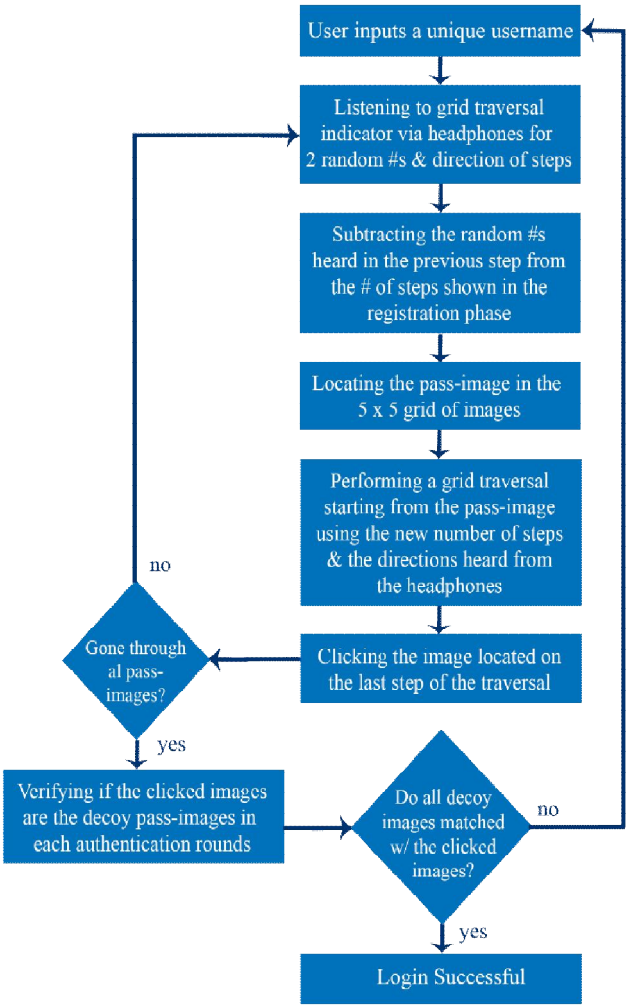

Figure 2: Process of Authentication Phase in Jumbled PassSteps

3.2. Applying Random Grid Traversal Technique

The authentication phase of the proposed Jumbled PassSteps shown in Figure 2 starts with entering the username was created in the registration phase. A new indicator comprising of two random numbers and directions of steps are conveyed to the user through audio feedback. These numbers will be subtracted to the randomly generated number of steps during the registration phase, whereas the other will serve as the random direction of the traversal. For example, if the audio output is "4 UP, 2 LEFT", then the first random number to be subtracted is 4 and the direction of the vertical grid traversal is upward; the second number to be subtracted is 2 and the direction of the horizontal grid traversal goes to the left.

To compute the number of steps to be performed in the traversal, the equations below are used:

For vertical grid traversal:

$$S_1 = P - y \quad (1)$$

For horizontal grid traversal:

$$S_2 = P - x \quad (2)$$

where,

P - a original number of steps previously saved in the registration phase

y - a random number produced for vertical traversal

x - a random number produced for horizontal traversal

S_1 - a number of steps used in performing vertical grid traversal

S_2 - a number of steps used in performing horizontal grid traversal

Absolute value will be considered to use once the difference is a negative number. For example, if the original number is 3, and the random number for vertical traversal is 4, then the number of steps to be used in performing vertical grid traversal is 1.

The user must locate his or her pass-image in the 5X5 grid after the number of steps is obtained. The location of the pass-image will serve as the starting point of the traversal. Meanwhile, the location of the decoy pass-image on the grid will be computed using the following equation:

$$decoyLoc = (decoyCol, decoyRow) \quad (3)$$

After visually locating the decoy pass-image, the user is required to click on it. The challenge round is considered complete until the user has gone through three rounds. Then, a verification will be done whether the decoy pass-images for each round are similar to the images clicked by the user. If all the decoy images matched with the clicked images, then the authentication or login process is successful, otherwise the user will again be required to repeat the whole process.

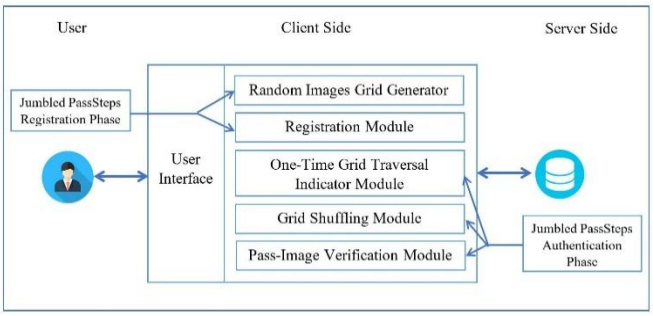

Figure 3: Framework of the Proposed Jumbled PassSteps

3.3. Framework of the Proposed Jumbled PassSteps

Figure 3 shows the framework of the proposed Jumbled PassSteps. Each module is discussed as follows:

a. Random Images Grid Generator - This module generates a 5X5 grid of random images taken from a list of jpeg files.
b. Registration Module - This module stores the username, pass-images, decoy images, and the random number of steps to the user database.
c. One-Time Grid Traversal Indicator Module - This module produces a random number to be subtracted from the random number of steps and a random direction for grid traversal (e.g. up, down, left, right). Headphones are used to acquire the audio output of this module. The random number and direction generated are used to locate the decoy pass-image.
d. Grid Shuffling Module - A 5X5 grid consisting of one pass-image and 24 decoy images are the output of this module. The locations of images are random positions in every new call to this module.
e. Pass-Image Verification Module - This module computes for the decoy pass-image basing from the user's pass-image, previously saved random number of steps, and from the output of the one-time grid traversal module. Then, it compares the image that the user clicked from the result of its grid traversal computation. If the two images match, then the user is authenticated.

The Jumbled PassSteps is made up of two phases. First, the registration phase asked the user to create a unique username and to pick-up a single pass-image from the image grid yielded by the random images grid generator. All remaining images are automatically saved as decoys. The process is repeated twice in order to produce three pass-images. Then, a random number is presented to the user that served as the original number of steps when performing the grid traversal. The user must memorize the three pass-images and the original number of steps produced in this phase. The registration module then saved the username, pass-images, decoy images, and the random number of steps to the database.

During authentication phase, the user must listen to the output of the one-time grid traversal indicator module which is the random number to be subtracted to the previously saved original number of steps, and the other is the random direction

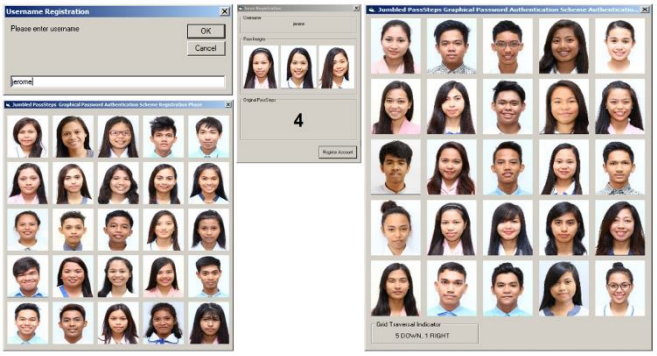

Figure 4: Screenshots of Jumbled PassSteps

of the traversal. The user then subtracted the random number heard from the original number of steps saved during the registration process. Next, the user must locate his or her pass-image from the output of the grid shuffling module. The location of the pass-image served as the starting point of the traversal. After the traversal, the final image became the decoy. The process is done within three authentication rounds. Finally, the pass-image verification module also computed for the decoy images. If the decoy images clicked by the user are the same as the decoy images computed by the verifier module, then the user is authenticated. It can be gleaned in Figure 4 the sample screenshots of registration and authentication in Jumbled PassSteps.

4. RESULTS AND DISCUSSION

The Jumbled PassSteps prototype was developed as a stand-alone application using Visual Basic 6.0 and MySQL 5.0.51. The prototype application was hosted on a laptop with a 15.6 inch screen display set at a resolution of 1366 x 768 pixels, Intel(R) Core(TM) i5 CPU with 4GB RAM, and running Windows 7 64-bit operating system. In addition, a compatible earphone or headset was used to capture the audio signal of the login indicator of the proposed prototype.

Further, a dataset of 2,394 images of ID pictures of students and employees of the Don Mariano Marcos Memorial State University - South La Union Campus was manually acquired to serve as candidate pass-images and decoy images in the simulation phase. In every authentication phase, 24 decoy images and one pass-image were randomly chosen from the dataset. Figure 5 shows sample ID pictures in the dataset.

We assessed the users' experience on Jumbled PassSteps, which includes the successful login rate if they know their passwords or memorability rate and the total time consumed for both registration and authentication. In doing this, there were 30 randomly selected students of the Don Mariano Marcos Memorial State University, College of Computer Science participated in the experiments. These participants are unfamiliar with graphical password authentication schemes. Before conducting tests and evaluations, participants were oriented on how to use the simulated Jumbled PassMatrix authentication scheme.

To measure the memorability rate of Jumbled PassSteps, each participant will try to log into his or her account five times. A successful attempt implies that a user passed the authentication with a correct graphical password. Whereas a failure attempt is marked if all five tries failed. The memorability rate was obtained using the equation below:

$$Memorability\ Rate = \frac{SuccessfulAttempts}{TotalAttempts} \qquad (4)$$

Table 1 shows the average memorability percentage of the participants in the two login sessions. Three pass-images were carefully picked out by each participant as his or her password. The experimental result shows that all participants managed to log into their accounts successfully in the first session (100%). This signifies that their passwords are authenticated within five tries. However, a drop by 9.10% was recorded in the second session (90.90%) which was conducted after two weeks of delay. This drop was caused by three participants who had trouble recalling the pass-images they had previously set in the registration phase. Viewed in its totality, the memorability of the proposed Jumbled PassSteps was impressive because the graphical pass codes were easily remembered, despite being system-assigned, likely due to the picture superiority effect.

Figure 5: Sample ID Pictures of Student and Faculty Members Stored in the Database

Table 1: Memorability of Log-in in Two Sessions

Log-in Session	Memorability Percentage
First Session	100.00%
Second Session	90.90%

Table 2: Elapsed Time Consumed During Registration and Authentication Phase

Activities	Average Time (s)
Registration	29.96
Log-in First Session	46.03
Log-in Second Session	63.43

Further, Table 2 gives the average elapsed time that participants consumed in both registration and authentication phases. The registration took 29.96 seconds on average. This entails that participants did not consume much time in selecting pass-images which they think are meaningful to them. In addition, being computer literate and the fact that only three pass-images are considered, became factors that influenced in spending shorter time in registration. While the results of the existing studies [5], [15] affirmed that 134 and 106 seconds are acceptable to users in practice, this study concludes that the average registration time of 29.96 seconds are also acceptable in general.

Relative to authentication phase, it is noteworthy to mention that participants took 46.03 seconds to log into Jumbled PassSteps in the first session after they registered an account. The result is lower than the average login time (63.43 seconds) recorded in the second session. The increase of login time was because the participants needed to recall their passwords after two weeks. Findings from interviews showed that familiarity plays the main role in helping the participants to recognize their graphical passwords. Some participants stated that they did not even try to remember their passwords because they selected the most familiar pictures to them as their graphical passwords. In addition, the interviews also manifest that the simplicity of the picture could aid the participants in the authentication phase. It removes the conflict that may happen if each pass-image contains more than one object. On the whole, the time spent in the login process is acceptable to the participants to make their passwords less vulnerable to hotspot guessing attack. The acceptability of the said result is based on the study of [15] where average login time in the first session (31.11 seconds) and second session (37.11 seconds) are acceptable to the participants.

5. CONCLUSION AND FUTURE WORK

In this paper, we evaluated the usability of the proposed hotspot guessing attack resistant graphical password authentication scheme based on the modified PassMatrix method, named Jumbled PassSteps. The modification involves replacement of the discretized pass-images with several independent pass-images and application of a random grid traversal method. Jumbled PassSteps is designed to resist security threats without sacrificing ease of use.

Based on the usability evaluations, results show that majority of the participants can log into their accounts successfully using their graphical passwords. Schemes with graphical password authentication enhanced the memorability. In addition, the time spent in registration and authentication of Jumbled PassSteps are acceptable to the participants. Hence, the proposed mechanism of authentication is usable in terms of memorability, and registration and authentication speed.

Some avenues for future work include enlarging the sample of participants and conducting more experiments for an extended period of time. Other aspects worth considering include finding the effects of a particular image utilized successfully as graphical passwords and investigating the effectiveness of the current design on different platforms.

ACKNOWLEDGEMENT

We thank Technological Institute of the Philippines, Don Mariano Marcos Memorial State University, and Commission on Higher Education for their support towards the fulfillment of this scholarly endeavor. Also, we are grateful to the students of the College of Computer Science, DMMMSU-SLUC for their actual participation in this work.

REFERENCES

1. P. Amarendra Reddy and O. Ramesh. **Security mechanisms leveraged to overcome the effects of big data characteristics**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol 8, no. 2, pp. 312-318, 2019.
2. K. Sudharani, N. K, Sakthivel, and S. Subasree. **B^{2}EIS-RG:Biometric-based bucket encrypting index structure with random generator**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol 8, no. 2, pp. 165-175, 2019. https://doi.org/10.30534/ijatcse/2019/10822019
3. T. Khodadadi, A. M. Islam, S. Baharun, and S. Komaki. **Evaluation of recognition-based graphical password schemes in terms of usability and security attributes**, *International Journal of Electrical and Computer Engineering*, vol. 6, no. 6, pp. 2939-2948, Dec. 2016. https://doi.org/10.11591/ijece.v6i6.11227
4. G. W. Bin, S. Safdar, and R. Akbar. **Graphical authentication based on anti-shoulder surfing mechanism**, in *Proc 2nd International Conference on Future Networks and Distributed Systems*, Amman, Jordan, 2018, pp. 20-25.

5. H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell. **Graphical one-time password (GOTPass): A usability evaluation**, *Information Security Journal: A Global Perspective*, vol. 25, pp. 94-108, May 2016. https://doi.org/10.1080/19393555.2016.1179374
6. A. V. Kayem. **Graphical password- A discussion**, *in Proc 2016 30th International Conference on Advanced Information Networking and Applications Workshops*, Crans-Montana, Switzerland, 2016, pp. 596-600. https://doi.org/10.1109/WAINA.2016.31
7. F. Alt, S. Schneegass, A. S. Shirazi, M. Hassib, and A. Bulling. **Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes**, in *Proc 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, Copenhagen, Denmark, 2015, pp. 316-322. https://doi.org/10.1145/2785830.2785882
8. G. Yang and H. Oh. **Implementation of a graphical password authentication system 'PassPositions**, *Journal of Image and Graphics*, vol. 6, no. 2, pp. 177--121, 2018. https://doi.org/10.18178/joig.6.2.117-121
9. S. A. Razvi, S. Neelima, C. Prathyusha, G. Yuvasree, C. Ganga, and K. M. Kumar. **Implementation of graphical passwords in internet banking for enhanced security**, in *Proc 2017 International Conference on Intelligent Computing and Control Systems*, Madurai, India, 2017, pp. 35-41. https://doi.org/10.1109/ICCONS.2017.8250743
10. P. Dunphy, J. Nicholson, and P. Olivier. **Securing passfaces for description**, in *Proc 4th symposium on Usable privacy and security*, Pittsburgh, PA USA, 2008, pp. 24-35. https://doi.org/10.1145/1408664.1408668
11. H. M. Aljahdali and R. Poet. **Users' perceptions of recognition-based graphical passwords: A qualitative study on culturally familiar graphical passwords**, in *Proc 7th International Conference on Security of Information and Networks*, Scotland, UK, 2014, pp. 279-283. https://doi.org/10.1145/2659651.2659728
12. J. P. Songcuan and A. M. Sison. **Jumbled passsteps: A hotspot guessing attack resistant graphical password authentication scheme based on the modified passmatrix method**, in *Proc 3rd International Conference on Cryptography, Security and Privacy*, Malaysia, 2019, pp. 55-59. https://doi.org/10.1145/3309074.3309099
13. K. Johnson and S. Werner. **Graphical user authentication: A comparative evaluation of composite scene authentication vs. three competing graphical passcode systems**, in *Proc Human Factors and Ergonomics Society Annual Meeting*, vol. 52, no. 6, pp. 542-546, Sep. 2008. https://doi.org/10.1177/154193120805200607
14. A. A. Cain and J. D. Still. **Usability comparison of over-the shoulder attack resistant authentication schemes**, *Journal of Usability Studies*, vol. 13, no. 4, pp. 196-219, Aug. 2018.
15. H. M. Sun, S. T. Chen, J. H. Yeh, and C. Y. Cheng. **A shoulder surfing resistant graphical authentication system**, *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180-193, 2018. https://doi.org/10.1109/TDSC.2016.2539942
16. S. Chowdhury, R. Poet, and L. Mackenzie. **Passhint: memorable and secure authentication**, in *Proc SIGCHI Conference on Human Factors in Computing Systems*, Toronto, Canada, 2014, pp. 2917-2926. https://doi.org/10.1145/2556288.2557153
17. R. R. Afandi and M. Z. Jali. **ChoCD: Usable and secure graphical password authentication scheme**, *Indian Journal of Science and Technology*, vol. 10, no. 4, pp. 1-5, Jan. 2017. https://doi.org/10.17485/ijst/2017/v10i4/110885
18. N. Woods and M. Siponen. **Improving password memorability, while not inconveniencing the user**, *International Journal of Human-Computer Studies*, vol. 128, pp. 61-71, 2019. https://doi.org/10.1016/j.ijhcs.2019.02.003