International Journal of Engineering & Technology, 7 (4.31) (2018) 400-407

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Usability Evaluation of Image and Emojis in Graphical Password

Nur Syabila Zabidi[1]*, Noris Mohd Norowi[2], Rahmita Wirza O.K. Rahmat[3]

Universiti Putra Malaysia
**Corresponding author E-mail: nursyabilazabidi@gmail.com*

Abstract

This paper presented user preferences in applying image and emojis use in graphical password authentication application. There is generally lack of two-factor authentication (2FA) approach in mobile devices. A preliminary study and a user study (N=30) have been conducted to investigate on usability and security issues. Both of the studies revealed the method of applying picture superiority effect to enhance memorability of graphical password.

Keywords: *smartphones; authentication; graphical password; usability;*

1. Introduction

HCI is turning into core components of the gadget development process to improve and decorate machine services to fulfill users' desires and necessities. With the development of smartphones and mobile network, people tend to store all the important information in mobile devices. The current infrastructure suffers from security vulnerabilities [1].

Human-Computer Interaction and Security, also referred to as Usable Security, is a relatively new area in the field of Computing Science combining: Human-Computer Interaction (HCI) and Computer Security. As to be said, "A chain is only as strong as its weakest link." This chain is referred to the human where to achieve high security in human computer interaction, human should play the main role. [2].

In that case, there is a need to protect and secure the personal information within smartphones. This protection is known as authentication. Generally, user authentication is a process of verifying identity of a user. It can be categorized into knowledge-based (password/PIN), possession based (certificate/card) and biometric based (finger/iris scan/face) [3].

Authentication evolves from Single Factor Authentication (SFA) to Two-Factor Authentication (2FA). SFA includes only one factor used to authenticate the subject [4]. An alternative passcode other than PIN is required to enhance the security of 2FA when creating the password [5].

One study has shown that memorability is the common cause of forgetting password [6]. The definition of memorability can be explained as ease of remembering a specific system for the purpose of enabling the casual user to log into the system back [7]. Despite of scoring poor in terms of memorability, passwords can be said as the almost universal authentication mechanism [8]. Typically, a text password consists of ASCII characters. Too simple a password increases the risks of being hacked. However, passwords which are too complicated are harder to be recalled. In terms of ease of use and memorability issues, text-based password is not really recommended because it is difficult to legitimate users and hard to recall [9].

Consequently, alternative technologies such as the use of card, tokens, biometric, are slowly replacing the use of passwords. As a matter of fact, biometric-based authentication also faces the issues of security and usability. For instance, Derawi has concluded that the technical challenges arise in biometric method, such as bias lighting conditions and unstable sample collection environment [10]. Klíma et al. also believe that for a number of applications in certain medical conditions, biometric authentication such as the finger or retinal scanning is not possible [11]. In the context of improving the memorability of passwords, and promoting users to practice safe authentication methods, this study will propose graphical password as a possible alternative to the traditional text passwords.

Graphical password use images as password to provide an alternative for text-based password which is difficult for users to memorize characters [12]. For over a century, psychology research have recognized the human mind's seemingly superior reminiscence for recognizing and recalling visual data in region of verbal or textual truth [13]. This is called Picture Superiority Effect (PSE) [12]. Images can be referred to a presentation of perceptual features that are being observed by the user [14]. For these reasons, other alternatives are certainly needed, and one of the methods that can be applied is the use of graphical password.

This study will implement a measurable metrics consists of usability and security metrics in order to provide basic specification and analysis of the proposed system. This study will measure on effectiveness in usability metrics and memorability in security metrics accordingly. This paper presents the findings of a preliminary study between single factor authentication (SFA) and two-factor authentication (2FA) and a user study of prototype. The goal is to gather and analyze user requirements for the purpose of designing graphical password authentication application for smartphones. The paper is organized as follows: Section 2 provides the related works of smartphones and mobile devices, user authentication, knowledge-based authentication, picture superiority effect, usability and security. Section 3 discusses preliminary study method and results. Section 4 reports on how the user study is conducted. While Section 5 presents discussion from user study. Finally, Section 6 concludes the work and highlights a direction for future research.

2. Related Works

2.1. Smartphones and Mobile Devices

Mobile phones are expected to be in the hands of 66% of the world's population by 2022, with mobile device usage slated to reach 5.5 billion users by then [41]. In Malaysia, the number of smartphone users was estimated to reach 19.9 million in 2017 [42]. Given the statistical percentage of mobile devices usage nowadays, it is important to establish the core usefulness of mobile devices in implementing graphical password.

One study has shown that smartphones is a small, portable and powerful device that can serve users with multiple task [15]. The NIST Special Publication 800-124 defines mobile devices: by having a (a) "small form factor", by providing (b) "at least one wireless network interface", by having a (c) "local built-in (non-removable) data storage", by using (d) "an operating system that is not a full-fledged desktop or laptop operating system", and by supporting (e) "applications available through multiple methods" [16]. Abate et al. defines smartphones and mobile devices as an equipment with progressive sensors such as high-resolution cameras, digital compasses, gyroscopes, accelerometers and positioning systems [17]. Consequently, a great deal of research has focused on the technology of mobile devices solely. This study defines the criteria of a mobile device as: (1) a visual display with a touch screen, (2) are primarily used to manage personal data and (3) focus on smartphones

The current study examines the usability and security part of the smartphones: authentication. This area had been less neglected until recently security has become an essential issue in protecting data privacy, as the majority of literature on mobile devices has focused on the technology side of mobile devices and smartphones. Abate et al. reported that users often declined to use passwords or other methods of securing their mobile devices [17]. To investigate the usability and security part of smartphones' authentication, the different methodologies must be examined.

2.2 User Authentication

Single factor authentication (SFA) is a means of verifying customer identity. The classic example is a PIN or password [18]. It was rated significantly less usable than two-factor authentication (2FA), contradicting the commonly-held assumption that increased security leads to poorer usability.

Two Factor Authentication, also known as 2FA, two step verifications or TFA (as an acronym), is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that user has only on them. For example, a piece of information only they should know or have immediately to hand - such as a physical token [43]. An example of this mechanism is Google 2- step Verification. This verification works by providing two steps of authentication. First, the user will enter the password. Second, a code will be sent to user's phone via text, voice or mobile app. The advantage of this verification is that the account will be protected both on the user's knowledge-based password and possession-based phone [44].

The multifactor authentication market was valued at USD 5.22 billion in 2016 and is expected to reach USD 12.51 billion by 2022, at a CAGR of 15.52% [45]. The interest in multi-factor authentication has been on an ascending trend, especially towards the second part of 2017. Despite being the new authentication hack target for attackers, multi-factor authentication is expected to continue its growth through 2018 [45]. Given the trending that multifactor authentication is expected to continue growing, it is relevant to create an understanding of user authentication in the context of multifactor.

User authentication is the verification of an active human-to-machine transfer of credentials required for confirmation of a user's authenticity. One study has defined that user authentication as a process to verify identity of a user. They categorized the authentication methods as knowledge-based (password/PIN), possession based (certificate/card) and biometric based (finger/iris scan/face) [3]. Consequently, a great deal of research has focused on the contexts of the authentication scheme itself, rather than investigating on how human reacts to different authentication scheme.

The current study analyzes the human behavior in different authentication based on context given [19]. The categorization of user authentication is further supported by the research work made by Liu et al.,in 2015, where they divided also authentication into three different types, knowledge-based, token-based and biometric-based [20].

In view of these categorization, it can be concluded that knowledge-based authentication is something a user knows such as password or PIN. On the other hand, possession-based or token-based authentication is something a user has. For example, a certificate or card. While biometric-based authentication is something a user is, such as iris scan, fingerprint and face recognition.

Table 1 compares the definition and examples for each category of user authentication. This section discusses knowledge-based authentication method as the main issue. By seeking problems of traditional password method, this section specifically emphasizes on past and present studies of password method in order to seek possible alternative solutions.

Table 1: The Categorization of User Authentication

Category	Definition	Example
Knowledge-based	Something a user knows	Password, PIN
Possession-based	Something a user has	Certificate, Card
Biometric-based	Something a user is (Physical or Behavioural)	Fingerprint, Iris Scan, Face

2.3 Knowledge-Based Authentication

Rogowski et al. define knowledge-based methods as some sort of user knowledge which require some effort to remember because it depends on user memory. For example, passwords, PINs, pattern locks and graphical passwords are all depending on user to do the authentication process [21]. Password faces multiple problems and it arises largely from limitations of human's memory. User must be able to memorize a bunch of strings during authentication which in result, tend to forget their passwords [22]. There is an accepted theory, dual-coding theory, which explaining word-based and image-based memory are represented differently in human's mind [14]. This is because user tend to have multiple accounts where it requires different credentials and passwords. This situation increases the password problem.

According to Grady et al., it is important to survive in visual environment by memorizing various aspects of a picture [23]. This statement further supported by Paivio in his book, where he stated that *"Imagery is somewhat ironic that imagery was largely neglected throughout the reign of dualistic experimental psychology that laid the assumptive foundations of cognitivism, which accepted imagery as a respected visitor."*[24]. Adequate security must be provided in order to achieve successful authentication system. At minimum, a proposed authentication system should be able to identify common attacks and satisfy usability requirements, such as efficiency and memorability[7].

2.4 Password

Early work by Renaud and De Angeli stated that the almost universal authentication mechanism is passwords, despite of poor memorability [8]. In 2013, Andriotis et al. stated that text-based password exposed for the attackers in terms of security and it is hard to remember [9].

Several researchers addressed the issues of usability and security which can be found in the use of password method. Humans feel difficult when it comes to memorize a bunch of strings which do not have any related meanings. To ease their way of remembering passwords, they often organize their less secure password by relating them with everyday things [8]. This led to the problems of security in password method. In 2014, Andriotis et al. stated that alphanumeric and textual passwords are exposed to dictionary attacks. The statement by Renaud and De Angeli in 2004 had also been supported by claiming that easy and non-complex passwords are the most chosen method in authentication process [25]. All these studies can further be justified that the reason for not using password method as the main authentication in this study.

2.5 PIN

Early in 2005, Clarke and Furnell has defined PIN as an authentication approach that depends on some sort of users' knowledge. It consisted of 4 – 8 digit Personal Identification Numbers (PINs) [26]. By considering PIN to be used in smartphones, Andriotis et al supported that in most cases PINs are used as phone lock mechanisms [9]. PINs or patterns alone may not be able to provide sufficient protection for the information stored on the device.

2.6 Pattern Lock

Android Pattern-Lock is a two- dimensional square grid of nine nodes that serves as a drawing canvas. The smartphone user has to form a shape that links between four and nine nodes [25]. To unlock device, people will have to swipe their finger on touch screen. It is called Android's pattern lock. Unfortunately, this action leaves behind smudges.

2.7 Graphical Password

Graphical password in smartphones is being introduced into mobile authentication at an increasing rate. Smartphones and mobile devices equipped with progressive sensors such as high-resolution cameras, digital compasses, gyroscopes, accelerometers, positioning systems provide a wide platform for researchers to enhance built in functions of these devices [17]. In 2015, Mayron described smartphones as small, portable and powerful device that serve users with multiple task [15]. This study classifies graphical password into three categories: recall-based, recognition-based, and cued-recall based [28].

Recall-based graphical password systems or *drawmetric* system refers to the action of recalling and reproducing a secret drawing [29]. This system allows users to draw password on blank canvas or a grid [28]. Recall is a difficult memory task as it requires retrieval without memory prompts.

The second category is recognition-based systems, also known as *cognometric* system [29]. It is concerning with memorizing a portfolio of images (faces, art, objects, etc)during password creation, and recognizing images among decoys to log in [28].

Another category is, cued-recall systems. This system requires user to remember and target specific locations within an image. It also called *locimetric* system [29]. This study applied the feature of clicking certain areas on image to able the users to accurately retain visual memories of objects they previously attended.

2.8 Picture Superiority Effect

The Picture Superiority Effect (PSE) is the well-established experimental finding in retrospective memory research that people exposed to stimuli in picture format perform better on explicit retrospective memory tests than people exposed to the same stimuli in word format. The picture superiority effect suggests that you would remember to complete more tasks with the picture to-do list [30]. In other words, graphical password method is more likely to be remembered experientially if presented as pictures rather than words [31].

2.8 Usability and Security

The definition of usability is the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (ISO 9241-11) [32].

According to Bevan, standards related to usability can be divided into the use of the product, the user interface and interaction, the process used to develop the product, and the capability of an organization to apply user centered design [32]. Further definition of usability can be described by Kainda et al. where they have concluded usability in one solid sentence, usability consists of effectiveness, efficiency, satisfaction, learnability, and memorability [33].

Another domain that will be described is security. Security is concerned with the study of how security information should be handled in the user interface and how security mechanisms and authentication systems themselves should be ease of use [34]. Kainda et al. stated that definitions of security are depends on the types of attackers [33].

Thus, in order to fulfil the needs in human computer interaction areas, there are three main contributions should be provided: a) implement the picture superiority effect (PSE), b) offer usable interaction capabilities (e.g. clicking on image on touch screen, dragging emojis), and c) provide adequate security for authentication scheme.

3. Preliminary Study

In order to understand user requirements for two-factor authentication, a preliminary study was conducted. The main aims of this study are as follows: a) to gather and analyze user requirements for the purpose of designing graphical password authentication application for smartphones; b) to understand user requirements for two-factor authentication.

In this preliminary study, 8 undergraduates and postgraduates' students (4 males and 4 females) from different courses of Universiti Putra Malaysia were voluntarily recruited. Age range of the sample was 21-30 years old (mean = 1.6 years and sd = 3.5 years). Participants were recruited to do the evaluation tasks for 20 minutes. Four smartphone-based prototype application Emoji Lock Screen, Pass-Go, MIBA (Multitouch image-based authentication on smartphones) and TAPI (Touch–screen authentication using partitioned images) were provided. Pass-Go, MIBA and TAPI were implemented by using GraphicalPassword.apk. project where it consists of four different graphical password schemes: MIBA, Pass-Go, TAPI and UYI. All these four schemes were chosen to facilitate replication of research results and encourage the use of graphical password schemes[35].

The study was carried out in the laboratory of Faculty of Computer Science. One experimenter evaluated the task by conducting briefings before and after the tasks. A consent form was given to each participant and a practice session was administrated. A questionnaire was provided to the participants after the evaluation tasks. The information requested included the participants' demographic, their current practice of smartphone authentication and usability and security awareness of graphical password.

3.1. Task Procedure

Prior to the evaluation study, a simple training task was conducted as a warm-up session to familiarize themselves with the features and functions of the system for at least 5 minutes. The training session included steps on how to create password and log into the application.

For the first task, the participants were required to use Emoji Lock Screen application (Single Factor Authentication – SFA) (Fig. 1). This application was developed by EmojiArtStudio with size of 14MB [46]. The main feature of this Android application is users can increase their privacy security by changing default phone lock screen with smiley. For Emoji lover, they can also set Emoji as PIN password in unlocking phone. Besides, this application allows users to set their favorite photos on their lock screen.

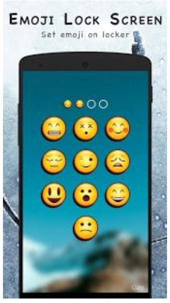


Fig. 1: Emoji Lock Screen

The second task is proceeded with Pass-Go application (Single Factor Authentication – SFA) (Fig. 2). This application is a grid-based scheme which requires a user to select (or touch) intersections, instead of cells, as a way to input a password [36]. Participants were asked to draw their desired pattern in the designated grid. The pattern has to contains six line segments and/or dots.

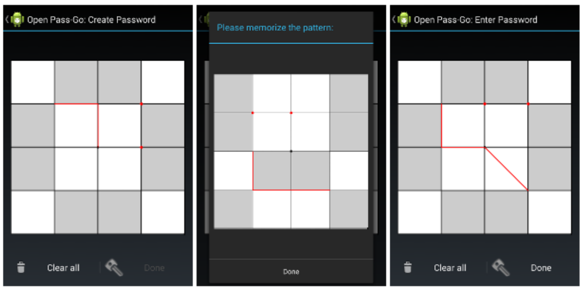

Open Pass-Go: Create Password
Clear all
Done
Please memorize the pattern:
Done
Open Pass-Go: Enter Password
Clear all
Done

Fig. 2: Pass-Go

The third task is by using MIBA (Multitouch image-based authentication on smartphones) (Two-Factor Authentication – 2FA) (Fig. 3). Participants were required to mark multiple points on an image, where it can be consisted of multiple rounds. MIBA resolves the image chosen in the second layer of authentication by using image background as cues [37].

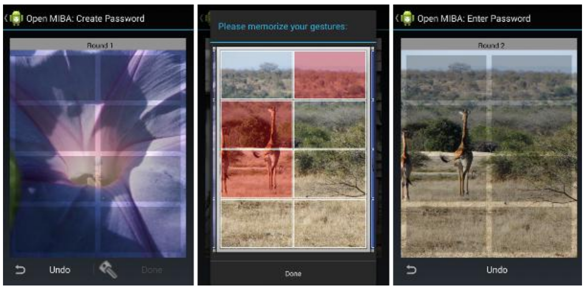

Open MIBA: Create Password
Round 1
Undo
Done
Please memorize your gestures:
Done
Open MIBA: Enter Password
Round 2
Undo

Fig. 3: MIBA

For the last task, the participants were required to use TAPI (touch–screen authentication using partitioned images) (Two-Factor Authentication – 2FA) (Fig. 4). Participants were required to select a correct partition of the image in a proper sequence. TAPI increases security by having the user not only enter one of 16 images in proper sequence, but also to select a correct partition of the image (in Fig. 4, the partitions of each image are top, right, bottom, and left as marked by the red Xs).

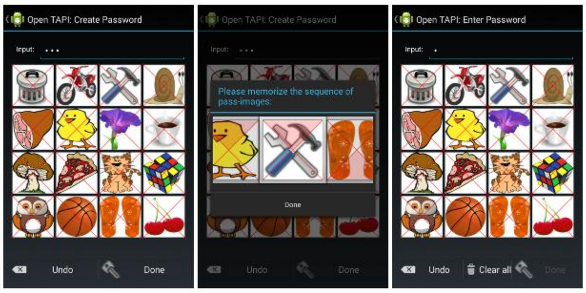

Open TAPI: Create Password
Input:
Undo
Done
Open TAPI: Create Password
Please memorize the sequence of pass-images:
Done
Open TAPI: Enter Password
Input:
Undo
Clear all
Done

Fig. 4: TAPI

All of these four tasks were conducted in the same way as stated here. First, the participants positioned themselves with the mobile device located on the table. Next, the participants were required to read the instructions provided by the experimenter. Then, participants needed to alert the experimenter when they were ready to do the experiment. At this point, the stopwatch started, and the video began recording. The users were asked to complete the tasks and informed the experimenter once they had successfully completed this first task. The time were recorded, and the video recording stopped. Upon completing the four tasks, each participant was required to complete the questionnaire; information included the participant's demographic background and the participant's current practice of smartphones' authentication method and authentication scheme preferences.

3.2 Results

A list of statements requiring agreement of level were asked to the participants in order to gain basic knowledge and perception towards single factor authentication. First, in terms of the easiness of understanding how single factor authentication works, 75% of the participants strongly agreed that single factor authentication is easy to understand (Fig. 5). Similarly, by determining the easiness of creating password in single factor authentication, 88% of the participants acknowledged this fact (Fig. 6).

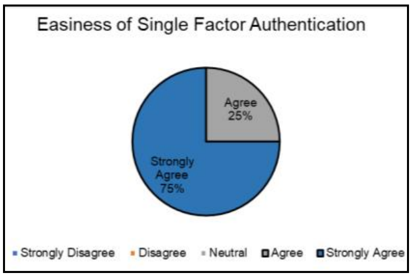


Fig. 5: Easiness of Single Factor Authentication

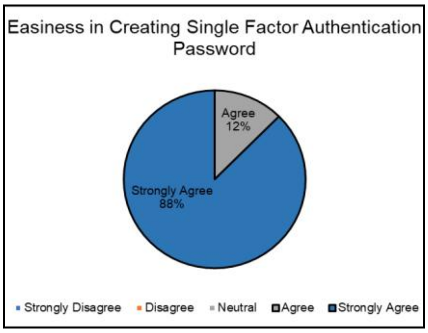


Fig. 6: Easiness in Creating Single Factor Authentication Password

On the other hand, the pie chart shows how respondents rated the easiness of remembering password in two-factor authentication compared to single factor authentication. As might be expected, it is clear from the data that two-factor authentication password are easier to be remembered than single factor authentication password. Referring to the statements of gaining their preferences in remembering two-factor authentication password, 25% of the participants agreed, being in neutral state, and disagreed to this statement distinctively (Fig. 7). There were also considerate numbers of 38% participants strongly agreed on two-factor authentication is more secured to single factor authentication (Fig. 8).

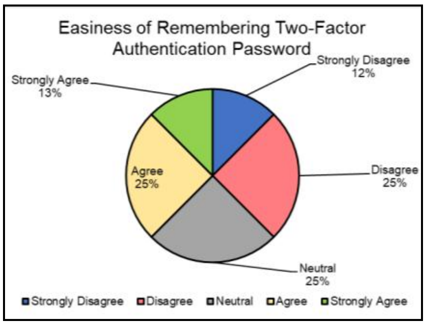


Fig. 7: Easiness of Remembering Two-Factor Authentication Password

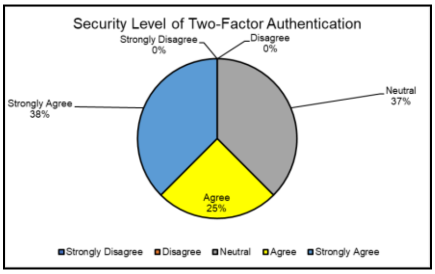


Fig. 8: Security Level of Two-Factor Authentication

Based on these results, it can be concluded that in terms of usability, users preferred single factor authentication compared to two-factor authentication, mainly because on the easiness of creating and remembering password. In contrast, in terms of security, two-factor authentication stands out to be the preferred authentication method. Therefore, this study will implement the use of two-factor authentication scheme.

4. User Study

SecureImageEmoji, a two-factor authentication mechanism was developed. In the first round of authentication, users need to create a graphical password by choosing an image from the six images provided. The process followed by choosing and dragging four selected emojis to the image selected before. There are a total number of 30 individuals who participated in this study (13 females, 17 males), in the range of age from 21 to 30 (m = 1.6; sd =13.4). Participants had interaction experience with smartphones. The participation from users were voluntary and all users consented their interactions with the prototype to be documented.

4.1 Task Procedure

In order to conduct the study in quiet environment, the experimenters held the study in a laboratory of Faculty of Computer Science, and each participant were asked to take a seat with camera mounted at the above of the smartphone approximately a 30cm distance from the display (Fig. 9). At the beginning, the participants were introduced to the procedure of the study, having completely familiarized themselves with how the prototype works. To generate a graphical password, the participants were required to register first and log into the prototype. Firstly, participants had been required to pick out an image from a grid of 6 pictures (Fig. 10). Then followed by selecting and dragging four desired emojis onto desired area on previously chosen image (Fig. 11). At the end of the study, participants were provided with questionnaires to gain their experience with prototype, and the strategies they implemented when selecting image and emojis.

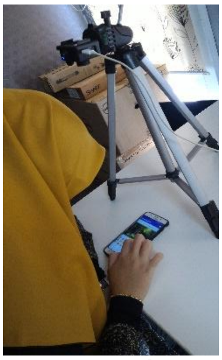


Fig. 9: User Study Setup

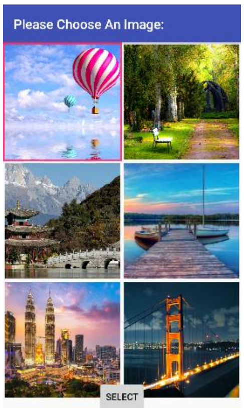
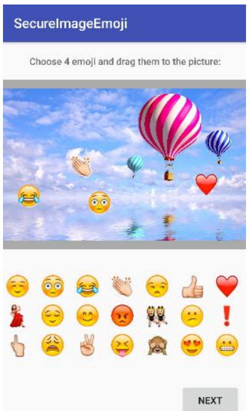


Fig. 10: Interface of Image Selection (1st Factor)



Choose 4 emoji and drag them to the picture:

Fig. 11: Interface of Emojis Selection (2nd Factor)

4.2 Results

According to Harrison et al., efficiency can be measured in a number of ways, such as the time to complete a given task, or the number of keystrokes required to complete a given task [7]. Efficiency of password was measured as the proportion of participants who logged into the prototype in a certain of time. Details of time to sign up and time to login into prototype were captured in this study.

The mean time when signing up a password for the experiment was at 86.49 seconds. This can be explained by three main factors: a) The time-consuming nature of the task put off a lot of participants. To complete the study, participants had to choose one image as background password and drag four emojis onto the previously chosen image; b) 23% of the participants reported that it was difficult to determine emojis' location on image (Fig. 12). It was probably because there were no specific cue or grid on image to be provided to users to put on their selected emojis [28]; c) 30% of the participants stated that they had difficulties in dragging and dropping the emojis, probably because lack of basic experience in drag and drop activity, which requires user to long press a certain object then drag (Fig. 12). Fig. 13 illustrates the mean value for time to sign up between gender. According to the bar chart, male participants had an average time of 76.35 seconds in registering their password (Fig. 13). Female participants also reported to be quite similar as male participants with the mean value of 72.62 seconds.

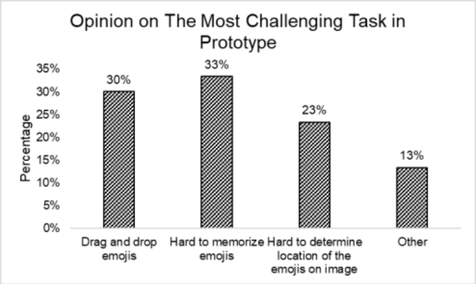


Fig. 12: Opinion on The Most Challenging Task in Prototype

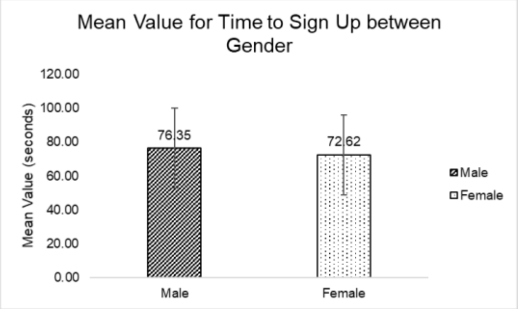


Fig. 13: Mean Value for Time to Sign Up between Gender

The overall time when logging in the prototype for the experiment was at 34.6 seconds. This can be explained by this statement, where 30% of the male participants and 27% of the female participants had successfully logged in to the prototype at the first attempt (Fig. 14). This is primarily because the picture superiority effect of images and emojis helped them in memorizing their password [30]. Further analysis on logging time can be supported by the total mean value by gender. The bar chart shows male participants had the average time of 29.71 seconds when logged into the prototype. While female participants stood out to have the mean value of 30.15 seconds in logging in the prototype (Fig. 15). It can be concluded that logging into the prototype would be much faster as the participants were able to recall all related image and emojis.

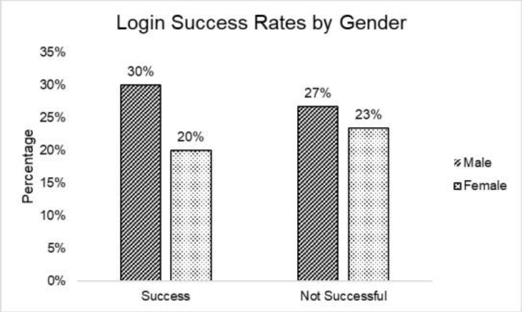


Fig. 14: Login Success Rates by Gender

Apart from that, a considerable number of participants stated that they used the strategy of remembering images that have picture superiority effect, primarily because the images provided are clear and attractive. In keeping with this superiority effect, humans have a significant, nearly limitless, visible memory, and images tend to be remembered some distance higher and for longer than words [29]. The pie chart shows the appearance of image plays an important part in determining graphical password. There are 50% of the participants strongly agreed the images used in this prototype are clear and attractive. However, the percentage decreases at 3% where the participants disagreed on this statement (Fig. 16). This is primarily because the participants preferred to choose their own images from gallery. For example, a participant stated *"please provide a picture that user can relate the emoji with that picture, so that people can memorize easily."*. This statement can further be supported by the results from this bar chart (Fig. 17). 60% of the participants preferred to choose image on their own. As it can be said that users did not know how to select images as password as there are no specific strategy given to them, hence the practical strategy was suggested.

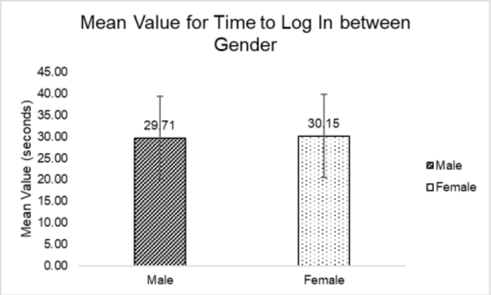


Fig. 15: Mean Value for Time to Log In between Gender

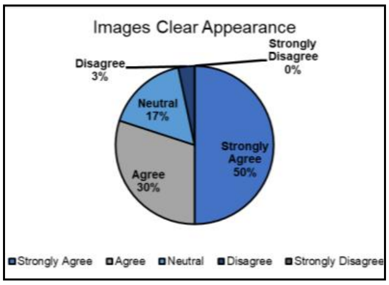


Fig. 16: Images Clear Appearance

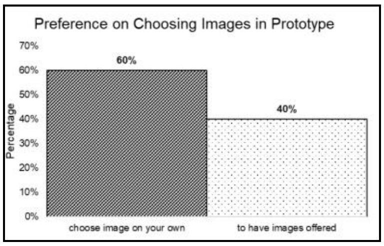


Fig. 17: Preference on Choosing Images in Prototype

Of the 30 participants that were recruited in this study, 45% of them stated that the emojis provided are clear and attractive (Fig. 18). This statement further supported by collecting the participants' opinion on what kind of emojis are useful for their own method in memorizing them. For instance, several participants stated *"daily emojis like love, smile and thumbs up", "funny and attractive emojis", "color and expression of emojis",* etc to support their method of determining emojis selection.

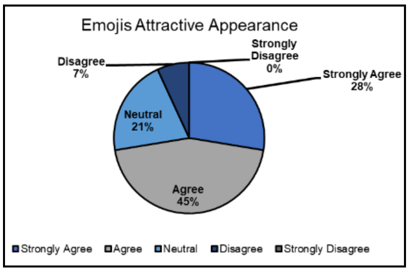


Fig. 18: Emojis Attractive Appearance

Apart from this, the results from this bar chart shows 80% of the participants love to have emojis offered to them, while there are only 20% of them preferred to choose emojis on their own (Fig.

19). The reason behind this is that emoji are part of the Unicode standard, and special emoji keyboards are available on all major mobile platforms [38]. According to Seitz et al., there are currently around 2600 different emojis as part of the Unicode standard [39].

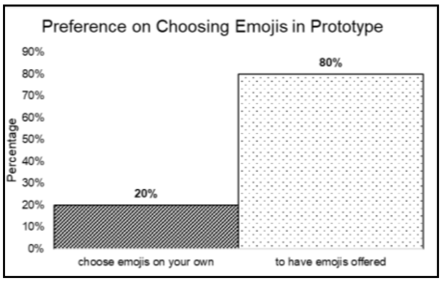


Fig. 19: Preference on Choosing Emojis in Prototype

To conclude this, further improvement on this prototype should include a subset of emojis ("people" category, "nature", "foods", "activity", "places", "objects", and "symbols") to study the effect of distinctiveness on memorability [39] since the majority of the participants responded positively to have emojis offered to them.

5. Discussion

The main findings of the paper discuss the use of image and emojis in graphical password has affected: (1) graphical password memorability; (2) time to sign-up; and (3) time to login.

Finding 1 – Picture superiority effect [30]. Picture superiority effects enhances the graphical password memorability. It can be explained as "Images are presented in a method of retaining visual features and are assigned meaning of what has been observed directly" [28]. The choices of images and emojis offered to the participants were clear and attractive.

Finding 2 –Determining the location of emojis in the image is the most difficult task during signing up password. Results reveal that the two problems (determine location of emojis and drag, drop emojis) are the least productive in creating a graphical password in this prototype. For the problem of determining location of emojis on image, a grid-based discretization on image should be provided [28], which prevents them for locating the emojis on image. However, the difficulty in dragging and dropping emojis prevents them for locating correctly on image.

Finding 3 – Measures in efficiency is the most usable in terms of graphical login. By linking emojis to the image background, it helps the participants to memorize their password. Regarding the emojis, variety of emojis helps the users to construct their series of emojis choices [40].

Overall, the study has shown that drag and drop activity prevents the users to log into the prototype quickly, which directs into a new solution when using graphical password.

6. Conclusion

This paper enhances graphical password authentication mechanisms by understanding users' preferences from the view of picture superiority effect and relation between security and usability. Regarding theory, the study stated that picture superiority effect has directly affect usability aspects in graphical password. Regarding application, the study revealed that the application should be enhanced on the usability issues. For example, the images and emojis used or the drag and drop activities may influence usability and security in different ways, which is something this study plans to explore in future work.

References

[1] B. Horne, "Humans in the loop," *IEEE Secur. Priv.*, vol. 12, no. 1, pp. 3–4, 2014.

[2] M. M. Eloff and J. H. P. Eloff, "Human Computer Interaction: An Information Security Perspectives," in *Security in the Information Society: Visions and Perspectives*, M. A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan, Eds. Boston, MA: Springer US, 2002, pp. 535–545.

[3] S. Srivastava and P. S. Sudhish, "Continuous multi-biometric user authentication fusion of face recognition and keystoke dynamics," in *2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2016, pp. 1–7.

[4] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[5] A. Kemshall, "Why mobile two-factor authentication makes sense," *Netw. Secur.*, vol. 2011, no. 4, pp. 9–12, 2011.

[6] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[7] R. Harrison, D. Flood, and D. Duce, "Usability of mobile applications : literature review and rationale for a new usability model," *Int. J. Mob. Hum. Comput. Interact.*, vol. 6, no. 1, pp. 54–70, 2014.

[8] K. Renaud and A. De Angeli, "My password is here! An investigation into visuo-spatial authentication mechanisms," *Interact. Comput.*, vol. 16, no. 6, pp. 1017–1041, 2004.

[9] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz, "A pilot study on the security of pattern screen-lock methods and soft side channel attacks," *ACM WiSec*, p. 1, 2013.

[10] M. O. Derawi, "Biometric options for mobile phone authentication," *Biometric Technol. Today*, vol. 2011, no. 10, pp. 5–7, 2011.

[11] M. Klíma, A. J. Sporka, and J. Franc, "You are who you know : user authentication by face recognition," *Proc. 7th ICDVRAT with ArtAbilitation, Maia, Port.*, pp. 97–102, 2008.

[12] S. Kumar Jena, "Graphical User Authentication," no. May, 2013.

[13] T. O. Nelson, G. Greene, B. Ronk, G. Hatchett, and V. Igl, "Effect of multiple images on associative learning," *Mem. Cognit.*, vol. 6, no. 4, pp. 337–341, 1978.

[14] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical Passwords : Learning from the First Twelve Years," *Security*, vol. V, pp. 1–43, 2009.

[15] L. M. Mayron, "Biometric Authentication on Mobile Devices," *2015 IEEE Secur. Priv.*, vol. 13, no. 3, pp. 70–73, 2015.

[16] M. Souppaya and K. Scarfone, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," *NIST Spec. Publ. 800-124, Revis. 1*, pp. 1–30, 2013.

[17] A. F. Abate, M. Nappi, and S. Ricciardi, "Smartphone enabled person authentication based on ear biometrics and arm gesture," in *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2016, pp. 003719–003724.

[18] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Comput. Secur.*, vol. 30, no. 4, pp. 208–220, 2011.

[19] E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie, "A Comparative Usability Study of Two-Factor Authentication," in *Proceedings 2014 Workshop on Usable Security*, 2014.

[20] C. L. Liu, C. J. Tsai, T. Y. Chang, W. J. Tsai, and P. K. Zhong, "Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone," *J. Netw. Comput. Appl.*, vol. 53, pp. 128–139, 2015.

[21] M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, and M. Adamski, "User Authentication for Mobile Devices," in *Computer Information Systems and Industrial Management: 12th IFIP TC8 International Conference, CISIM 2013, Krakow, Poland, September 25-27, 2013. Proceedings*, K. Saeed, R. Chaki, A. Cortesi, and S. Wierzchoń, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 47–58.

[22] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords," *Proc. 2005 Symp. Usable Priv. Secur. - SOUPS '05*, pp. 1–12, 2005.

[23] C. L. Grady, A. R. McIntosh, M. N. Rajah, and F. I. M. Craik, "Neural correlates of the episodic encoding of pictures and words," *Proc. Natl. Acad. Sci.*, vol. 95, no. 5, pp. 2703–2708, Mar. 1998.

[24] A. Paivio, *Mind and Its Evolution*, no. 2007. Routledge, 2006.

[25] P. Andriotis, T. Tryfonas, and G. Oikonomou, "Complexity metrics

and user strength perceptions of the pattern-lock graphical authentication method," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8533 LNCS, pp. 115–126, 2014.

[26] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones - A survey of attitudes and practices," *Comput. Secur.*, vol. 24, no. 7, pp. 519–527, 2005.

[27] Y. Li, J. Yang, M. Xie, D. Carlson, H. G. Jang, and J. Bian, "Comparison of PIN- and pattern-based behavioral biometric authentication on mobile devices," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2015–Decem, pp. 1317–1322, 2015.

[28] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical Passwords : Learning from the First Twelve Years," *ACM Comput. Surv.*, vol. 44, no. 4, pp. 1–43, 2012.

[29] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 128–152, 2005.

[30] Y. Ma, "Can More Pictures Bring More Readership?: An Examination of the 'Picture Superiority Effect' in the News Consumption Process," *Procedia - Soc. Behav. Sci.*, vol. 236, no. December 2015, pp. 34–38, Dec. 2016.

[31] P. Dunphy, "Usable, Secure and Deployable Graphical Passwords," no. November, p. 189, 2012.

[32] N. BEVAN, "International standards for HCI and usability," *Int. J. Hum. Comput. Stud.*, vol. 55, no. 4, pp. 533–552, 2001.

[33] R. Kainda, I. Flechais, and A. W. Roscoe, "Security and usability: Analysis and evaluation," *ARES 2010 - 5th Int. Conf. Availability, Reliab. Secur.*, pp. 275–282, 2010.

[34] C. Braz and J.-M. Robert, "Security and usability," *Proc. 18th Int. Conf. Assoc. Francoph. d'Interaction Homme-Machine - IHM '06*, no. January, pp. 199–203, 2006.

[35] F. Schaub, M. Walch, B. Könings, and M. Weber, "Exploring the design space of graphical passwords on smartphones," *Proc. Ninth Symp. Usable Priv. Secur. - SOUPS '13*, p. 1, 2013.

[36] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Secur.*, vol. 7, no. 2, pp. 273–292, 2008.

[37] D. Ritter, F. Schaub, M. Walch, and M. Weber, "MIBA: Multitouch Image-Based Authentication on Smartphones," *CHI '13 Ext. Abstr. Hum. Factors Comput. Syst.*, pp. 787–792, 2013.

[38] M. Golla, D. Detering, and M. Dürmuth, "EmojiAuth: Quantifying the Security of Emoji-based Authentication," *Proc. Usable Secur. Mini Conf.*, pp. 1–13, 2017.

[39] T. Seitz, F. Mathis, and H. Hussmann, "The Bird is the Word: A Usability Evaluation of Emojis inside Text Passwords," *Proc. 29th Aust. Conf. Human-Computer Interact. (OzCHI 2017)*, p. 9, 2017.

[40] M. Belk, A. Pamboris, C. Fidas, C. Katsini, N. Avouris, and G. Samaras, "Sweet-spotting security and usability for intelligent graphical authentication mechanisms," *Proc. Int. Conf. Web Intell. - WI '17*, pp. 252–259, 2017.

[41] L. Fullerton, "Global mobile device usage is expected to reach more than 5.5bn users by 2022," 20 July 2017. [Online]. Available: http://www.thedrum.com/news/2017/07/20/global-mobile-device-usage-expected-reach-more-55bn-users-2022. [Accessed 14 March 2018].

[42] "Number of smartphone users in Malaysia from 2015 to 2022 (in millions)*," [Online]. [Accessed 14 March 2018].

[43] "What is 2FA?," A Shearwater Group plc Company , [Online]. Available: https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm. [Accessed 14 March 2018].

[44] "Stronger security for your Google Account," [Online]. Available: https://www.google.com/landing/2step/index.html#tab=how-it-protects. [Accessed 14 March 2018].

[45] "Multifactor Authentication Market by Model (Two-, Three-, Four-, and Five-Factor), Application (Banking and Finance, Government, Military and Defense, Commercial Security, Consumer Electronics, Healthcare), and Geography - Global Forecast to 2022," May 2017. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/multi-factor-authentication-market-877.html. [Accessed 14 March 2018].

[46] EmojiArtStudio, "Emoji Lock Screen," Google, 27 February 2018. [Online]. Available: https://play.google.com/store/apps/details?id=com.emoji.smiley.locker&hl=en. [Accessed 21 March 2018].