# Password Recovery Using Graphical Method

**Wafa' Mohd Kharudin, Nur Fatehah Md Din and Mohd Zalisham Jali**

**Abstract** Authentication with images or better known as graphical password is gaining its recognition as an alternative method to authenticate users, for it is claimed that images or pictures are easier to use and remember. The same method can be applied to password recovery, with the purpose to ease the process of users in regaining their account in case of forgotten passwords. A total of 30 participants were asked to use a prototype implementation of graphical password recovery and provide feedbacks. The data gained were analyzed in terms of attempts, timing, pattern, and user feedback. Overall, it was found that participants had no problem in using graphical password recovery despite they were new to it. Most of them preferred the choice-based method, even though they agreed that it provided less security. Graphical recovery has potential to be used more widely in current technology, although more works need to be done to balance the issues of usability and security.

**Keywords** Graphical password · Password recovery

## 1 Introduction

Normally upon signing up on systems which require usernames and passwords, for example, social media sites (i.e., Facebook and Twitter) and e-mail accounts (Gmail and Yahoo), users are also required to fill up the recovery options for their passwords. The purpose of these recovery options is to make sure users can still login or regain their account in case of passwords forgotten. There are a few options of recovery methods that are being used by almost all systems and sites such as recovery using challenge questions, recovery by e-mail, and recovery by text message.

Recovery by using challenge questions works by asking users to select desired questions from a set of questions and then gives answers to those questions. This

W.M. Kharudin (✉) · N.F.M. Din · M.Z. Jali
Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800, Nilai, Negeri Sembilan, Malaysia
e-mail: wafamohdkharudin@gmail.com



A. Abraham et al. (eds.), *Pattern Analysis, Intelligent Security and the Internet of Things*, Advances in Intelligent Systems and Computing 355,
DOI 10.1007/978-3-319-17398-6_2

kind of method will help the system to recognize legitimate users later in case if they forget their passwords. Only users who can answer all challenge questions correctly will be granted access to recover or reset their old password. Recovery by e-mail or text message works by the system sending a reset link (or a new password) to their preregistered e-mails or mobile phone numbers.

However, how secure it actually is to be using these methods in case of forgotten passwords? It is no doubt that all the methods provide some sort of protection to users' accounts and data, but then again, is it perfectly secure? Imagine a situation where a hijacker tries to gain access on someone's Facebook account and the hijacker has somehow managed to gain control of the particular user's e-mail account or mobile phone. Then, it will be so easy for the hijacker to log into the user's Facebook account or any other accounts registered under the same e-mail address or phone number. This situation is perfectly possible which could result in breaches of data and even more severe consequences, so it is very crucial to address this issue.

Having said that, we are proposing graphical recovery as an alternative for password recovery. The idea of graphical recovery is to apply graphical methods in graphical recovery technique. The aim of this study was to investigate the usability of graphical recovery. A trial was conducted where 30 participants were asked to use a prototype and later provide feedback. The data collected were then analyzed in terms of number of attempts, timing, pattern, and user feedback.

This paper is arranged as follow. Section 2 discusses the state of the art of graphical authentication, which also highlights the advantages of graphical authentication, especially from psychological aspect. Section 3 describes the methodologies used in this study, while Sect. 4 provides the results gained from the trial. Lastly, conclusion and future works are discussed in Sect. 5.

## 2 Graphical Recovery

Password recovery process is just as essential as login process, where both can be compromised by malicious attempts. A non-legitimate user might gain access to an account by using some techniques to recover someone's password. One of the most compelling reasons for exploring the use of a graphical method comes from the fact that humans seem to possess a remarkable ability for recalling pictures, whether they are line drawings or real objects [1].

Graphical authentication is not a new thing. Beginning around 1999, a multitude of graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks [2]. It is reported that there is a growing interest in using pictures as an authentication method, but not much research has been done so far. But the research on this area has now started gaining more attention from researchers; from their classifications up until to their specific applications, both positive and negative findings were reported [3].

From the psychological view, the usability of graphical password schemes is promising as many studies have explained about the 'picture superiority effects' toward verbal and words. The idea behind graphical method is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches. A number or psychological studies explaining the 'picture superiority effects' toward verbal and words explain the usability of graphical passwords. A study claimed that humans have exceptional ability to recognize images previously seen, even those viewed very briefly [4].

In a study by [5], four experiments were conducted to examine the relationship between perception and memory. The first two experiments were about memory recognition for pictures. Experiment 1 used 1100 pictures taken from the magazines, with Experiment 2 used 2560 pictures obtained from the photographers. Overall, they found that participants scored up to 95 % success for Experiment 1 and for Experiment 2, participants still scored 85 % recognition success even after 4 days time. The last two experiments were about the effect of duration and the effect of reversing and orienting the pictures during viewing. From the results, it was summarized that participants still managed to score above 90 % success rate even the images were reversed. On the whole, they concluded that participants managed to obtain higher success rate for picture recognition. These psychological studies have given an insight to the claim that using images or pictures was superior to using words, with regard to recognizing and memorizing.

In this paper, graphical techniques were grouped into three categories, namely 'choice-based,' 'draw-based,' and 'click-based.' These categories were solely based on the users' actions while carrying out authentication tasks. Briefly, choice-based refers to the action of selecting a series of images from among a larger set of images, draw-based refers to the action of drawing a pattern on an image, whereas click-based refers to the users' action clicking on areas within a given image [6].

The idea of graphical recovery is to allow users to log into their accounts using the conventional usernames and text passwords method as they are used to. But in case of forgotten passwords, instead of recovering their accounts through challenge questions which they might forget the answers of, or by e-mail which may exposed to the risk of being controlled by a hijacker, they can recover their passwords by using graphical method. Graphical recovery is advantageous in the sense that only the right user would know the secrets, it is more memorable as images can trigger user's memory, and it is also more secure as compared to other types of recoveries such as by e-mails or phone.

## 3 Methodology

In order to test the feasibility of graphical password recovery, a prototype on graphical recovery was developed and a survey was conducted. A number of 30 participants with different backgrounds were asked to use the prototype and then answer a related questionnaire. This activity took approximately 10–20 min to

complete depending on the participants' familiarity of using computers. The same participants were tested a week later using the same prototype to reproduce the same secrets, without any prior information.

There were two main modules in the prototype—registration and recovery. In the registration module, participants needed to register their recovery secrets by entering a desired username and password, and then, they needed to choose a picture out of a selected theme, with each theme consisted of a set of images (choice-based). Participants then needed to draw a line on the image they have chosen (draw-based), and finally, they needed to click three times on the same image (click-based). In the recovery module, participants can recover their passwords by using their secrets, with no limitations were made toward the number of trials they were allowed to do.

The development of the choice-based method was made with reference to the scheme [7–9]. The photographs were taken from previous research by [6]. In choice-based, participants were needed to choose an image from three themes which were flowers, places, and animals. These themes were chosen because they were common images which were easy to recognize and remember. Click-based method was made with reference to the scheme by [6, 10], where the tolerance scale of the image was 18 × 18 pixels. The display size of the images was 320 × 320 pixels.

All three methods of graphical authentication were combined, making it a hybrid instead of just taking one method with the purpose to make it less guessable. The combination of these three methods was hopefully would result in a hard-to-guess secret, which was not only advantageous in the aspect of security, but also aided memorability and usability.

The setting for this trial was set for the participants to do as following:

1. Register username and password.
2. Register the secrets for graphical recovery.
   (a) Select an image from given theme.
   (b) Draw a line on the image.
   (c) Click 3 points on the image.
3. Test the secrets.
4. A week later—retest the secrets (Figs. 1, 2, and 3).


**Fig. 1** The screenshot of the prototype's main menu


**Fig. 2** Screenshot from choice-based secret


**Fig. 3** Screenshots of examples from draw-based secret (*left*) and click-based secret (*right*)

## 4 Results and Findings

A total of 30 participants took part in this study (14 males and 18 females), with an average age of 21 (sample range from 12 to 30). The participants were of various backgrounds, and all of them had more than 3 years of experience using computers.

### *4.1 Observation*

All participants started their registration after being briefed about how the prototype worked. Overall, only 13 out of 30 participants managed to complete both registration and recovery tasks without any failed attempts. The remaining participants needed 2–5 attempts before completing their tasks. These suggest that appropriate training should be provided beforehand for the graphical recovery to be effective.

Based on the observation, it was apparent that the participants were initially quite confused with graphical recovery, as only a few of them were aware about graphical authentication. Only 6 participants claimed that they were aware of it through personal exposure, while the others have never knew about it. Majority of them had problems to understand how it worked, and they drew and clicked on the image during registration without taking into account the memorability of their secrets. As a result, during confirmation process, they needed a couple of (two to four) attempts until they got their secrets right.

### *4.2 Attempts and Memorability*

All participants managed to successfully completed all the tasks required (registration, confirmation, and recovery). For the first step which was choosing an image (choice-based), all participants were able to complete the choosing task with only one attempt. The second step was to draw a single line on the chosen image (draw-based). The number of attempts was significantly higher for this step as they had to precisely draw the exact line as they did for the first time.

The third step required the participants to click 3 points on the same, chosen image (click-based). The number of attempts for this step was also as high as the draw-based. These results were predicted as participants had to carefully click on their secret areas in sequence, which sometimes they did not manage to do.

A week later, the participants were tested again if they remembered their secrets. Most of the participants were able to do choice-based step with only one attempt. However, majority of them needed several (two to five) attempts until they got their secrets for draw-based and click-based right.

## 4.3 Timing

Each participant's registration and recovery duration were recorded to calculate their average time. The time was measured from they first chosen their secret image until they finished with their drawing and clicking secrets. Table 1 gives the mean and standard deviation (SD) for each registration and recovery process. Note that each process consisted of the three methods—choice-based, draw-based, and click-based.

It was noticeable that participants took longer during registration compared to the confirmation and recovery tasks. It is probably because during registration, it was the first time for most of the participants to be using any sort of graphical authentication or recovery, so it took them time to familiarize themselves with the state of the art of it. As they became clear with the process, it can be seen from the table that the participants took much lesser time for confirmation and immediate recovery.

All participants were tested again a week later to see if they can reproduce their secrets—and from the results in Table 1, they took almost double the time they needed for immediate recovery. All of them did not expect to be tested again; therefore, they did not try to remember their secrets. Majority of them needed two to four attempts until they got their secrets right.

## 4.4 Pattern

For the choice-based method where participants needed to choose an image, it can be seen that the image chosen was mostly influenced by participants' personal preferences. For example, female participants were most likely to choose image from flowers or animals theme, while male participants tend to choose image from places theme. They would choose the image that they found the most interesting or beautiful. Table 2 shows image popular from each theme.

For the draw-based where they had to draw a line on the chosen image, most of the participants chose to draw from and stop at a point that was sharp (i.e., the tip of a finger). There is admittedly a constraint at this part of study where participants were only allowed to draw a single line. If they were allowed to draw more complex pattern on the image, presumably more interesting patterns can be found.

**Table 1** Mean and standard deviations for time taken

| $N = 30$ | | Time (s) |
|---|---|---|
| Registration | Mean | 228 |
| Confirmation | Mean | 78 |
| Recovery—immediate | Mean | 48 |
| Recovery—one week later | Mean | 96 |

**Table 2** Popular image from each theme

| Theme | Image description | No. of participants |
|---|---|---|
| Flowers | Sunflower | 7 |
| | Single pink rose | 5 |
| Places | Sea port | 4 |
| | Flight runway | 2 |
| Animals | Lions | 4 |
| | Cats | 4 |

For the click-based where participants needed to choose 3 click-points, it was found that most of them liked to click on something sharp or edgy (i.e., the edgy petal of a flower). This would do favor in accuracy aspect, as participants were more likely to accurately clicked on their secret points. Figure 4 shows examples of secrets made by a few participants.

## *4.5 Participants' Feedback*

In general, participants had different perceptions for each method of the whole process. For the choice-based method, 28 out of 30 participants agreed that they could remember their images well and had no problems to perform the task of choosing an image. However, 21 participants thought that it was too vulnerable for security attacks and thus did not offer good security.

For the draw-based, 22 participants agreed that they could remember their secrets well, despite some of them suggested that they should be allowed to draw


**Fig. 4** Samples of click secrets. *Different shapes* represent different users

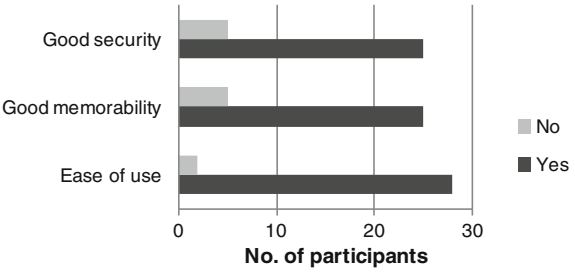


**Fig. 5** General feedback from participants based on questionnaire

more complex patterns on the image. However, complex patterns may cause disadvantages in terms of memorability.

For the click-based, 25 participants felt that it was easy to use and agreed that they could remember their click-points well. Majority of them also agreed that click-based provided better security as compared to choice-based. Around 10 participants suggested that they should be allowed to click as many click-points as they like.

Overall, it can be seen that this graphical recovery prototype was well received by the participants, despite some suggestions were made based on their preferences and ease of use (Fig. 5).

## 5 Conclusion

From the results of survey made to 30 participants, it can be said that many are still not familiar with graphical authentication or recovery. They found it interesting, albeit a little confused with the state of the art of graphical recovery in the beginning. After a brief explanation, all of them were able to carry out all required tasks.

The prototype consisted of a hybrid or 3 combined methods which were choice-based, draw-based, and click-based. This has made participants to develop preferences over which method they liked best. Majority of them preferred choice-based, for its memorability and ease of use. However, they also agreed that choice-based might be prone to attacks such as guessing and shoulder surfing. In regard to security, many of them preferred draw-based and click-based. Nonetheless, participants agreed that this hybrid method which combined all these three graphical methods provided adequate security for their secrets.

Participants were tested again a week after the first survey was conducted to test their memorability on their secrets. Despite taking longer time than the previous week, majority of the participants were able to recall their secrets.

One of the lessons learned from this evaluation came from a number of feedbacks that suggested participants wanted to be allowed to draw any pattern as they liked and clicked as many click-points as they wanted. They believed that this

would provide tighter security. However, from the researcher's point of view, this may also lead to less memorability.

This study has proven that graphical recovery has potential to be implemented more widely in the future. Future work will focus on the mechanism of control to be provided in graphical recovery, in order to balance the usability and security of graphical method.

**Acknowledgments** The authors wish to thank USIM for funding this research. This research is funded under the USIM grant scheme with reference number of PPP/FST/SKTS/30/13612.

## References

1. Monrose, F., Reiter, M.K.: Graphical Passwords. Human Centered Systems Group. Department of Computer Science, University College London, London (2005)
2. Biddle R., Chiasson, S., Oorschot, P.C.: Graphical Passwords: Learning from the First Twelve Years. (2010)
3. Ray, P.P.: Ray's scheme: graphical password based hybrid authentication system for smart hand held devices. J. Inf. Eng. Appl. **2**(2) (2012)
4. Standing, L., Conezio, J., Haber, R.: Perception and memory for pictures: single-trial learning of 2500 visual stimuli. Psychon. Sci. **19**(2), 7374 (1970)
5. Standing, L.: Learning 10,000 pictures. Q. J. Exp. Psychol. **25**, 207–222 (1973)
6. Jali, M.Z.: A Study of Graphical Alternatives for User Authentication. School of Computing and Mathematics, Faculty of Science and Technology, University of Plymouth (2011)
7. Passfaces. http://www.realuser.com/personal/index.htm
8. Dhamija, R., Perrig, A.: Déjà Vu: a user study using images for authentication. In: 9th USENIX Security Symposium (2000)
9. De Angeli, A., Coventry, L., Johnson, G., Renaud, K.: Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. Int. J. Hum. Comput. Stud. **63**(1–2), 128–152 (2005)
10. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N.: PassPoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum. Comput. Stud. **63**(1–2), 102–127

http://www.springer.com/978-3-319-17397-9

Pattern Analysis, Intelligent Security and the Internet of Things

Abraham, A.; Muda, A.K.; Choo, Y.-H. (Eds.)

2015, X, 359 p. 67 illus., Softcover
ISBN: 978-3-319-17397-9