

PICTURE-BASED PASSWORD SCHEME

BY

SEOW YANG JIIN

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION SYSTEM (HONS)

BUSINESS INFORMATION SYSTEM

Faculty of Information and Communication Technology

(Kampar Campus)

MAY 2019

REPORT STATUS DECLARATION FORM

Title: _____

Academic Session: _____

I _____
(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

(Author's signature)

(Supervisor's signature)

Address:

Supervisor's name

Date: _____

Date: _____

PICTURE-BASED PASSWORD SCHEME

By

Seow Yang Jiin

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION SYSTEM (HONS)

BUSINESS INFORMATION SYSTEM

Faculty of Information and Communication Technology

(Kampar Campus)

MAY 2019

DECLARATION OF ORIGINALITY

I declare that this report entitled “**PICTURE-BASED PASSWORD SCHEME**” is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : _____

Name : _____

Date : _____

ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisor, Mr. Ku Chin Soon who has given me this bright opportunity to engage in picture-based password scheme project. It is my first step to establish a career in developing a graphical authentication system with mobile application. A million thanks to you.

To a very special person in my life, Aw Ming Yeh, for his patience, unconditional support and love, and for standing by my side during hard times. Finally, I must say thanks to my parents and my family for their love, support and continuous encouragement throughout the course.

ABSTRACT

This project is a developing a picture-based password scheme to prevent shoulder-surfing attacks. This proposed system is introducing a rules that their password image is clicking the direction of their real password image which set during registration phase. This proposed authentication scheme is using recognition-based which user is recognizing the image. This rules is simple and easy for user to memorize and yet the security is strong enough against shoulder-surfing attacks. Human are easier to memorize image compared to traditional text-based password in authentication system. This project will need to evaluate the capabilities of user's memorability in using the proposed system. Research will also be done to evaluate user in different categories such as duration of user login, times for successful login and user's difficulty in memorizing their password image. By comparing the proposed system with other existing authentication scheme is to find out the difference between them and compare which system is better and more resist to shoulder-surfing attack.

TABLE OF CONTENTS

TITLE PAGE	i
DECLARATION OF ORIGINALITY	ii
ACKNOWLEDGEMENTS	iii
ABSTRACT	iv
TABLE OF CONTENTS	v
LIST OF FIGURES	viii
LIST OF TABLES	xii
LIST OF ABBREVIATIONS	xiii
Chapter 1 Introduction.....	1
1.1 Project Inspiration.....	1
1.2 Problem Statements	3
1.3 Project Objective.....	4
1.4 Project Scope	4
1.5 Project Impact and Contribution.....	5
1.6 Chapter Summary	6
Chapter 2 Literature Reviews.....	7
2.1 Overview.....	7
2.2 Review on existing related works	7
2.2.1 ColorLogin.....	7
2.2.2 Pass-Matrix	10
2.2.3 Two Step Random Colored Grid	13
2.2.4 Falsification.....	15
2.2.5 Digraph substitution rules (DSR)	17
2.2.6 Secure Passface	22
2.2.7 Comparison Table among all system reviewed	24

Chapter 3 System Methodology	25
3.1 Project Development.....	25
3.2 Information Gathering (Data Collection).....	26
3.3 Project Verification Plans	26
Chapter 4 System Design	33
4.1 Design of picture-based authentication system.....	33
4.1.1 Registration	33
4.1.2 Login	34
4.1.3 Demo.....	35
4.2 System Architecture Design	36
4.3 Hardware and Software Requirements	37
4.4 Graphical User Interface Design.....	38
4.4.1 Home Page UI.....	38
4.4.2 Registration Process.....	39
4.4.3 Proposed algorithm	42
4.4.4 Login Process.....	50
4.4.5 Demo.....	54
4.5 Data Storage Design	55
Chapter 5 System Testing	56
5.1 First User Study	56
5.1.1 Procedure	56
5.1.2 Results from Survey Questionnaire	57
5.2 Second User Study.....	63
5.2.1 Procedure	63
5.2.2 Results Collected from Shoulder-surfing test Survey Form	64
5.3 Accuracy	73
5.4 Usability.....	74
5.5 Security Analysis against Shoulder Surfing Attack.....	81

Chapter 6 Discussion	82
Chapter 7 Conclusion	84
BIBLIOGRAPHY	85
APPENDICES	A-1
POSTER	B-1
PLAGIARISM CHECK RESULT	C-1
CHECKLIST FOR FYP2 THESIS SUBMISSION	D-1

LIST OF FIGURES

Figure Number	Title	Page
Figure 2.1.1	A group of chosen-color icons are displayed for user to set as his pass-icons	8
Figure 2.1.2	The icons displayed in login screen	8
Figure 2.1.3	A line of substitute icon replacement after user click its desired icon on that line	8
Figure 2.2.1	Pass-grid selection from 7x11 grid image	11
Figure 2.2.2	One-time login indicator	11
Figure 2.2.3	Graphical pass-image authentication where numbers scattered all over the grids	12
Figure 2.3.1	6x6 grid with pattern line enter by user	14
Figure 2.4.1	Registration	15
Figure 2.4.2	Type alphanumeric character from football team category	15
Figure 2.4.3	A random image categories (Pet)	16
Figure 2.5.1	User Interface of registration phase	17
Figure 2.5.2	Options for user to select his password image	17
Figure 2.5.3	A sample of user's password images	18
Figure 2.5.4	First password image for scenario 1	19
Figure 2.5.5	Second password image for scenario 1	19
Figure 2.5.6	Password image of scenario 2 which on the same vertical line	20
Figure 2.5.7	Password image of scenario 3 which on the same horizontal line	20

Figure 2.6.1	First login round of S-Passface	22
Figure 2.6.2	Second login round of S-Passface	23
Figure 3.1	System Development Life Cycle (SDLC)	25
Figure 3.3.1	Pre-test Questionnaire	27
Figure 3.3.2	Post-Test Questionnaire part 1	28
Figure 3.3.3	Post-test Questionnaire part 2	29
Figure 3.3.4	Shoulder-Surfing Test Questionnaire (Proposed system)	30
Figure 3.3.5	Shoulder-Surfing Test Questionnaire (Passfaces)	31
Figure 3.3.6	Shoulder-Surfing Test Questionnaire (DSR)	32
Figure 4.1.1	Activity diagram for account registration	33
Figure 4.1.2	Activity diagram for account login process	34
Figure 4.1.3	Activity diagram of system demo	35
Figure 4.2	SQLite Database	36
Figure 4.4.1	Home Page UI	38
Figure 4.4.2.1	Register Username and Secret Code	39
Figure 4.4.2.2	Password Image and Direction Selection	40
Figure 4.4.2.3	Account Confirmation	41
Figure 4.4.3.1	Example of user pass-image in Scenario A	42
Figure 4.4.3.2	Identify the password image in Scenario A	42
Figure 4.4.3.3	Special case for scenario A (Left)	43
Figure 4.4.3.4	Special case for scenario A (Right)	43
Figure 4.4.3.5	Example of user pass-image in Scenario B	44
Figure 4.4.3.6	Identify the password image in Scenario B	44
Figure 4.4.3.7	Special case for scenario B (Top)	45

Figure 4.4.3.8	Special case for scenario B (Bottom)	45
Figure 4.4.3.9	Example of user pass-image in Scenario C	46
Figure 4.4.3.10	Identify the password image in Scenario C	46
Figure 4.4.3.11	Three special case of Scenario C (Top-Left)	47
Figure 4.4.3.12	Example of user pass-image in Scenario C	48
Figure 4.4.3.13	Identify the password image in Scenario C (i)	48
Figure 4.4.3.14	Identify the password image in Scenario C (ii)	49
Figure 4.4.3.15	Identify the password image in Scenario C (iii)	49
Figure 4.4.4.1	Login Page	50
Figure 4.4.4.2	Example of a user account and his password	51
Figure 4.4.4.3	Login for First password image	51
Figure 4.4.4.4	Login for Second password image	52
Figure 4.4.4.5	Login for Third password image	52
Figure 4.4.4.6	Success Login Page	53
Figure 4.4.5.1	Fixed image with eight direction buttons	54
Figure 4.4.5.2	Guide of Bottom-Right direction	54
Figure 4.5.1	Example of User's Table in SQLite database	55
Figure 4.5.2	Example of Login Attempt's Table in SQLite Database	55
Figure 5.1.2.1	Pie Chart of Gender	57
Figure 5.1.2.2	Pie Chart of knowledge about graphical password	57
Figure 5.1.2.3	Pie Chart about experience of using graphical password	58
Figure 5.1.2.4	Pie Chart about knowledge about shoulder-surfing attack	58
Figure 5.1.2.5	Evaluation of Proposed system	59
Figure 5.1.2.6	Pie Chart of participants' choice of best understandability	61

Figure 5.1.2.7	Pie Chart of participants' choice on best password memorability	61
Figure 5.1.2.8	Pie Chart of participants' on best system security	62
Figure 5.2.2.1	Chart of first attack trial for proposed method	64
Figure 5.2.2.2	Chart of second attack trial for proposed system	65
Figure 5.2.2.3	Chart of participants' attack method for proposed system	66
Figure 5.2.2.4	Chart of reason of unsuccessful login	66
Figure 5.2.2.5	Chart of first attack trial for Passfaces	67
Figure 5.2.2.6	Chart of second attack trial for Passfaces	68
Figure 5.2.2.7	Chart of participants' attack method for Passfaces	69
Figure 5.2.2.8	Chart of reason of unsuccessful login	69
Figure 5.2.2.9	Chart of first attack trial for DSR	70
Figure 5.2.2.10	Chart of second attack trial for DSR	71
Figure 5.2.2.11	Chart of participants' attack method for DSR	72
Figure 5.2.2.12	Chart of reason of unsuccessful login	72
Figure 5.4.1	Registration time of three authentication systems	74
Figure 5.4.2	Login time of three authentication systems on first day	75
Figure 5.4.3	Average Login Time of three systems on first day	77
Figure 5.4.4	Average Login time of proposed system for total five days	78
Figure 5.4.5	Average Login time of proposed system for total five days (Group 1)	79
Figure 5.4.6	Average Login time of proposed system for total five days (Group 2)	80

LIST OF TABLES

Table Number	Title	Page
Table 2.1	Factors comparison on existing password schemes and proposed system.	24
Table 5.3.1	Proposed System Accuracy	73
Table 5.4.1	Registration time of three authentication systems	74
Table 5.4.2	Login time of three authentication systems on first day	76
Table 5.4.3	Average Login Time of three systems on first day	77
Table 5.4.4	Average Login time of proposed system for total five days	78
Table 5.4.5	Average Login time of proposed system for total five days (Group 1)	79
Table 5.4.6	Average Login time of proposed system for total five days (Group 2)	80

LIST OF ABBREVIATIONS

DSR Digraph Substitution Rules

Chapter 1 Introduction

1.1 Project Inspiration

Nowadays, many authentication systems are suffering from many weaknesses. Textual password is very vulnerable to guessing, key loggers, shoulder-surfing, hidden camera and spyware attacks. There are some new techniques has been introduced to overcome the limitations of text-based password such as two-factor authentication and graphical password. Graphical Password is an authentication system that works by letting users to select pictures in a specific orders and it had to present in a graphical user interface (GUI). It also known as graphical user authentication (GUA). Most people are easier to remember graphical password than a text-based password. Graphical password is using several pictures to represent a user's password instead of using text as password. During the login process, user need to select the same pictures in correct orders that has been set during account registration to access into the system. The advantage of graphical password is to prevent hacker from stealing passwords if they had implanted some key loggers such as Trojan in order to capture the text-based passwords. For these authentication system also had some vulnerability too, applications and input devices such as mouse and touch-screen that allow hackers using spyware to record the graphical authentication process, that is why it also vulnerable to shoulder-surfing attacks too.

Generally, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques. In recognition-based techniques, Users is presented with a set of random pictures during registration and users had to select particular number of pictures from the set as their password. During authentication process, users had to recognize those pictures they had selected during registration in a correct sequence. Some examples of this techniques are ImagePass technique and ColorLogin technique. While in recall-based techniques, during login phase user is asked to reproduce something that he/she has created or selected during registration phase. There are some examples of this techniques that are Passdoodle technique and Draw-a-Secret (DAS) technique.

Chapter 1: Introduction

One of the recall-based graphical techniques is Draw a Secret (DAS), it was developed by Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K.Reiter and Aviel D.Rubin and presented in a paper at the 8th USENIX Security Symposium in August 1999 (Jermyn, et. al., 1999). The password scheme replaces alphanumeric password strings with a picture that drawn on a grid, instead of entering an alphanumeric password. Users need to use a set of gestures drawn on a grid to authenticate by using this method of authentication. The user's drawing is mapped to a grid on which order of coordinate pairs used to draw password and it was recorded in a sequence order. The new coordinates are inserted to the recorded "password" sequence when users ends one stroke and begins another on the grid.

The purpose of this project is to develop a picture-based authentication scheme to prevent shoulder-surfing attacks that is one of the commons attacks we can found nowadays used by hackers to get our privacy info for their self-benefits such as stole money by hacking people's account, invade others privacy and other bad purposes. This project also need to evaluate the system on the capabilities of how user memorize their password by using pictures in the proposed system. To let user easier to memorize their password, the system should not be designed as too complex as user will also feel frustrated to use it. If too easy for user to use then system will have weak security to prevent attacks. So to balance both level of security and user's memorability, I will develop a proposed picture- based authentication scheme which easier for user to memorize and also had strong enough of security against shoulder-surfing attack. This proposed system will be develop as a mobile application and install inside phone to let user use it and also can evaluate user on how difficult in using the app and user's memorability.

The motivation to develop this project is to prevent direct observation and shoulder surfing attacks on login process, many current authentication system are very vulnerable for attacks such as key loggers for text-based authentication system and some of them can be easily known by only just direct observe when they are entering their password.

1.2 Problem Statements

Vulnerable to Shoulder Surfing attacks

Most of the authentication system nowadays are having the same weaknesses that is lacking of security and it is vulnerable to shoulder surfing attacks. Authentication is like the first defense line of all systems to protect their information and resources. There are many people that are not aware of shoulder surfing attacks and the attacks are invisible because they cannot see the attacks are occurring when strangers are attack from other side by just only using their computer to get their password and personal information. Other than that, even when users are using input devices to enter their password such as keyboard and touch screen, hackers may be able to observe the process of how user login through shoulder surfing attacks. This is a serious problem that occurs to many authentication system nowadays and many people are trying to solve it with different schemes.

Memorability Problem

Users have difficulty in remembering complex passwords overtime. The Power Law of Forgetting describes rapid forgetting soon after learning, followed by much slowed decay over long time. Users will likely forget a password that is not regularly or frequently used, as the password would not “refreshed” or “activated” sufficiently often. When users have too many accounts with different passwords, they will only remember some familiar password in their important account such as bank account and Facebook account, but user will also confuse of which password is belongs to which account when they have many different passwords in different accounts.

Strength of Password used by Users

Users normally tend to use password with less complexity and less number of password to make them easier to memorize and decrease the possibility of forgetting their password, but it will also reducing the password security. The Power Law of Forgetting (Bahrick, 1984, pp.1) describes rapid forgetting soon after learning, followed by much slowed decay over long time. Generally, some users are likely to ignore the password recommendations such as 8 characters or longer, with upper-case characters, lower-case characters and digits

to strengthen their password. They will likely to have short and simple passwords as they are not aware that the weak password are very vulnerable to most attacks.

1.3 Project Objective

Develop a suitable method of picture-based authentication scheme to resist shoulder-surfing attacks

- This application will be developed as having stronger security against shoulder-surfing attack and also does not have complex rules so that user can easily understand the rules and memorize their password.

To study more effective method to let users easily understand and memorize the graphical passwords.

- To enhance user's memorability of memorizing password, the rules will not be too complicated and simple enough for them to understand in short time to use the apps.

1.4 Project Scope

This picture-based password scheme is used in authentication process of mobile application to prevent shoulder-surfing attacks with using images as password. This application will be develop with java programming language in Android Studio, which only can be used and support by android-based operating system of smartphone only and iOS will not be supported such as iPhone and iPad. The registration and login data will be stored in local database inside the smartphone with SQLite. This proposed password scheme is involve of 25 different random image that has been set and one of them will be the password of users. This project is using similar logic to digraph substitution rules which user had to choose their selected password as image and the direction from the image with eight different direction to let them choose. During login process, user only need to choose the direction of image from their real selected image they choose during registration. Example, user A set a car image as his password and left as his password direction, so when he login to the application he only need to click the left side of the car image to proceed.

1.5 Project Impact and Contribution

This project will prove to audience that password are not limited only to text-based and it can be picture-based in another form of authentication system. To increase the security against shoulder-surfing attacks, the traditional direct image clicking password is very vulnerable to those attacks or even direct observation while user are clicking his image password. This project is proposing a new picture-based authentication system with some indirectly rules to prevent those attacks. User can also learn something new that picture-based authentication can be set with different rules with clicking different images every time they login. This can prevent shoulder-surfing attacks by clicking the button that only user know real password image while hackers would be confused with user's password.

This project is only using a simple indirect rules that is clicking image on the direction of selected image. The only simple thing to remember is their password image and their direction, this will help them easier to keep in memory because the less thing needed to remember the easier for a human to memorize them.

By using this mobile application authentication system, more user can learn more knowledge about picture-based authentication system and how differently they can be used with different rules or algorithms. This will enhance our current authentication system with not only by using traditional text-based password or direct clicking password image.

1.6 Chapter Summary

The first chapter is discussing about the existing problem of our current authentication system that are vulnerable to shoulder-surfing attacks. The project objectives, project scope and project impact and contribution are stated in the chapter to discuss the proposed system and its benefit to user.

The second chapter is comparing other existing authentication system to find out their strengths and weaknesses. The proposed are trying take their strength to apply into the system and overcome their weaknesses by providing a better solution on it. By comparing the proposed system to other existing system in different categories such as login time, time for user to understand the rules and difficulty of user to memorize their password.

The third chapter will be discussing about system methodology for this project development. This project will follow each phase in SDLC to develop the mobile application. The design flow of the authentication system for each module is stated with activity diagram. The data storage design and system architecture design will be discussed in the chapter. The hardware and software requirements of using the development tools are stated on the last part of this chapter.

Chapter 2 Literature Reviews

2.1 Overview

Graphical password is one of the best methods to solve the problem of text-based password. In this section, I will be doing review on existing work on the problem they found and method they trying to use to solve the problem.

2.2 Review on existing related works

2.2.1 ColorLogin (Gao et al., 2009)

The first research paper proposed a new picture-based password scheme that is ColorLogin. ColorLogin is basically a recognition-based graphical password scheme, choosing multiple images as password icons or pass-icons. ColorLogin uses background color to decrease login time greatly. Multiple colors are used to confuse the peepers or watchers, while not burdening the legitimate users. This proposed scheme is also resistant to shoulder surfing attack. There are four levels of ColorLogin that are low, medium, high and self-define.

In registration phase, user need to choose a security level as mentioned above, then choose one color from many random colors and a number of images from the chosen color sets as their password. For this example, it chooses *one* color from three colors provided and *two* images as pass-icons. In ColorLogin scheme, they defined password as pass-icons. During authentication process, the login screen is divided into (number of color chosen) x (number of color chosen) that is three times three equals to nine background color squares as in Figure 2.2. The color and its positions for the same user are fixed once he chooses his color. All icon of each color are randomly chosen from database. The chosen number of pass-icons are displayed on different rows. In Figure 2.3, there is a function that replace the whole row with substitute icon after user click the desired icon on that specific line to

prevent shoulder surfing attack because they don't know which icon was clicked. For safety purpose, the default numbers of pass-icons had to be choose is set to two because one will increase the chances of letting other people login into their account. If the number is more than two, user will also need to take longer time on login process.



Figure 2.1.1 A group of chosen-color icons are displayed for user to set as his pass-
icons



Figure 2.1.2 The icons displayed in login screen



Figure 2.1.3 A line of substitute icon replacement after user click its desired icon on that lin

Strength(s)

1. The icons on the screen are distinguished clearly by different colors. When users are asked to recognize the pass-icons in the authentication, they only need to pay attention to the icons of the predefined color rather than all the icon displayed. The higher level used, the more color are introduced and the more workload are reduced.

Limitation(s)

1. If the authentication procedure is too tedious, it may create memorization difficulties and annoy users.

Suggested Solution:

The use of background colors can make the user interface friendly, which helps users escape from the irritation of large number of confusing icons.

2.2.2 Pass-Matrix (Aravindh et al., 2017)

Next, the second research paper proposed a system that can be implemented on a range of mobile applications and devices to make user more convenience. To prevent hackers from observing the input process of users, they proposed to implement a technique termed Pass-Matrix where the rows and columns filled with data. During registration process, user need to enter user details and select the graphical pass image or even upload image by users themselves to increase user friendliness. Pass-Matrix split images into 7x11 grids as in Figure 2.4 and user can select any one of the grids to be use to verify during login process. The arrangement of horizontal alphabetical bar letters and vertical numbers are randomly not as ascending or descending. This also provides robust security against shoulder surfing attackers.

During login process, first user need to login with username and then will get a one-time login indicator showed in Figure 2.5. After that, it will show the pass-grid and user had to move the one time login indicator grid to the pass-grid that has been selected just now. The method mentioned above are easily seen by attackers of where the pass-grid is located if they can observe the process through shoulder surfing attack. To overcome this problem, they use a method by putting a set of numbers ranging from zero to nine over all seventy-seven grids. When user moving one-time indicator grid to the pass-grid, the whole respective row is also moved to the other side as shown in Figure 2.6. Attacker will be confused since whole row is moving. Even if they knew the location of login indicator, they will also be confused by many same numbers over the grids. After the validation is complete, then user are successfully login. The password input by users must go through the validation of server to access to the system. They only can login successfully if their password is valid, if they entered several times of incorrect password, the server will block the account and intimate user through E-mail or mobile number via SMS about current login location of the account.

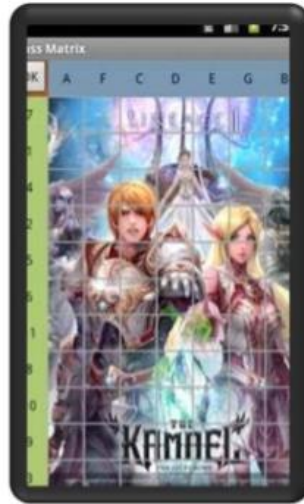


Figure 2.2.1 Pass-grid selection from 7x11 grid image



Figure 2.2.2 One-time login indicator



Figure 2.2.3 Graphical pass-image authentication where numbers scattered all over the grids

Strength(s)

1. This technique improved the scope of security by the method of pass matrix where the attackers had no clue about hacking the accounts.
2. This technique also resist against shoulder surfing attacks because the password used by user is not directly, which strengthening the security.

Limitation(s)

1. This method is still not secure enough to resist against hackers. The pass-matrix allows user to select an image from a set of pre-defined images, which could be guessed by hackers.

Suggested Solution:

This limitation can be overcome by letting user choose either want to upload their desired image, this will also improving the security of the system

2.2.3 Two Step Random Colored Grid (Purushothaman *et al.*, 2016)

Another research paper that proposed a two-step random colored grid graphical password scheme. This scheme can be implemented on smartphones, web application and even traditional desktop systems. This password scheme consist of two phases that is registration phase and login phase.

In registration phase, first user had to register his username and password. Then it will show a 6x6 grid total of thirty-six grids consists of twenty-six alphabets and ten numeric from zero to nine in six colors (Pink, Blue, White, Green, Red, Yellow) shown as in Figure 2.7. User need to draw a line across those squares and characters which will be the password of this account.

Now we will proceed to login phase, first user will need to enter his username in order to proceed to next step. After that, a 6x6 square grids will be show on screen. User had to enter the first letter of the grids according to the password set during registration. For example in figure 2.7, his password is “ou067” during registration while login phase user had to enter “PRPGY” as password to proceed. The password “PRPGY” means first letter of the password grid: P-pink, R-red, P-pink, G-green, and Y-yellow. Every time user wants to login, the colors of the grids will be randomized but the alphabets and numbers are fixed for user convenience. This method can prevent shoulder surfing attack because they cannot identify the exact password since there consists of different colors and characters.

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

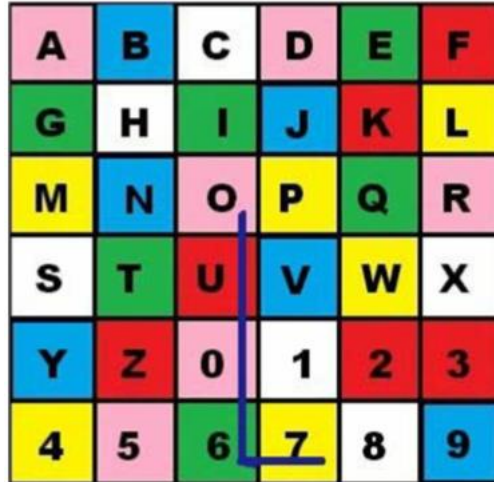
A 6x6 grid of characters. The characters are arranged in rows and columns. A blue pattern line is drawn starting from the character 'U' in the third row, third column, moving vertically down to '6' in the sixth row, third column, then horizontally right to '7' in the sixth row, fourth column.

Figure 2.3.1 6x6 grid with pattern line enter by user

Strength(s)

1. Attackers would have no chances in knowing the real password entered by user.
2. The proposed methods can confused attackers when shoulder surfing.

Limitation(s)

1. The length of password are not strong enough because as the time flows hackers will surely find ways to surpass this proposed system.

Suggested Solution:

They can increase the default length required for user to choose to six characters or above to increase the level of security and also to prevent shoulder surfing.

2.2.4 Falsification (Chee Yeung *et al.*, 2015)

This graphical password scheme is using falsification to resist against shoulder-surfing attacks. It also consists of two phases that alike with other password scheme that is registration and authentication phase.

In registration phase, user will need to enter their full name, email and username. Then user will also need to select minimum 5 of them out of 8 image categories options. After user click the submit button, they will need to choose their graphical password in those categories they choose. For example, the first category options appeared is football team, then user need to type the alphanumeric character which is beside those image shown in Figure 2.9. The steps will be repeated for all above categories they choose during registration phase.

REGISTRATION Already a member?
[Log in Here](#)

Full Name:

E-mail:

Username:

Please Select your preferred category for your graphical password.
**choose at least 5 and maximum 8 category of graphical password

- Favourite Car Brand
- Favourite Country Flag
- Favourite Fast Food
- Favourite Phone Brand
- Favourite University
- Favourite Basketball Team
- Favourite Football Team
- Favourite Superhero
- Favourite Pet
- Favourite Sport

Figure 2.4.1 Registration

Please Select your Favourite football team as your graphical password.

Selection:

Figure 2.4.2 Type alphanumeric character from football team category

Chapter 2: Literature Review

Next for authentication phase, user will first need to enter their username then user interface will appear a random categories image with a false image added automatically as shown in Figure 2.10. User will need to know whether this image categories are one of his selected categories then he can pick the correct image, otherwise he will need to pick the false image to ignore the image category. This can confuse shoulder-surfing attacker that will though the false image is their real password.



Figure 2.4.3 A random image categories (Pet)

Strength(s)

1. Can confuse the shoulder-surfing attacker who are trying capture their password.
2. The input character is using typing instead of using mouse to select the graphical password.

Limitation(s)

1. Vulnerable to key loggers when they will know which character user typing.
2. User will feel confused when they need to remember five to eight image in different categories.

2.2.5 Digraph substitution rules (DSR) (Por *et al.*, 2017)

This password scheme is recognition-based with using digraph substitution rules (DSR) to conceal the image password to prevent shoulder-surfing attacks. This password scheme also having two phase that also similar to others scheme that is registration phase and authentication phase. These two phases basically are needed mostly for every password scheme for having to register user's password and authentication process during login.

During registration phase, user is required register their username and select two images as password from a 5x5 image grid as shown in Figure 2.7. Then user also need to choose whether he want to choose first image or second image as their password shown in Figure 2.9 to complete the registration process.

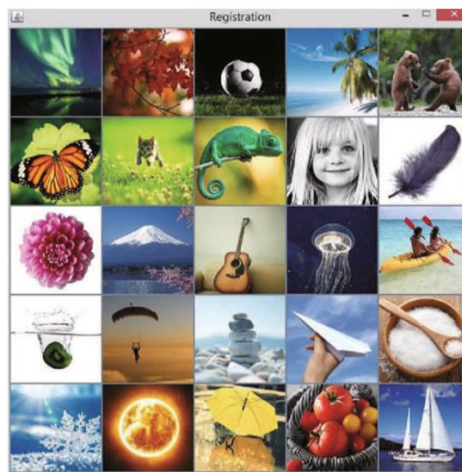


Figure 2.5.1 User Interface of registration phase



Figure 2.5.2 Options for user to select his password image

For the next step that is authentication phase, firstly user will need to key in their username to proceed to picture-based authentication. After that, there will be a set of 5x5 randomize image grid to ensure all image are randomly distributed into different place every time they login. To complete the authentication process, user has to complete three consecutive of challenge sets by using the digraph substitution rules to identify their password image. To identify their password image, user is needed to understand three rules of digraph substitution rules as followings:

- Scenario 1: Both password images are diagonal to each other's.
- Scenario 2: Both password images are on the same vertical line.
- Scenario 3: Both password images are on the same horizontal line.

Scenario 1

As for example of a user want to login, Figure 2.10 shown the two selected images set by user as his password image during registration process. Then user will need to use this two password images to find out the correct password image. For scenario 1, if this two images are appear diagonal to each other's, user is required to identify the row of his first password image and the column of his second password image. After obtaining both row and column for each images, the intersection point which marked as P1 in Figure 2.11 is his first real password image. To identify the second password image, it also similar on identifying first password image, but different is it will start at identifying row of his second password image and follow by column of his first second password image. Then the intersection point which marked as P2 in Figure 2.12 will be his second real password image.

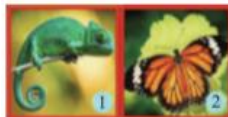


Figure 2.5.3 A sample of user's password images



Figure 2.5.4 First password image for scenario 1

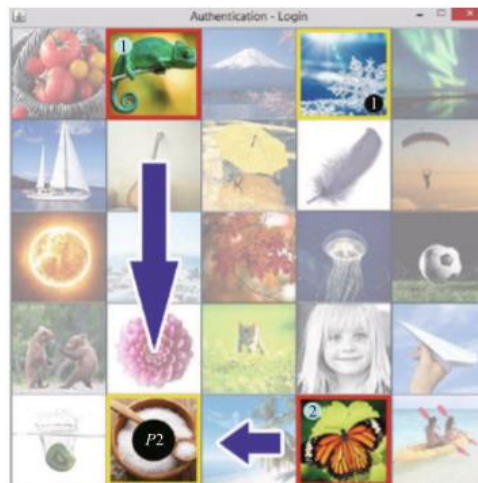


Figure 2.5.5 Second password image for scenario 1

Scenario 2

For scenario 2, this kind of scenario will only happen when both of the password image are appear on the same vertical line. First, user also need to identify their both password image first and their real password image is set directly below their password image. As the figure shown in Figure 2.13, P1 is the first real password image below first pass-image while P2 is the second real password image below second pass-image.

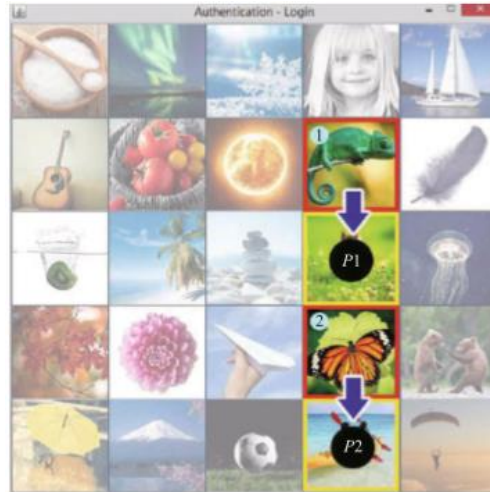


Figure 2.5.6 Password image of scenario 2 which on the same vertical line

Scenario 3

For scenario 3, this scenario is almost same as scenario 2 which the difference is only both of the password image are appear on the same horizontal line. Firstly, user need to identify their both password image first and their real password image is set directly right of their password image. As the figure shown in Figure 2.14, P1 is the first real password image on the right of first pass-image while P2 is the second real password image on the right of the second pass-image.

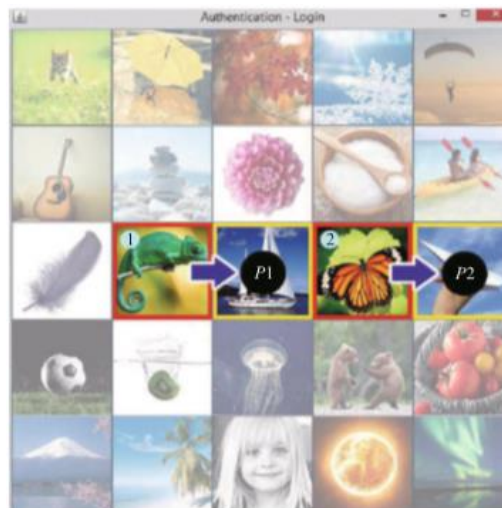


Figure 2.5.7 Password image of scenario 3 which on the same horizontal line

Strength(s)

1. Able to conceal user's password as user only need to click one of the password image instead of the two selected password image.
2. Able to reduce shoulder-surfing attacks and it also does not weaken the password security.
3. Even shoulder-surfing attackers know the digraph substitution rules, these attacks also cannot obtain the password images used by user.

Limitation(s)

1. Having limited password spaces is also a disadvantage of recognition-based system.

2.2.6 Secure Passfaces (Towhidi, Masrom and Manaf, 2013)

This Secure Passfaces (S-Passfaces) authentication system is an enhance version of Passface, it improving the vulnerability of the Passface against shoulder surfing attack. They changed it to input text-based password with the alphabet below their each password image instead of directly clicking the image with mouse. This is also more resist to shoulder-surfing attack. User will need to register his username and his four password image. Then during login process, user will need to input the alphabets show below the password images rather than directly clicking the image. User will only can login with correct combination of all four groups of alphabets corresponding to their password images.



Figure 2.6.1 First login round of S-Passface

To let the password looks random and differently, this system allow user to register two passwords where the first password is included old men and old ladies while the second password contain of faces of clowns and kids. So user had to login for both two round to successfully login into the system.

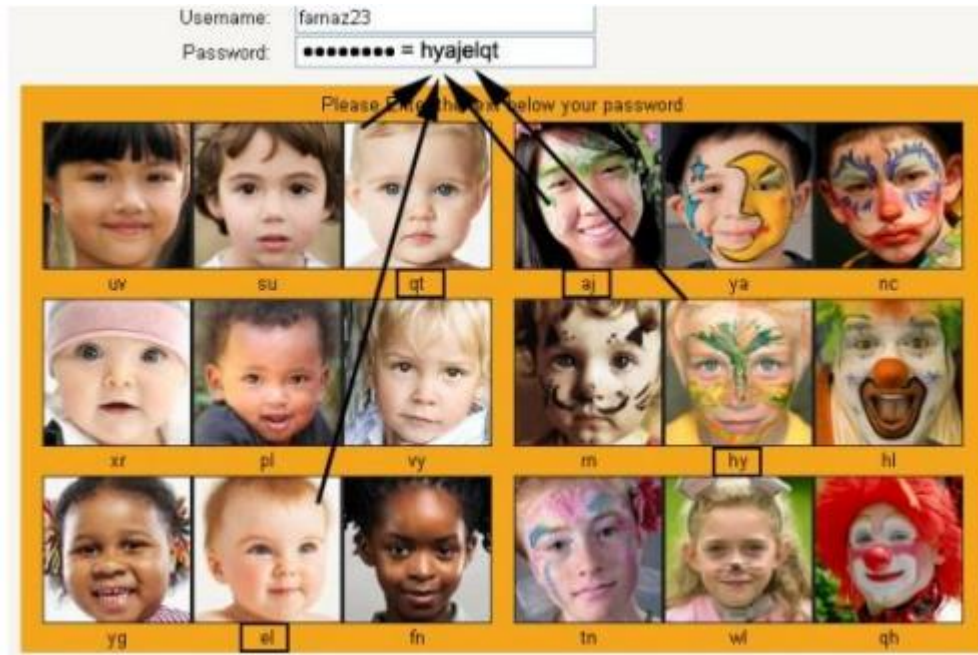


Figure 2.6.2 Second login round of S-Passface

Strength(s)

1. Able to resist to shoulder surfing attack as it does not need to use mouse to click the image as it only need keyboard to input correct password.
2. Enhance version of Passface and stronger security against shoulder-surfing attack than Passface.

Limitation(s)

1. Vulnerable to keylogger and shoulder-surfing attack if both attack occurs at the same time and attacker can record their input and his login process to compare which image is their real password image.

2.2.7 Comparison Table among all system reviewed

Table 2.1 shows the comparison between five different existing password schemes on criteria could affect the user-friendliness and efficiency of users using this systems. There are three different criteria that evaluate the five existing password schemes that user spend how much of time to understand how the system works, time spend to login and the level of resistant to shoulder surfing.

Systems Criteria	ColorLogin	Pass-Matrix	Two Step Random Coloured Grid	Falsification	Digraph Substitution rules	Proposed Method	S-Passface
Time used to understand the rules	Medium	Long	Medium	Medium	Short	Short	Short
Login Time	Long	Medium	Long	Short	Short	Short	Short
Resistant to Shoulder surfing	High	Medium	High	Low	High	High	High

Table 2.1 Factors comparison on existing password schemes and proposed system.

Chapter 3 System Methodology

3.1 Project Development

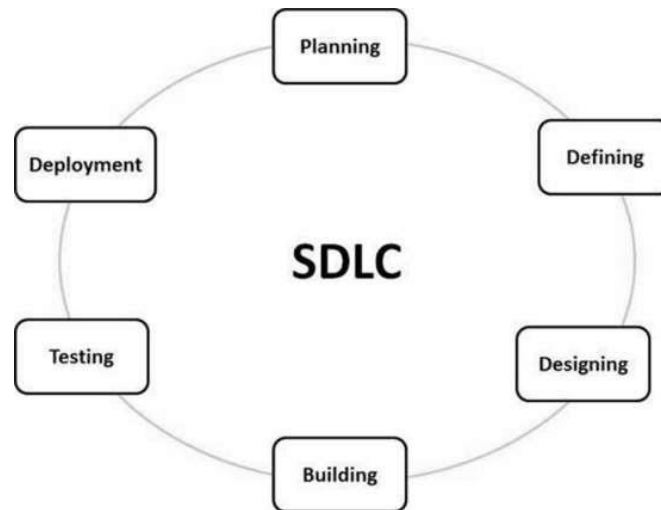


Figure 3.1 System Development Life Cycle (SDLC)

First of all, during planning phase the problem is already identified and trying to propose a method to overcome the problem. After that in defining phase is setting project objective to proceed to next phase. Then the basic concept design of the proposed method is completed and the discussion is made with supervisor to make sure that it's able to resist to shoulder-surfing attack. Next step will be development phase which will start to code the mobile application prototype until finish. The proposed system including both similar authentication system will also be code inside the apps for evaluation purpose.

For the next phase is testing phase, the system will be tested with a group of people in 6 days including first day of survey test and shoulder-surfing test while next 5 consecutive days is for memorability test for the proposed system. After finish gathering the information of the group of people, analysis can be carried out with statistics of the info. Finally the last phase will be the documentation that will collected all the data to be analyze and put it into the report.

3.2 Information Gathering (Data Collection)

For system evaluation, this project need to gather the information for capabilities of user's memorability by using three times of successful login for each days, total of 5 days of login into the apps to record users' login attempt including unsuccessful and successful. It will also record their password creation time for each set of password, the duration of user every time they login to analyze the difference login duration of first day login until last day login. The lesser the duration user spend to login their account by each days prove that user had getting more familiar with the system and had better user's memorability to memorize their own password in using this application. For the shoulder surfing test, participants will need to fill up a survey after finish the test to evaluate whether they can perform shoulder-surfing attack to the authentication system to analyze the vulnerability of both three systems.

3.3 Project Verification Plans

For the verification plan, there are 20 participants are needed to participate in the evaluation test including three different authentication that is proposed system, Passfaces and Digraph Substitution Rules. All of them is code inside a mobile apps to let them test using a smartphone during evaluation test. All the process of registration and login process of three systems are demonstrated to participants to teach them learn how to use the system. Then they are needed to register an account for all systems and perform login to familiarizing themselves with the systems. Participants need to at least perform five times of successful login for each system proceed to next step. Then participants need to continue fill in the survey form to evaluate which system is easier to use, easier to understand and most invulnerable system. After that, only ten of them will be selected for shoulder-surfing test that required to watch video of login process to the account for each system. Then, participants will be given three attack attempt to try login into the account. If they success then it means that it is vulnerable to shoulder-surfing attack, if not then it is resist to shoulder-surfing attack. There is no method limited to how they perform attack such as pause the video to record the pictures or take pictures of login process to analyze the pass-image. There are maximum of three times to watch the video to perform attack and later they will need to fill up the post-test questions after the test finish for each systems. All the data will be collected and will be analyzed later.

Graphical Password to prevent Shoulder-Surfing Attack Survey Form

* Required

Pre-Test Questions

Username: *

Your answer

Gender *

Male

Female

1) Do you know what a picture-based/ graphical password is? *

Yes

No

2) Have you ever login using picture/ graphical password? *

Yes

No

3) Have you ever heard/ read about 'shoulder-surfing' attack? *

Yes

No

Figure 3.3.1 Pre-test Questionnaire

Figure above shown, this survey form requires participants to fill in their username which used to match with their username that will be register later on in the authentication system for documentation purpose. It also need participants to select their gender and next three questions is asking about whether do they know what is graphical password, have they used it before and do they know about “shoulder-surfing attack”.

Post-test Questions 1

User need to LEARN the THREE system rules

- Proposed Method
- Passfaces
- Digraph Substitution Rules (DSR)

Evaluate the proposed system: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1. I felt very easy in memorizing the password.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. I felt very confident using the system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. I though the system was easy to use.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. I would Imagine that most people would learn to use this system very quickly.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. I needed to learn a lot of thing before I could get going with this system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. I think that I would like to use this system frequently.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7. I found the system unnecessarily complex.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 3.3.2 Post-Test Questionnaire part 1

Next, this figure purpose is to let participants to evaluate the proposed system with seven different questions from Strongly Disagree to Strongly Agree. The data collected through this evaluation will be analyzed later.

Among THREE systems, which one is the easiest to understand?

*

- Proposed Method
- Passfaces
- Digraph Substitution Rules

Among THREE systems, which one was easiest to remember the password? *

- Proposed Method
- Passfaces
- Digraph Substitution Rules

Among THREE systems, which one you think that is most invulnerable to Shoulder-surfing attack? (Safest) *

- Proposed Method
- Passfaces
- Digraph Substitution Rules

Figure 3.3.3 Post-test Questionnaire part 2

Then, there are three questions to let participants answer by making comparison among three selected systems including proposed system, Passfaces and DSR. The questions let participants choose whether which systems are better in understandability, password memorability and system invulnerable to shoulder-surfing attack.

Post-test Questions 2 (Shoulder-surfing test)

User will be demonstrated some video to see whether they can success login into those account.

Proposed Method

1) By watching the recorded video [ONE times], were you able to perform shoulder-surfing attack successfully using your strategy/method? *

- Yes
- No

2) By watching the recorded video [THREE times], were you able to perform shoulder-surfing attack successfully using your strategy/method? *

- Yes
- No

3) What strategy/method did you used when trying to perform shoulder-surfing attack? *

- Random guessing/ Brute force
- Direct observation and click according to images used in video
- Direct observation and click according to coordinates used in video
- Other: _____

4) If not successful, what do you think caused your strategy/method to fail? *

- Success
- This method is SECURED
- Too RANDOM in every challenge set
- Used the WRONG strategies to obtain the pass-images used
- Confused about the password images and pass-images
- Other: _____

Figure 3.3.4 Shoulder-Surfing Test Questionnaire (Proposed system)

First test of the shoulder-surfing attack is for the proposed system. First and second question is answer for participants to view a video clip whether they can perform shoulder-surfing attack and successful login. Third question is asking participants on what method they used to perform shoulder-surfing attack while last question is reason of failure attack or will be skipped if perform successful attack.

Passfaces

1) By watching the recorded video [ONE times], were you able to perform shoulder-surfing attack successfully using your strategy/method? *

- Yes
- No

2) By watching the recorded video [THREE times], were you able to perform shoulder-surfing attack successfully using your strategy/method? *

- Yes
- No

3) What strategy/method did you used when trying to perform shoulder-surfing attack? *

- Random guessing/ Brute force
- Direct observation and click according to images used in video
- Direct observation and click according to coordinates used in video
- Other: _____

4) If not successful, what do you think caused your strategy/method to fail? *

- Success
- This method is SECURED
- Too RANDOM in every challenge set
- Used the WRONG strategies to obtain the pass-images used
- Confused about the password images and pass-images
- Other: _____

Figure 3.3.5 Shoulder-Surfing Test Questionnaire (Passfaces)

The questions for Passfaces is similar to proposed system which participants will watching a video clip of user login using Passfaces.

Digraph Substitution Rules (DSR)

1) By watching the recorded video [ONE times], were you able to perform shoulder-surfing attack successfully using your strategy/method? *

- Yes
- No

2) By watching the recorded video [THREE times], were you able to perform shoulder-surfing attack successfully using your strategy/method? *

- Yes
- No

3) What strategy/method did you used when trying to perform shoulder-surfing attack? *

- Random guessing/ Brute force
- Direct observation and click according to images used in video
- Direct observation and click according to coordinates used in video
- Other: _____

4) If not successful, what do you think caused your strategy/method to fail? *

- Success
- This method is SECURED
- Too RANDOM in every challenge set
- Used the WRONG strategies to obtain the pass-images used
- Confused about the password images and pass-images
- Other: _____

Figure 3.3.6 Shoulder-Surfing Test Questionnaire (DSR)

The questions for Digraph Substitution Rules (DSR) is similar to both system above with participants trying to perform attack to a video clip of user login into DSR authentication system.

Chapter 4 System Design

4.1 Design of picture-based authentication system

4.1.1 Registration

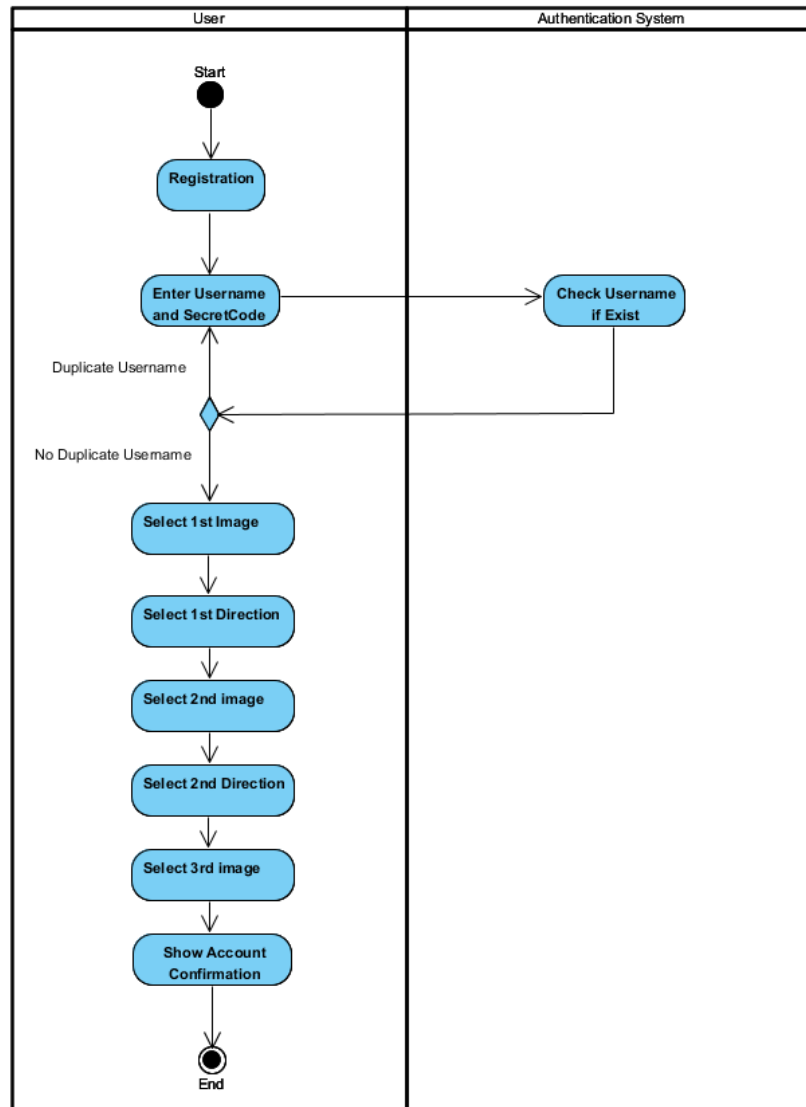


Figure 4.1.1 Activity diagram for account registration

During registration, the system will prompt user to enter his desired username. If the username already existed then user will need to enter another username again. Next, user will need to select an image from a group of images and then select the direction to complete the registration process.

4.1.2 Login

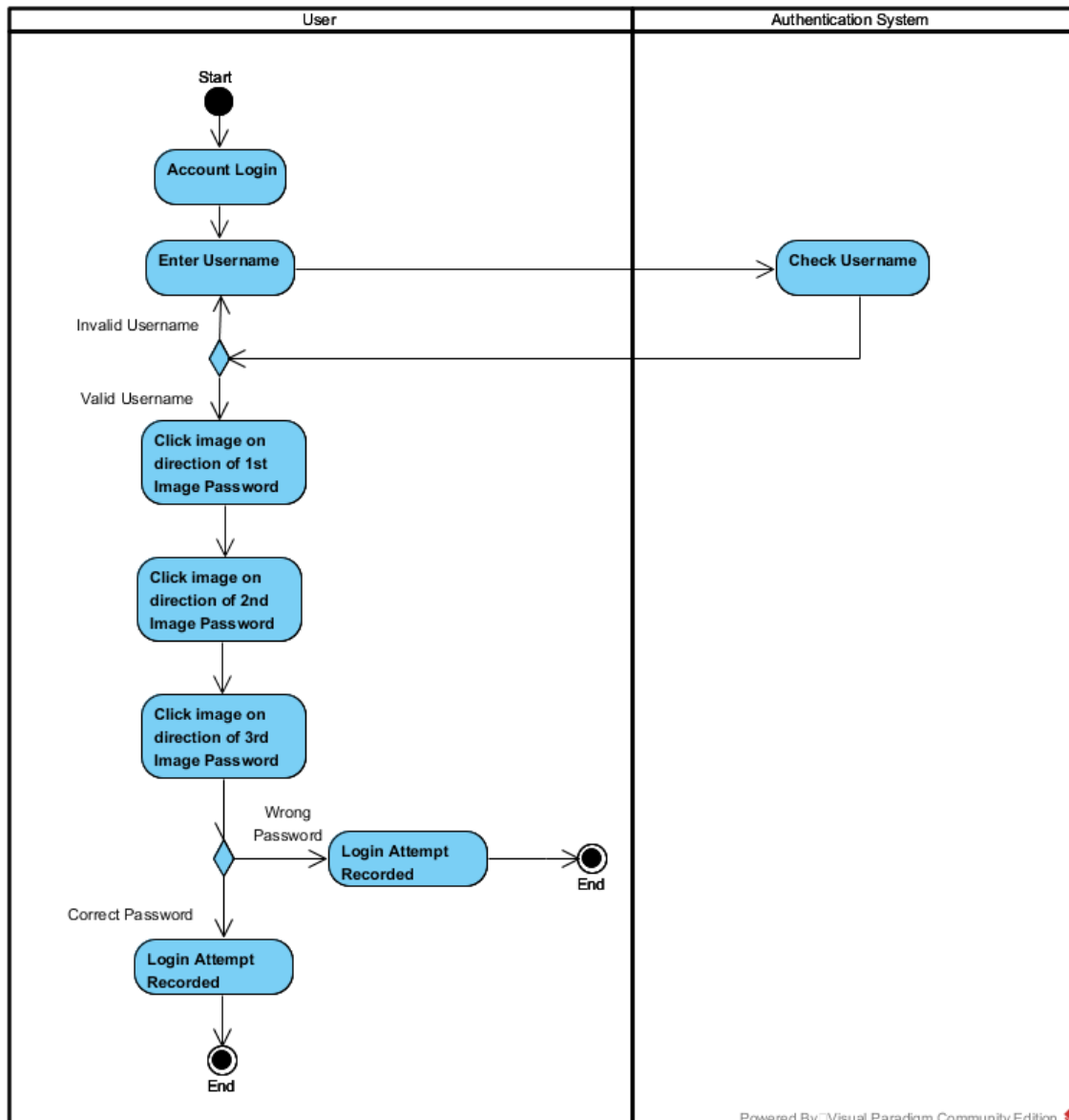


Figure 4.1.2 Activity diagram for account login process

When user want to login to this system, user will need to enter his username to proceed further. If username entered is valid, then a set of random image grid with 5x5 will appear on the screen. User will need to select the image on the direction of his registered image to successfully login. If more than three failed attempt, the system will be closed. User can only login successfully with all three correct pass-image.

4.1.3 Demo

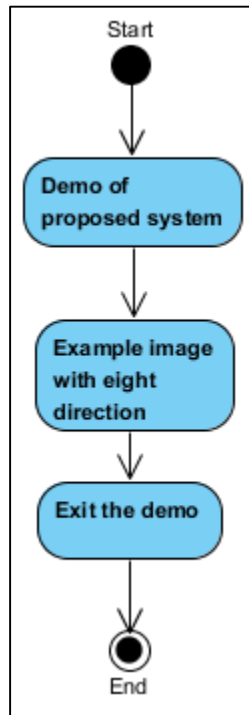


Figure 4.1.3 Activity diagram of system demo

This module is providing a demo to let user learn how actually they need to do during login process with the example image and direction select by them.

4.2 System Architecture Design

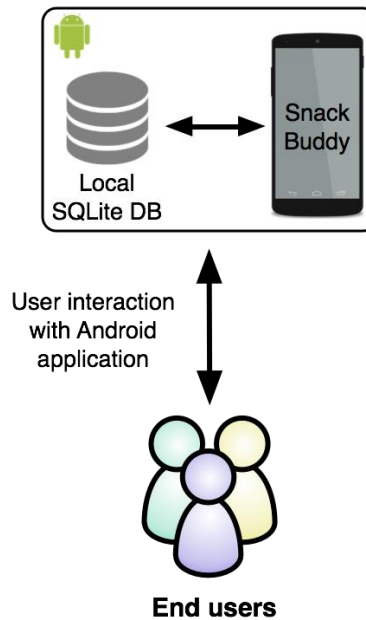


Figure 4.2 SQLite Database

For the data storage, SQLite will be chosen to use as a database for Android Studio to store in the local storage inside the smartphone. The data that is registered by the user will only be stored by SQLite inside the application itself and will be used for the login process after finishing registration.

4.3 Hardware and Software Requirements

The development tools used in this project to develop mobile application is Android Studio. There are some minimum requirements of hardware and software before using Android Studio to develop the mobile applications.

Hardware

- 3 GB RAM minimum and 8GB RAM is recommended for smooth work environment, 1 extra GB of RAM is needed if using Android Virtual Device Emulator.
- Minimum of 2GB available disk space, although 4GB of disk space is recommended(500MB for IDE + 1.5GB of Android SDK and emulator system image)
- Minimum of screen resolution is 1280x800.

Software

- Operating System of PC must be at least Microsoft Windows 7/8/10(32-or 64-bit)

4.4 Graphical User Interface Design

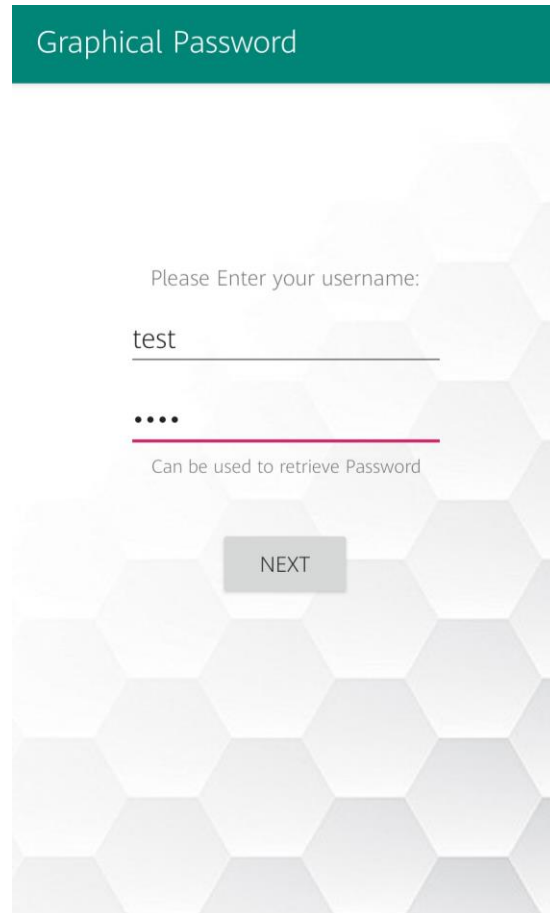
4.4.1 Home Page UI



Figure 4.4.1 Home Page UI

This is the home page of the proposed system where included login button, signup button, demo guide button, other similar authentication system, attempt checking and admin control. The login button will proceed to the login process while signup button will proceed to the registration process. The demo guide is to let user get more familiar with the rules of the system with the fastest way it can. Other similar system is another authentication system that is Passfaces and Digraph Substitution Rules (DSR) to do comparison with my proposed system. It also had function of signup and login. Attempt checking is to check the total of every attempt of user login. While admin control is only for admin to check all the user and delete user.

4.4.2 Registration Process



The screenshot shows a registration form with a teal header containing the text "Graphical Password". Below the header, the form has a light gray background with a hexagonal pattern. The first input field is labeled "Please Enter your username:" and contains the text "test". Below this is a second input field containing four black dots, with a red underline and the text "Can be used to retrieve Password" underneath. At the bottom of the form is a gray button labeled "NEXT".

Figure 4.4.2.1 Register Username and Secret code

The first step of registration process is register their username with alphanumeric characters. If the username is already existed, then it will not allow user to register their username as the right figure shown above. Then the next will be the secret code where user can use to retrieve their password if they had forgot their password. After that click next button to proceed to next step.

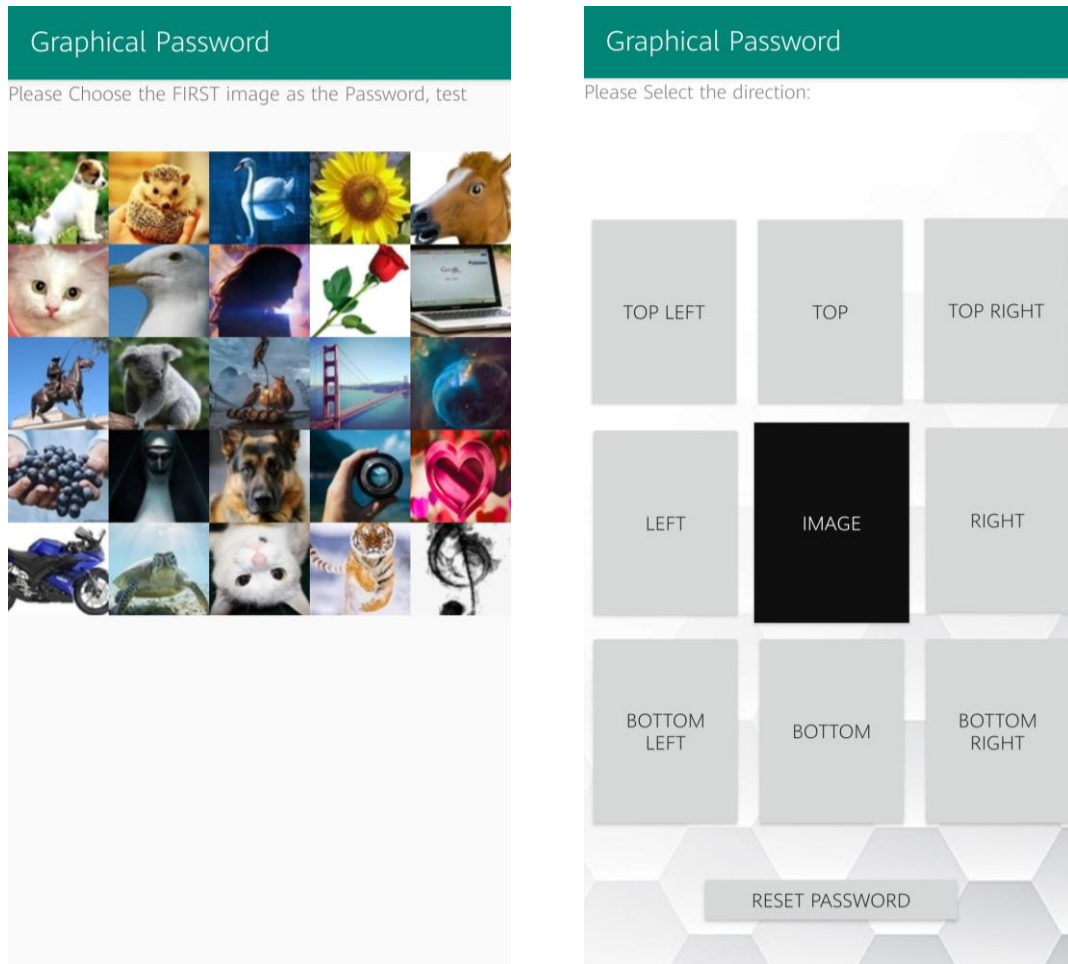


Figure 4.4.2.2 Password Image and Direction Selection

After finish enter their username, the next step of the registration process is to select their desired first image and the direction as their first password. Then reset password button is only available after select their first password image in case if they want to change their password or forgot their password. Same step as first password also applied for second and third image and directions as their second and third image password.

Graphical Password

Username : test

1st Password: 

1st Direction: Top

2nd Password: 

2nd Direction: Top

3rd Password: 

3rd Direction: Top

Time Spend to Register (seconds)			
1st	2nd	3rd	Total
18.03	1.50	1.60	21.13

CONFIRM




Figure 4.4.2.3 Account Confirmation

After finish select all three image and direction as password, a confirmation of user interface that will show all the details including username and their three image password and direction. It also shows the total password creation time and each pass-image creation time. They can click the confirm button after they had confirm their account creation to go back the home page.

4.4.3 Proposed algorithm

This proposed contain of image with eight directions to be click including top, top left, top right, left, right, bottom, bottom left and bottom right. There are 3 scenario included in this proposed algorithm:

- Scenario A: The direction of image is either **Left** or **Right**.
- Scenario B: The direction of image is either **Top** or **Bottom**.
- Scenario C: The direction of image is either **Top Left, Top Right, Bottom Left** or **Bottom Right**.

- ①.  = User pass-image registered during registration.
- ②.  = Image that should be click during login process.
- ③.  = The original location that the image should be clicked.

Scenario A

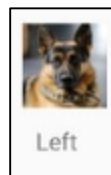


Figure 4.4.3.1 Example of user pass-image in Scenario A



Figure 4.4.3.2 Identify the password image in Scenario A

For the example, the password will be set as dog and the direction as left. Then during login process, user will only need to click the image on the left of the dog image as their pass-image. Same method is also applied to right direction. The images is randomize so the location will be different each time user login.

Special case for Scenario A

There are special case for scenario A when the left or right of his pass-image is near the edge of the user interface and there was nothing at there. Then it the password will be set as another side of image as their pass-image to be clicked.



Figure 4.4.3.3 Special case for scenario A (Left)



Figure 4.4.3.4 Special case for scenario A (Right)

Scenario B



Figure 4.4.3.5 Example of user pass-image in Scenario B



Figure 4.4.3.6 Identify the password image in Scenario B

As the example above, his password image is tiger and direction set as top. So user will need to click the top image of the tiger during login process to proceed further. Same method is also applied to bottom direction.

Special case for Scenario B

There are also had special case for scenario B when top or bottom of the pass-image is near the edge of the user interface and next to them is empty there. Then the password will be set on another side of image as their pass-mage to be clicked.



Figure 4.4.3.7 Special case for scenario B (Top)

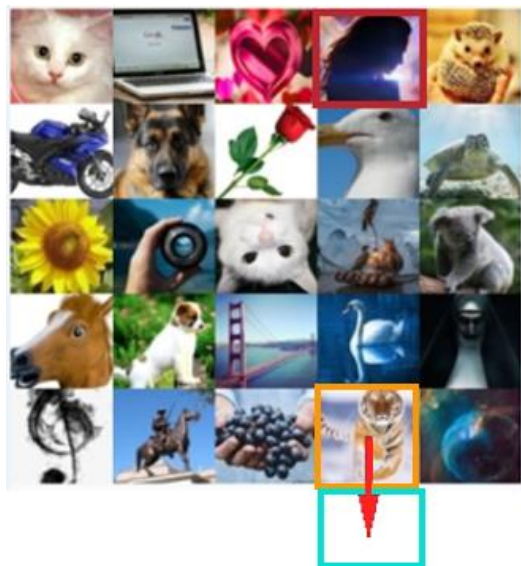


Figure 4.4.3.8 Special case for scenario B (Bottom)

Scenario C



Figure 4.4.3.9 Example of user pass-image in Scenario C



Figure 4.4.3.10 Identify the password image in Scenario C

This time the user pass-image will be set as a koala image and direction as Bottom-Right. So user will only need to click the Bottom-Right of the koala image as their pass-image during login to continue. Same method is also applied to Top-Left, Top-Right and Bottom-Left.

Special case for Scenario C

Scenario C is the most special among all the scenarios because all directions of the scenario C had three special scenario for each of them. For example below shown direction set as top-left so there are three special scenario for scenario C. Same method also will be applied for other three directions such as top-right, bottom-left and bottom-right.



Figure 4.4.3.11 Three special case of Scenario C (Top-Left)

- Scenario C (i): **Blue** indicates that image appear on **First Row**.
- Scenario C (ii): **Green** indicates that image appear on **First Column**.
- Scenario C (iii): **Red** indicates that image appear on the **Corner** of the interface.

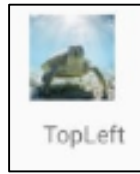


Figure 4.4.3.12 Example of user pass-image in Scenario C

The example that shown above is the turtle image is set as his pass-image and direction as Top-Left.

Scenario C (i)

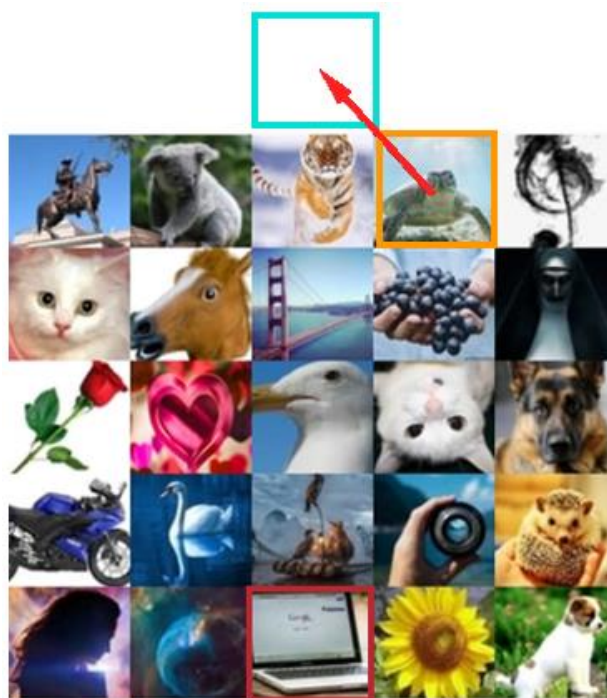


Figure 4.4.3.13 Identify the password image in Scenario C (i)

Scenario C (ii)



Figure 4.4.3.14 Identify the password image in Scenario C (ii)

Scenario C (iii)

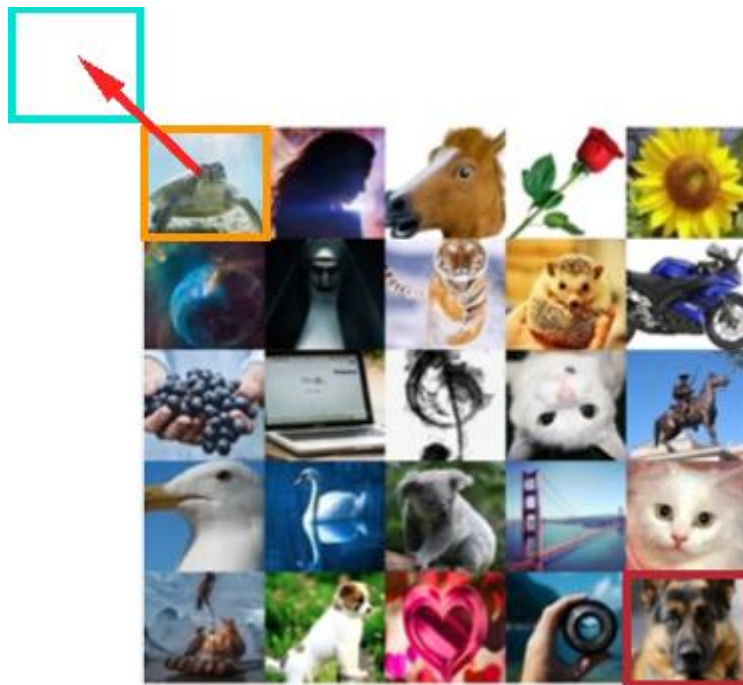


Figure 4.4.3.15 Identify the password image in Scenario C (iii)

4.4.4 Login Process

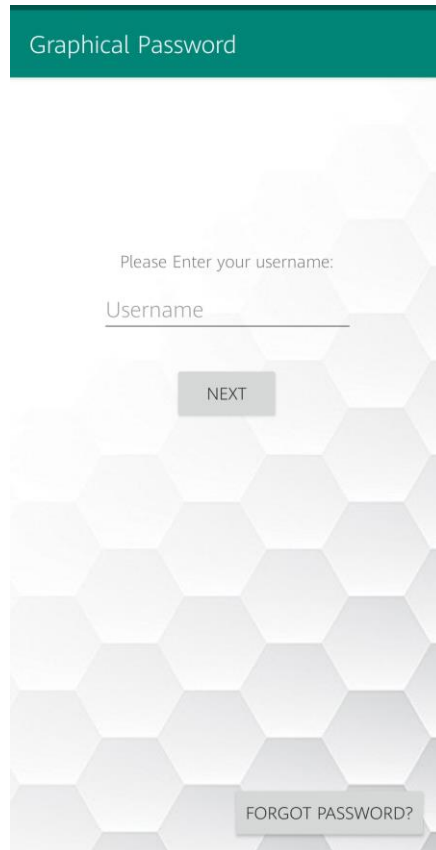


Figure 4.4.4.1 Login Page

User had to enter their username to login into system. The forgot password button at the bottom of the interface is to let user retrieve their password with secret code they registered during registration if they forgot their pass-image.




Username :	abcd
1st Password:	
1st Direction:	Left
2nd Password:	
2nd Direction:	Top
3rd Password:	
3rd Direction:	BottomLeft

Figure 4.4.4.2 Example of a user account and his password

For example, a user named as “abcd” had his first image password as a cat and left direction, second image password as tiger and top direction, and third image password is koala and bottom-left direction.



Figure 4.4.4.3 Login for First password image

User will need to click the bridge image where it is on the left of his first password image of a cat. User had three attempt to enter his correct password shown at bottom of the

interface. If user failed to enter correct password with three failed attempt, user will be kicked out of the login process back to home page. User can only proceed to second pass-image with correct pass-image within three attempt.

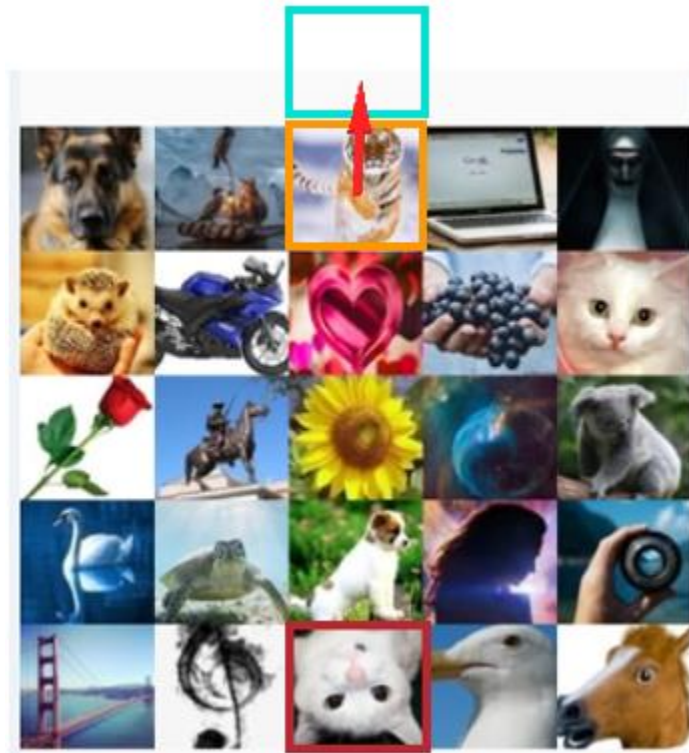


Figure 4.4.4.4 Login for Second password image

Same as the first pass-image, this time user need to find out the correct pass-image where top direction of the tiger image. This time also meet the special case for scenario B so it should be the image on the other side of the interface that is the upside-down cat image.

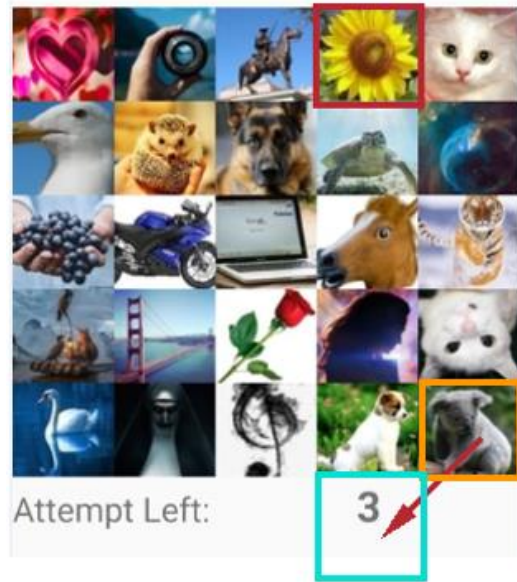


Figure 4.4.4.5 Login for Third password image

This time the password image has match with the special case scenario C that is bottom-right of the koala image is the sunflower image that is on another side of the interface.



Figure 4.4.4.6 Success Login Page

After user successfully login with his three pass-image, then it will pop-out a Successful Login message and the duration of user spend during his login process.

4.4.5 Demo

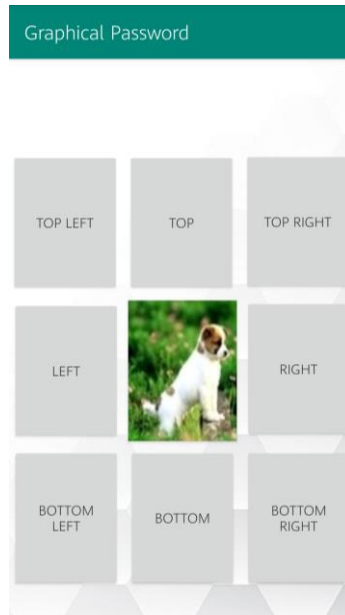


Figure 4.5.1 Fixed image with eight direction buttons

Inside the demo guide, the default image will be set as the dog and eight buttons of each directions. Each direction only provide its own rules as the name.



Figure 4.5.2 Guide of Bottom-Right direction

After click into one of the directions, it will let user easier to learn how to use the system.

4.5 Data Storage Design

For the database table, it contains some common attributes such as username, first/second/third password image and directions choose by user. Username, password image, directions, total creation time, each password creation time and the secret code will be store in local storage on user’s phone for easier to let them test the password scheme and record their login attempt.

While for the login attempt’s table record every attempt of user login whether is fail or success including the total login time and each image login time. The date will be store as which day they login.

	username	password1	direction1	password2	direction2	password3	direction3	TotalCreateTime	PassTime1	PassTime2	PassTime3	SecretCode
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	seow	A1	TopLeft	B2	Top	C3	TopRight	8.378	5.344	1.526	1.508	seow
2	ks	A1	Left	L12	Right	W23	Bottom	5.824	2.558	1.594	1.672	ks
3	test	P16	BottomLeft	I9	Top	T20	TopRight	5.635	2.142	1.634	1.859	test

Figure 4.5.1 Example of User’s Table in SQLite database

	username	date	LoginTime	SuccessRate	LoginTime1	LoginTime2	LoginTime3
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	seow	2019-08-02	6.547	1	2.285	1.651	2.611
2	seow	2019-08-02	4.145	0	1.812	1.251	1.082
3	seow	2019-08-02	6.519	1	1.438	2.108	2.973
4	seow	2019-08-02	7.388	1	3.864	1.879	1.645

Figure 4.5.2 Example of Login Attempt’s Table in SQLite Database

Chapter 5 System Testing

For this project, the evaluation of usability of the proposed system is needed by making comparison with another two similar authentication system including Passfaces and Digraph Substitution Rules (DSR). There are three different sets of results to be analyzed. First set of result is the information collected from the survey questionnaire on the first day of test which is the day they fill the survey form after they finish learn how to use all systems before starting to login for five days. Every participants are required to fill in this survey form. The second set of results will be the survey form for shoulder-surfing test where participants will need to fill in the survey form after finish the test. Only ten participants will be selected to take shoulder-surfing test among all of the participants. Last but not least, the last set of result is the time recorded of five days login by all participants. There are two groups of participants which are ten participants login with five consecutive days and ten participants login every other day (day after tomorrow).

5.1 First User Study

5.1.1 Procedure

In first user study, participants were required to fill in their username, gender and knowledge about graphical password and shoulder-surfing attack. After that participants will need to learn how to use three different authentication systems including Passfaces, Digraph Substitution Rules (DSR) and proposed system to login on mobile application. Before start learning, the process of registration and login will be demonstrated to them for all three systems. Then they will need to register a new account and perform at least five times successful login for every systems. Next, after finish login for three systems then participants will had to continue fill up the survey including evaluation of the proposed system in seven questions and three questions of comparison between three different systems.

5.1.2 Results from Survey Questionnaire

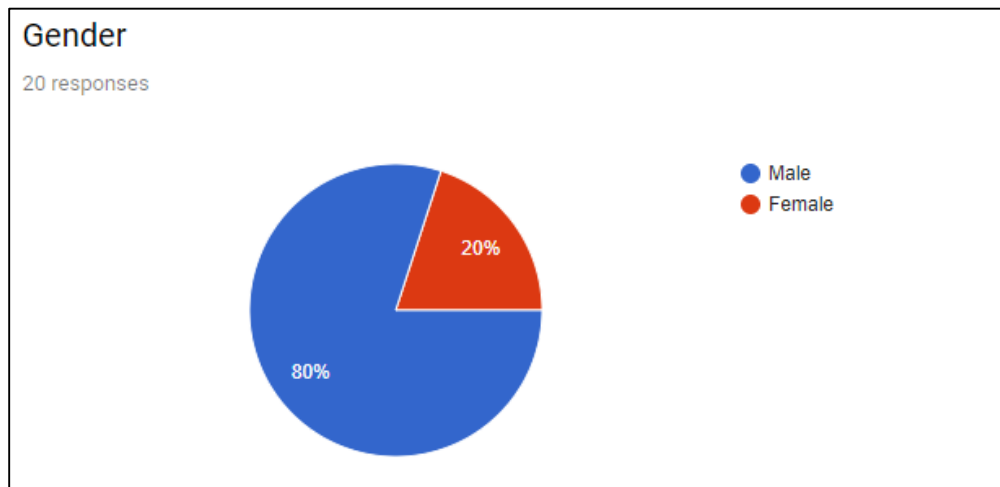


Figure 5.1.2.1 Pie Chart of Gender

From the pie chart shown above, it shows that majority of the participants are boys (80%) while only minority of them are girls (20%).

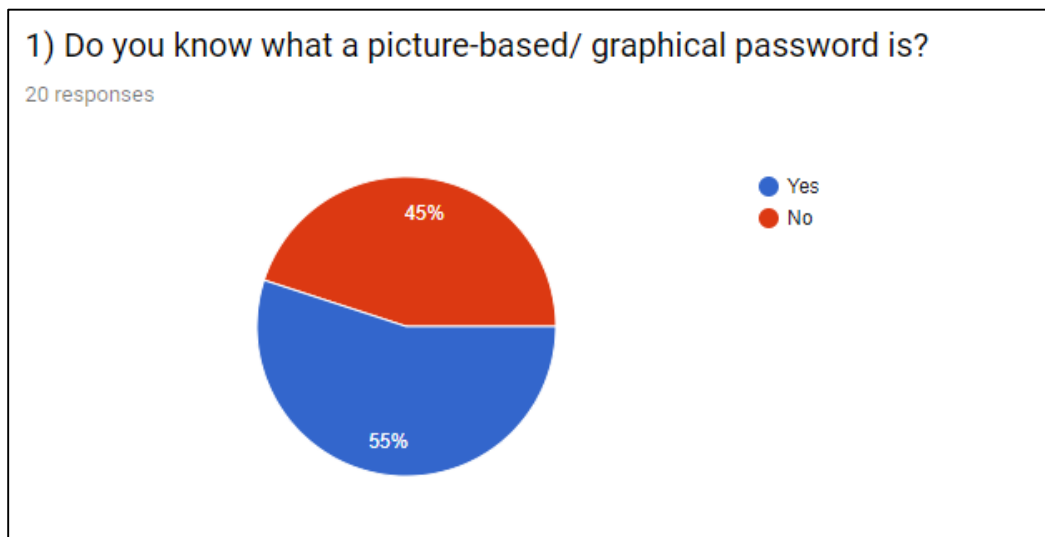


Figure 5.1.2.2 Pie Chart of knowledge about graphical password

Before start learning how to use the authentication system, participants will be asked about the knowledge of graphical password. Pie Chart above shown more than little half of them (55%) know what graphical password is, while another half of them (45%) does not know about that.

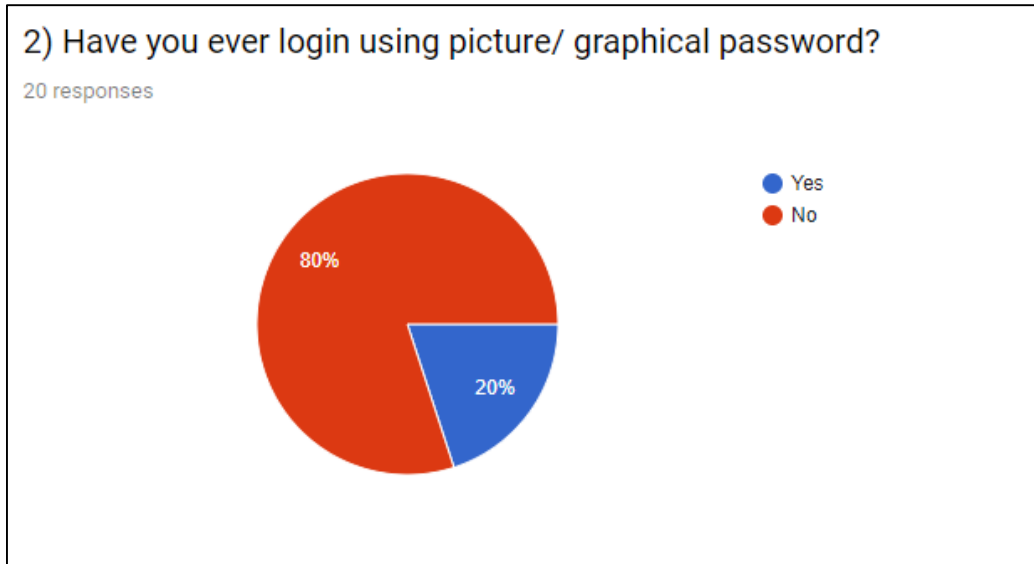


Figure 5.1.2.3 Pie Chart about experience of using graphical password

From the chart above shown majority of participants (80%) haven't using graphical password to login before, while only minority of them (20%) have experience in login with graphical password.

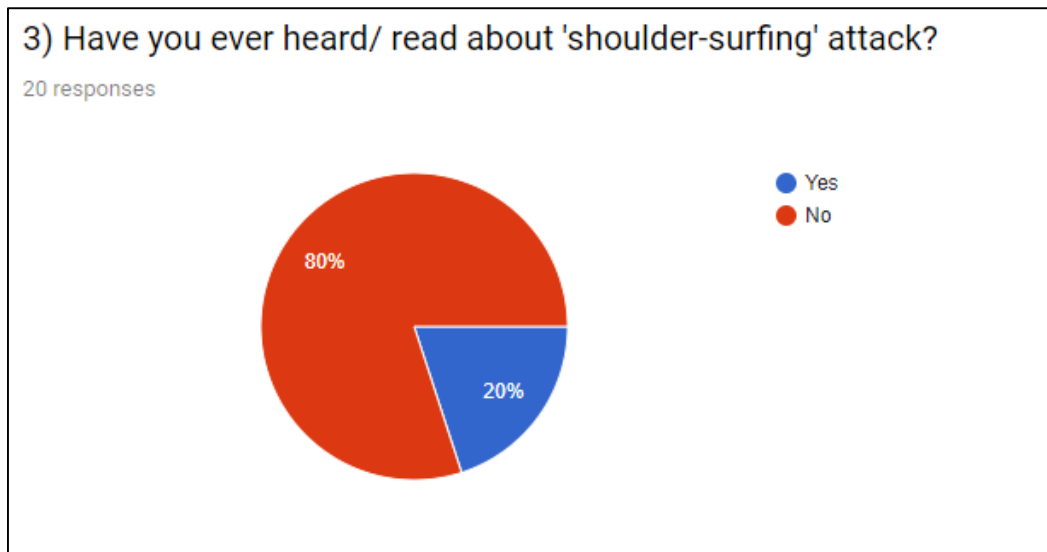


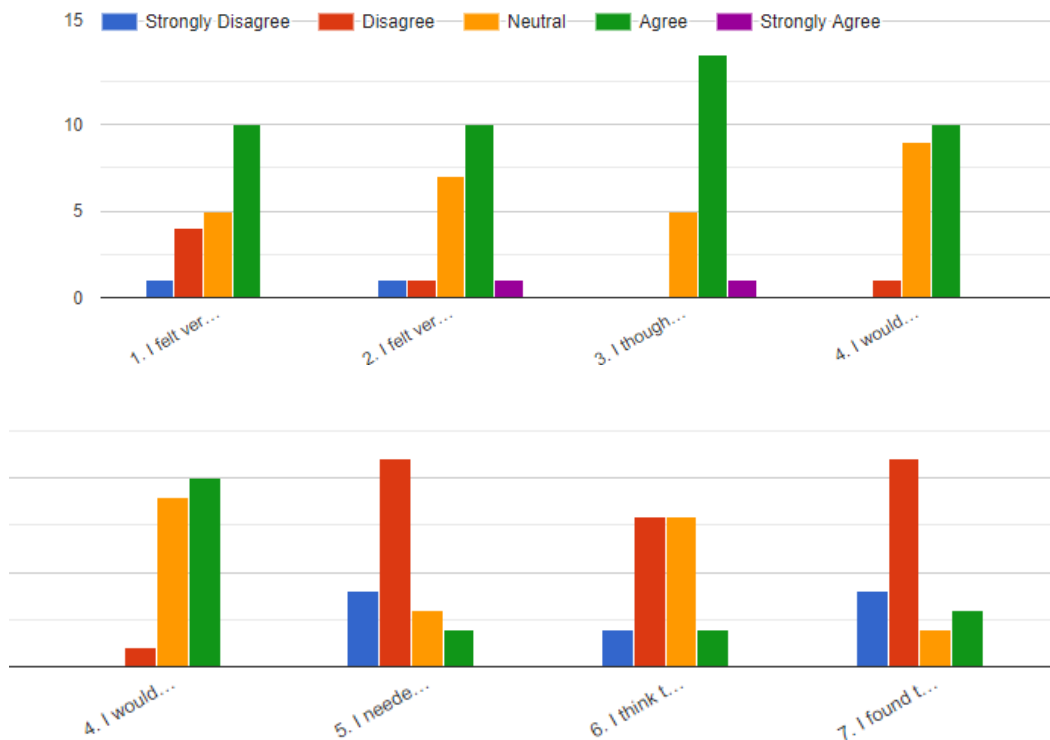
Figure 5.1.2.4 Pie Chart about knowledge about shoulder-surfing attack

Pie chart above shown that most of the participants (80%) does not know what is about shoulder-surfing attack, while only 20% of them have heard it before.

Post-test Questions 1

User need to LEARN the THREE system rules

Evaluate the proposed system:



1. I felt very easy in memorizing the password.
2. I felt very confident using the system.
3. I thought the system was easy to use.
4. I would imagine that most people would learn to use this system very quickly.
5. I needed to learn a lot of thing before I could get going with this system.
6. I think that I would like to use this system frequently.
7. I found the system unnecessarily complex.

Figure 5.1.2.5 Evaluation of Proposed system

Question 1: Most of them felt easy in memorizing the password because some of them are using same image or directions as their pass-image so that will bring convenience to them and also easier to memorize password. Half of them are neutral and below is because if they have more different image and directions so it will cause them more difficult to remember the password.

Chapter 5: System Testing

Question 2: It seems that most of the participants are being neutral and agree that they felt confident in using the proposed system.

Question 3: Most of the participants are agree that the proposed system is easy to use.

Question 4: Only half of the participants are agree in most people can learn the system quickly while another half are being neutral.

Question 5: From the chart above shows that most of the participants are disagree that they need to learn a lot things before get going with the system.

Question 6: This chart shows that most of the participants are neutral and disagree that they would like to frequently use this system. The reason is most people nowadays still preferring using traditional textual as their password instead of graphical password.

Question 7: Most of the participants are disagree that this proposed system is unnecessarily complex.

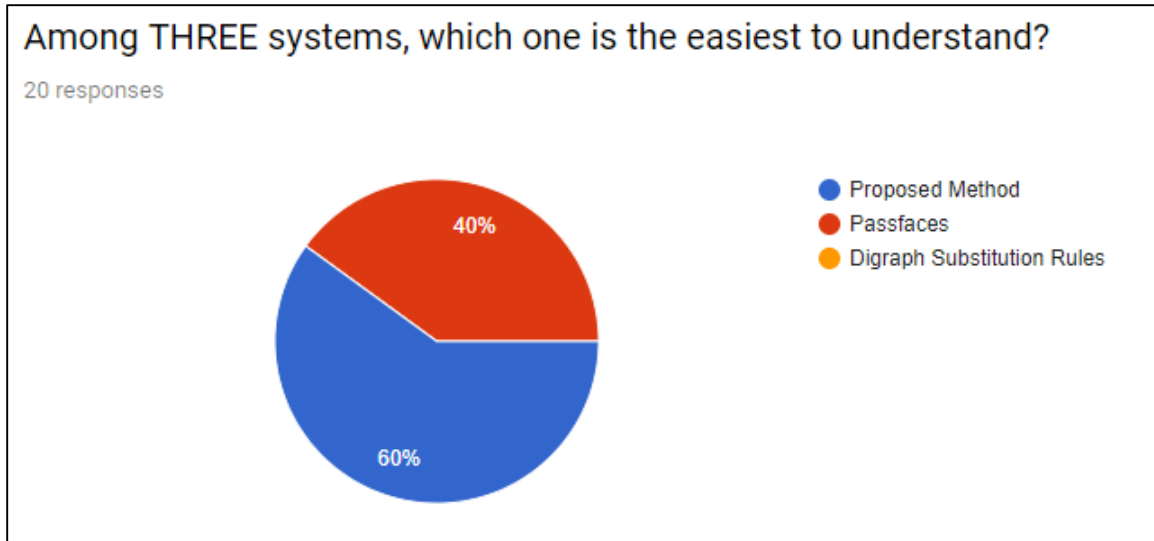


Figure 5.1.2.6 Pie Chart of participants' choice of best understandability

From the chart above shown that 60% of the participants think that proposed method are easier to understand while 40% of the participants think that Passfaces are easier to understand. The reason of why no participants will choose DSR because the rules in this system is quite complicated and hard for them to understand.

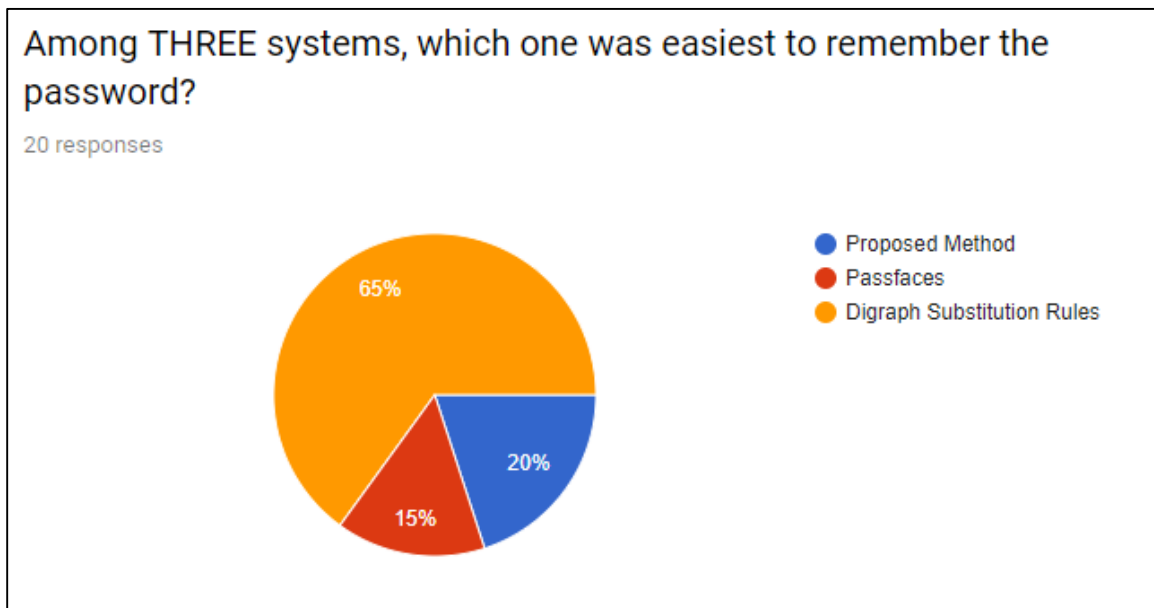


Figure 5.1.2.7 Pie Chart of participants' choice on best password memorability

We can see the results shown by the chart above that 65% of the participants are choosing DSR as the easiest to remember the password because DSR only need to remember two image and a choice. While proposed method had to remember three image and three directions although they can choose the same image or directions, Passfaces is the least participants choose because they are having difficulty in remember human face which difference is not much with only men and women.

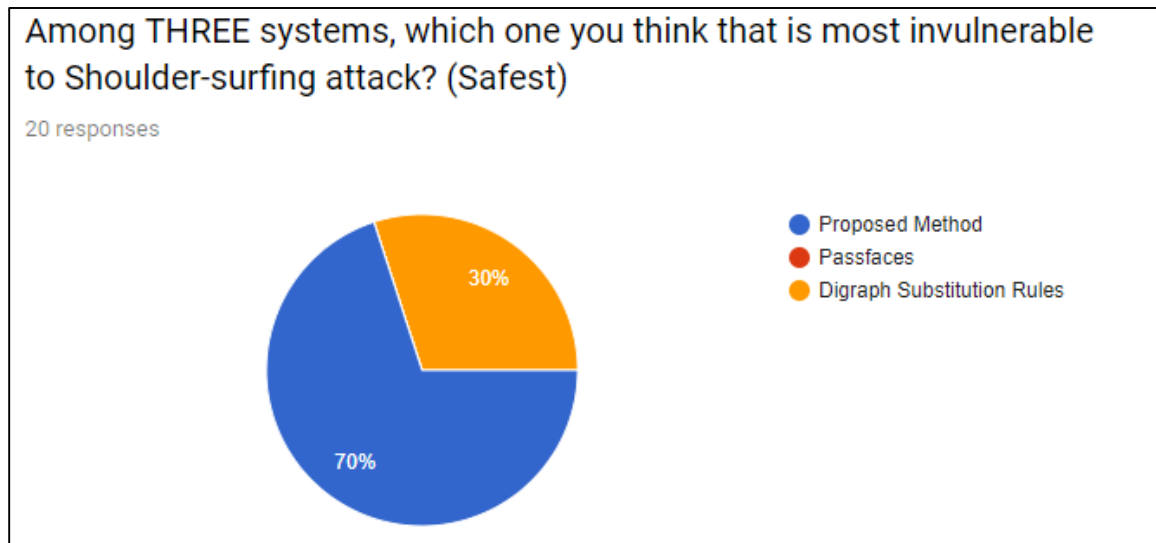


Figure 5.1.2.8 Pie Chart of participants' on best system security

From the chart shown above, 70% of the participants are select proposed method as the safest system against shoulder-surfing attack while only 30% of them select DSR as the safest system. There is no participants select Passfaces because people can remember the faces image they clicked and is vulnerable to shoulder-surfing attack. Although DSR can resist to shoulder-surfing attack but if the attacker perform more analyze to their password attempt, the system still have some vulnerability to shoulder-surfing attack compared to the proposed system.

5.2 Second User Study

5.2.1 Procedure

The second user study is consist of shoulder-surfing attack test which may need participants to perform shoulder-surfing attack by watching a video clip of user login using three different authentication system including proposed system, Passfaces and DSR. After finish fill up the survey form of first user study, only ten participants will be selected to going this shoulder-surfing test. A user account will be registered for all three different authentication systems. At first, participants are required to watch a video clip of first attempt to login into system. After finish watching the video clip, participants have three attempt chances to successfully login into the account by performing attack. If they were not able to login into the test account, then participants will watching user login video clip with second and third attempt. Next, participants will also have another three attempt chances can try to successfully login into the test account. All of the steps mentioned above are repeated for all three systems. Then participants were required to fill in the survey form after the test.

5.2.2 Results Collected from Shoulder-surfing test Survey Form

Shoulder-surfing test 1: Proposed System

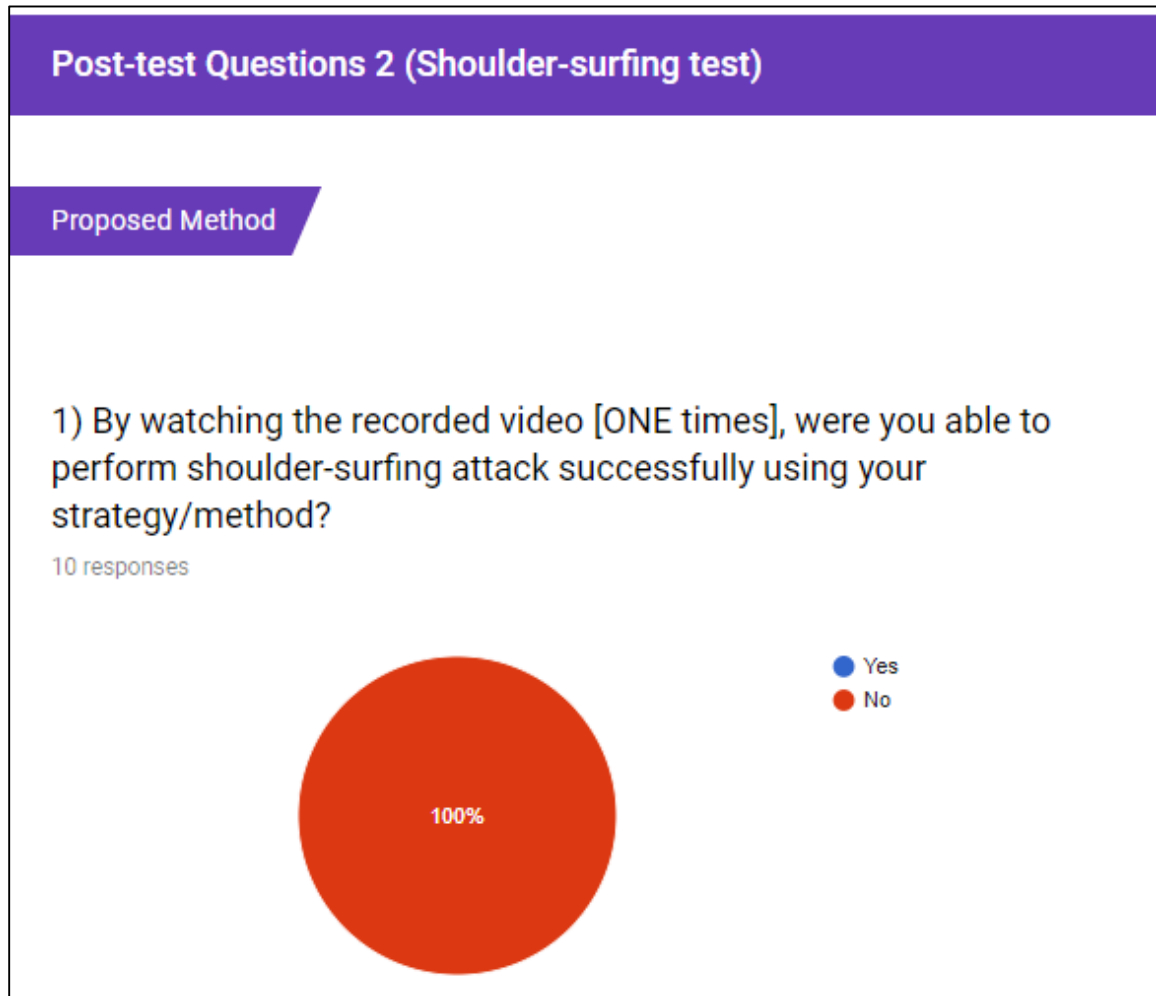


Figure 5.2.2.1 Chart of first attack trial for proposed method

From the chart above shown that all participants are not able to perform attack and not able to login into the test account. This prove that the proposed system can completely resist to shoulder-surfing attack if attacker perform first time attack. Because the test account only can be login with all three correct image and directions and cannot login even one of pass-image is wrong. If the attacker is performing password guessing, then the complexity of the password will be $8 \times 8 \times 8 = 512$ and password guess is very hard to get the right answer.

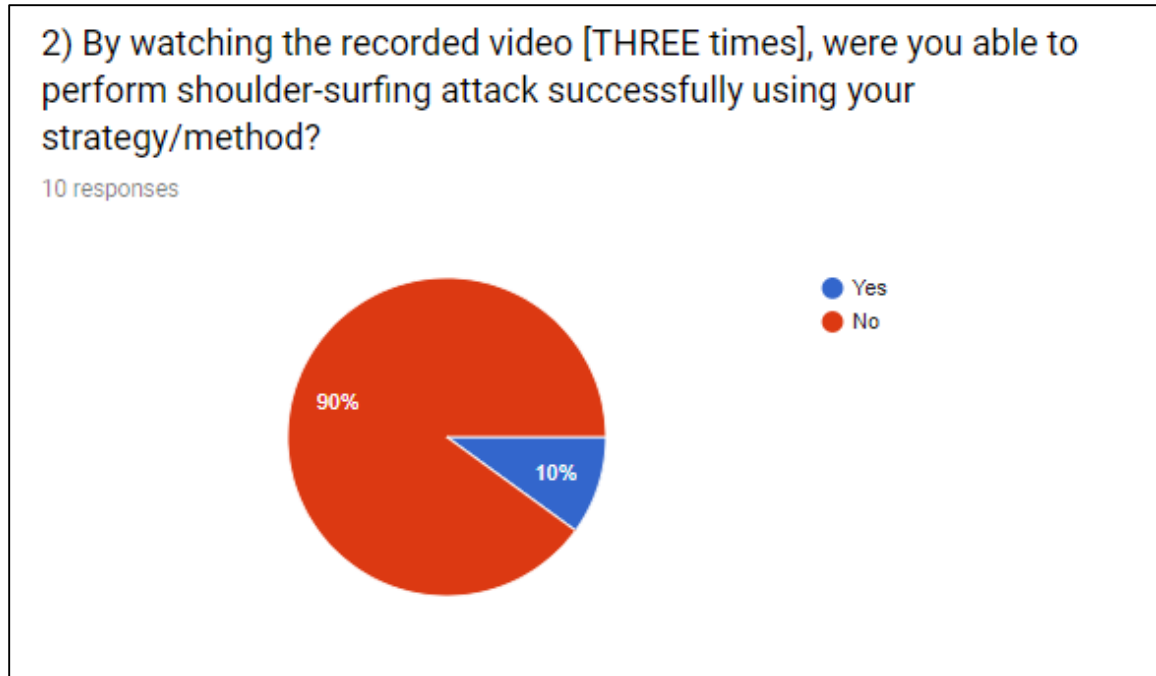


Figure 5.2.2.2 Chart of second attack trial for proposed system

Chart above shows that nine out of ten participants were still not able to successfully login into the test account by performing shoulder-surfing attack. The reason is because they had to compare too many pictures of attempt to find out the answer and they felt frustrated and give up to perform attack. They are having difficulties in remembering all eight pictures beside the image clicked and also three pass-image with three attempts, because they need to spend too much effort so most of them give up even to try to login into the test account. As the chosen one, there is one participants are willingly to spend more effort by taking pictures of every attempt and every pass-image clicked then compare and analyzed to find out the real password. Although he spend much times in recording the pictures and analyze the real password, but finally he successfully login into the test account after he putting so much effort into it. This prove that the proposed system can completely resist to single shoulder-surfing attack but still vulnerable to multiple shoulder-surfing attacks.

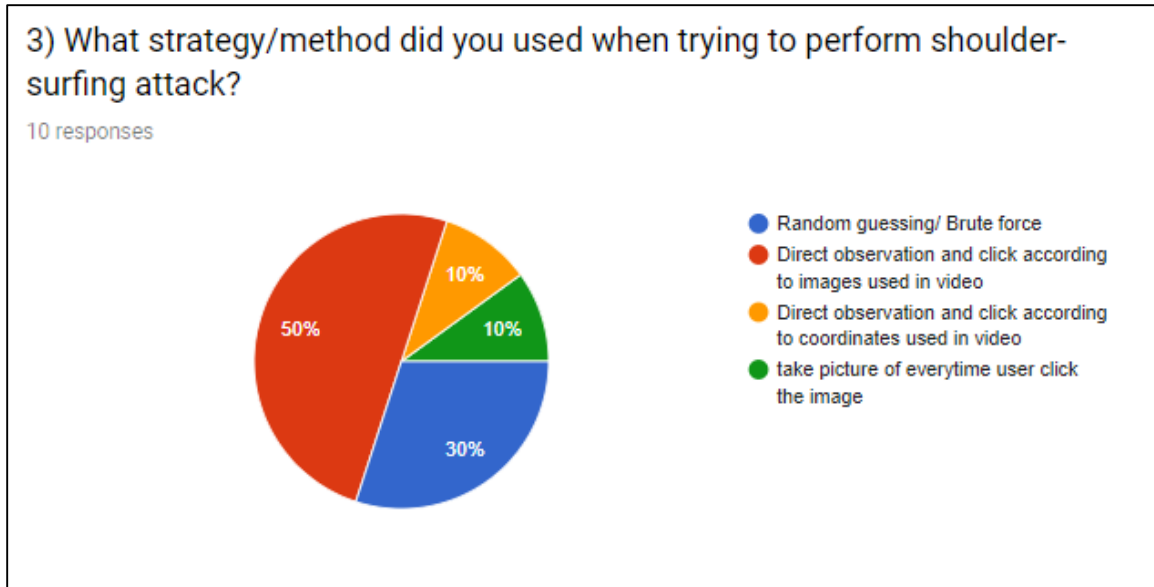


Figure 5.2.2.3 Chart of participants' attack method for proposed system

Chart above shown half of the participants are using direct observation according the images used in video to find the real pass-image while 30% of them are random guessing.

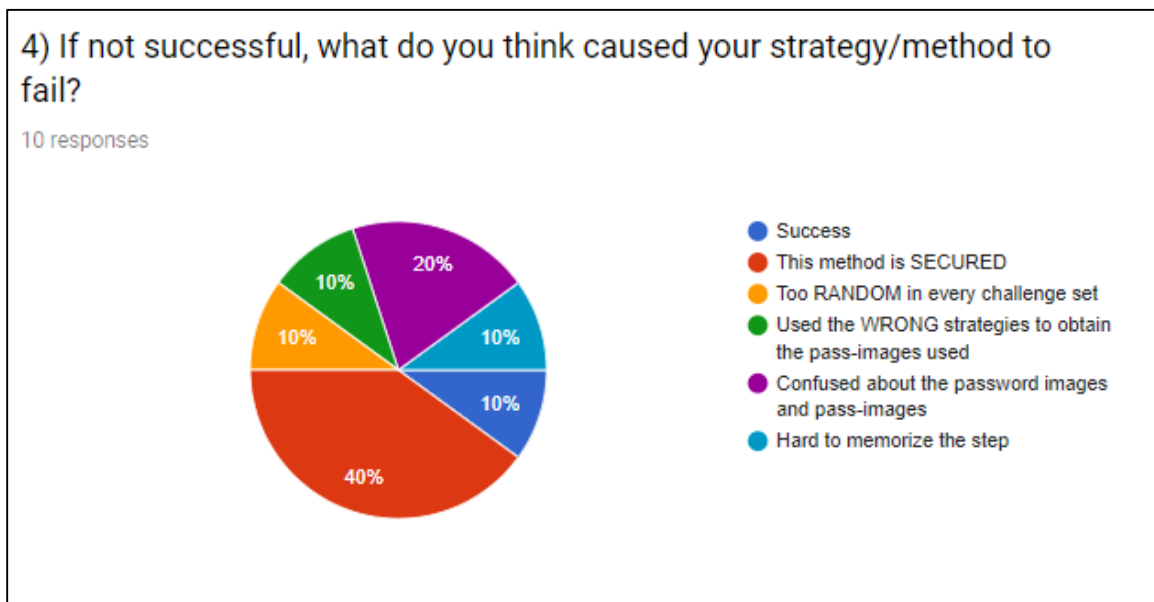


Figure 5.2.2.4 Chart of reason of unsuccessful login

Four of the participants agree that the proposed method is secured while two of them are confused about the password images while minority of them are having their own reason.

Shoulder-surfing test 2: Passfaces

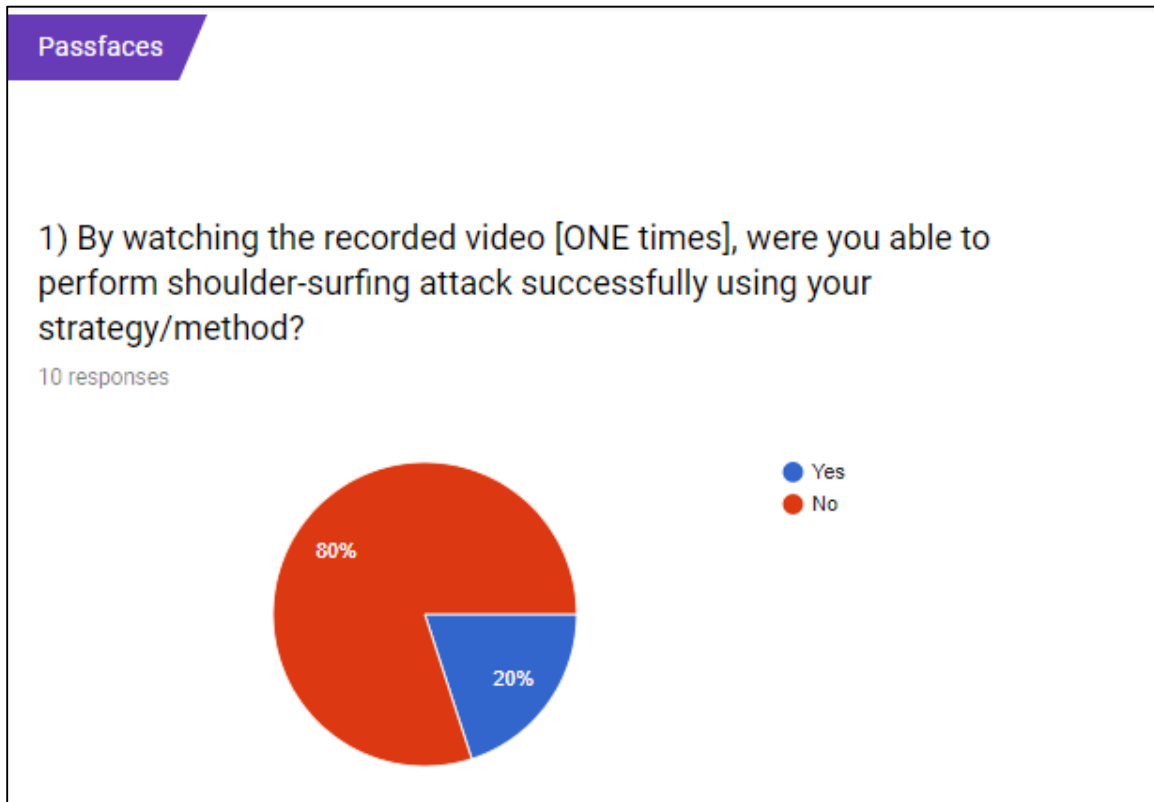


Figure 5.2.2.5 Chart of first attack trial for Passfaces

From the chart shown above, eight out of ten participants are not able to login into the test account of Passfaces system. This is because they might not that easy in remembering the faces the see for the first time in the video clip so they were not able to login. While only two of them were successfully login into the test account in first attempt trial because they might have stronger memorability that can easier remember the face images used in the video clip.

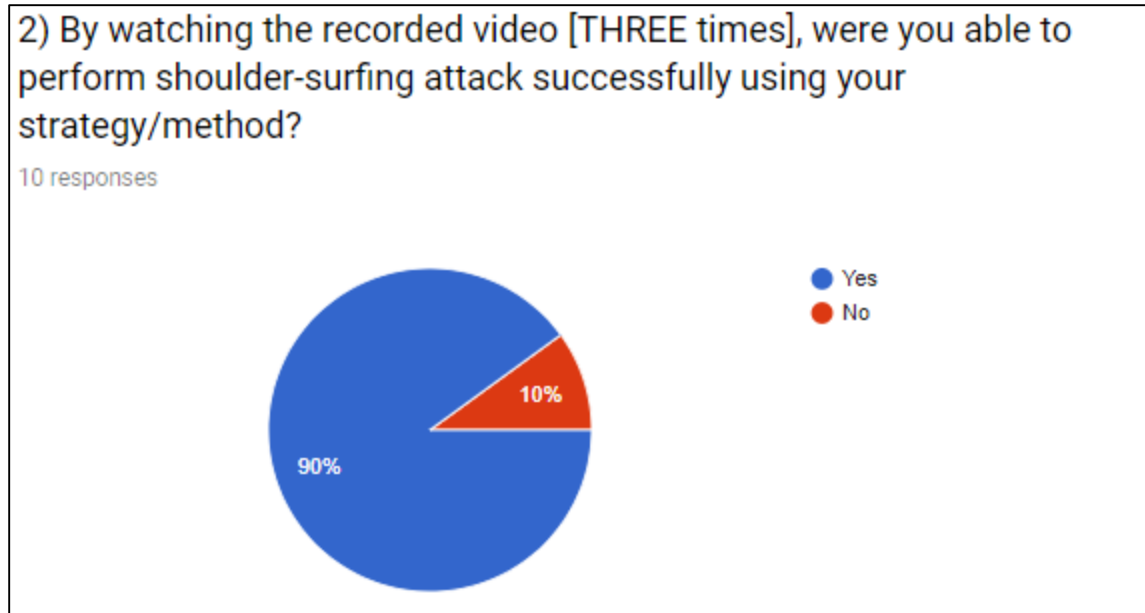


Figure 5.2.2.6 Chart of second attack trial for Passfaces

After watching three times of user login with Passfaces system, nine of the participants were able to successfully login into the test account. They should be easily remember the face images after many times of watching the video clip so they can login into it. There are one participants that still cannot login into the test account after watching three video clip, the reason may because the person have weak memorability in remembering people faces. This prove that Passfaces is quite vulnerable to shoulder-surfing attack.

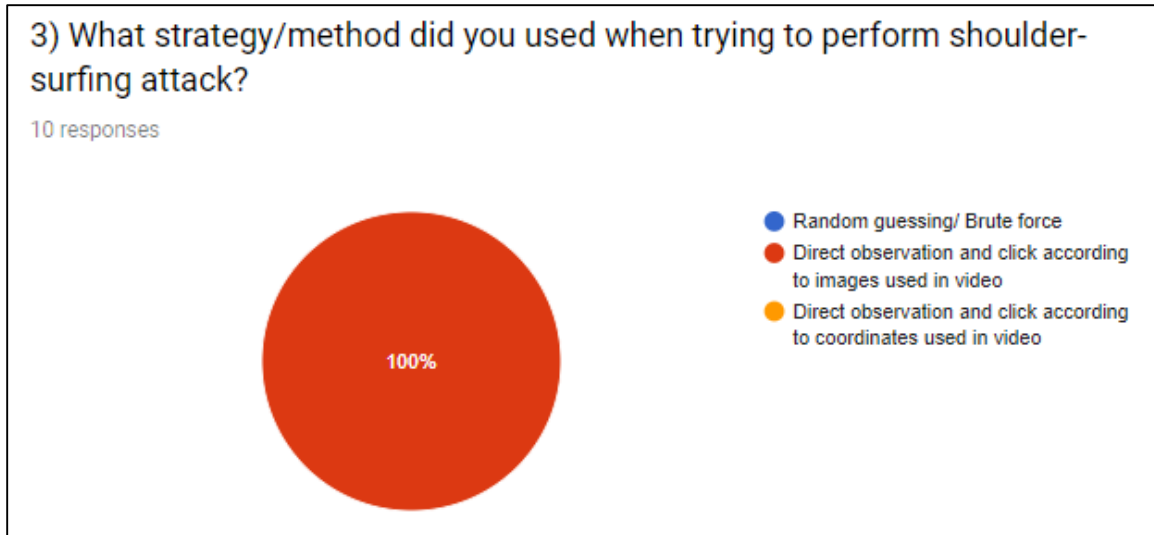


Figure 5.2.2.7 Chart of participants' attack method for Passfaces

The chart above shown that all the participants are using method with direct observation and click according the images used in video because it is so directly login with the face image used.

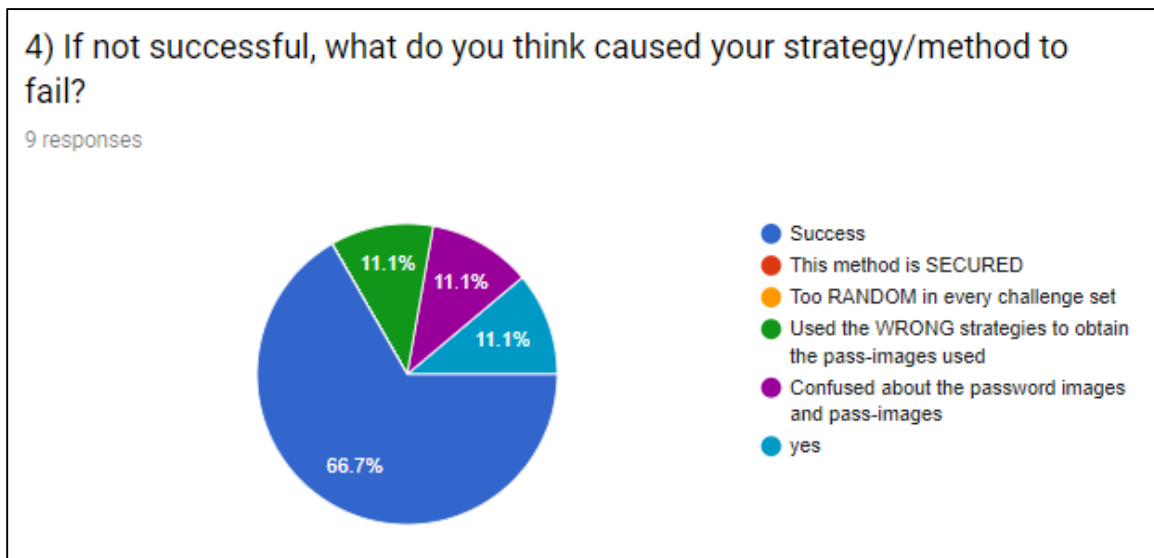


Figure 5.2.2.8 Chart of reason of unsuccessful login

Chart above show majority of them are successfully login into the test account while less of them are having other reason. There are missing one responses due to technical issues while setting the questions at start.

Shoulder-surfing test 3: Digraph Substitution Rules (DSR)

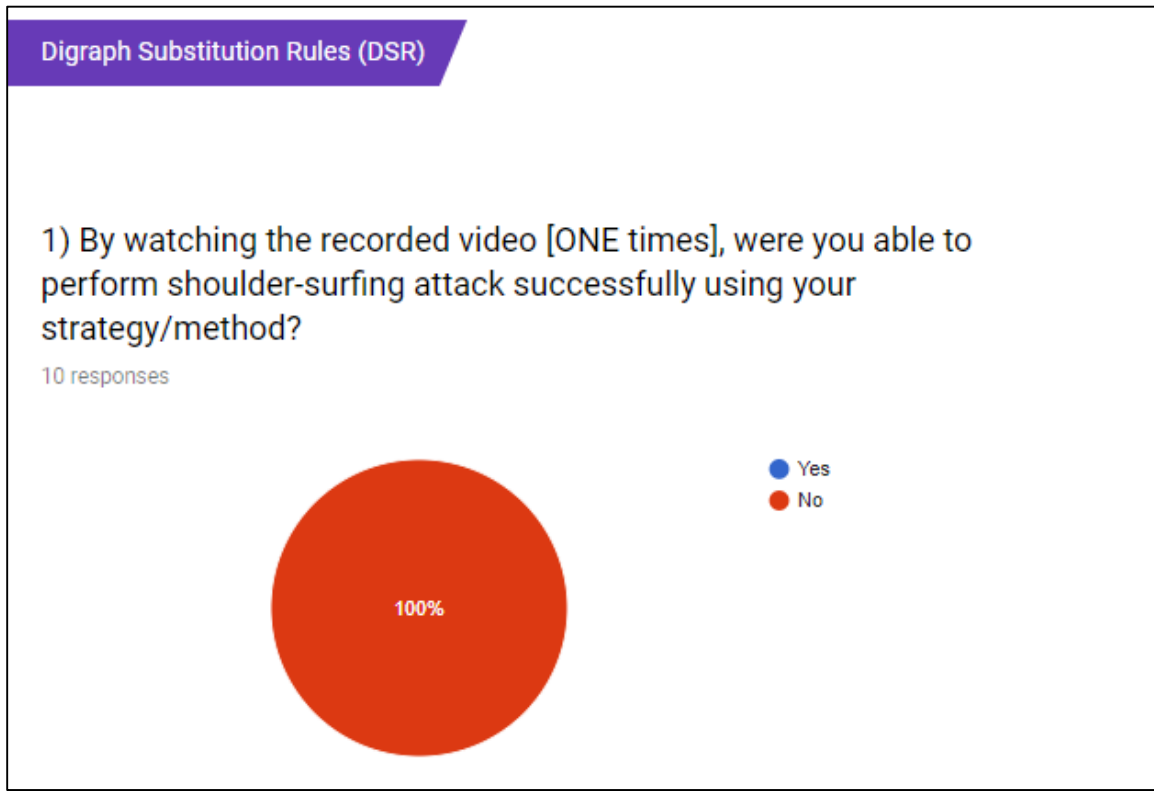


Figure 5.2.2.9 Chart of first attack trial for DSR

From the chart above shown that all of the participants were not able to login into the test account of DSR system. They tried to remember the location of image used by user in video clip to analyzed but failed because first time is not enough for them to perform attack. This can prove that DSR system is stronger and more invulnerable to shoulder-surfing attack compared to Passfaces.

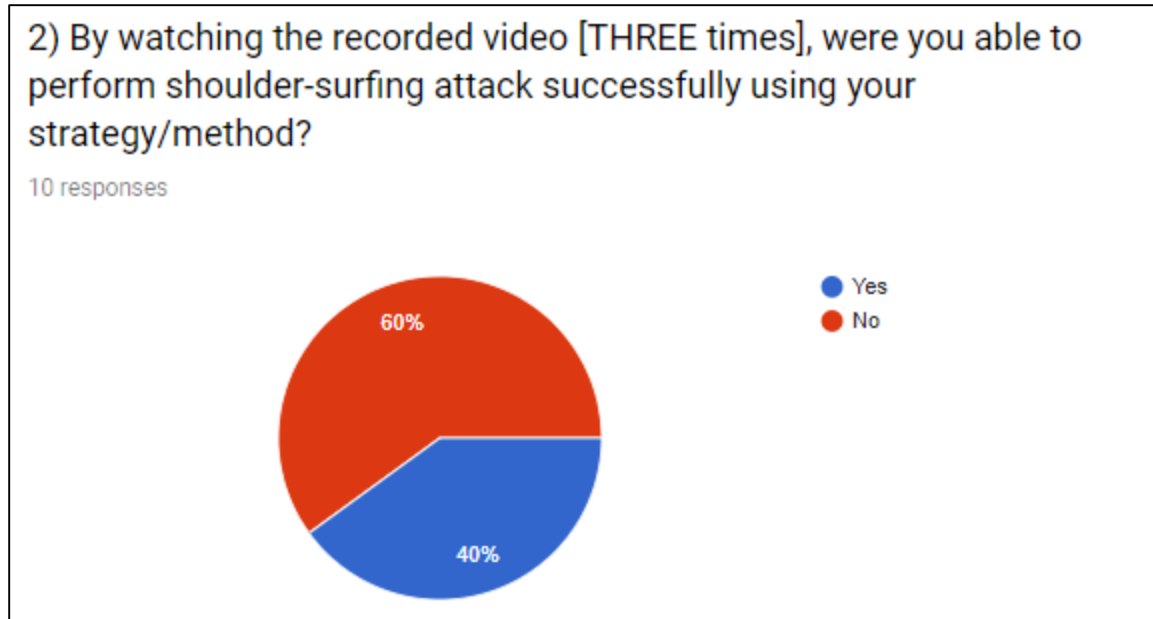


Figure 5.2.2.10 Chart of second attack trial for DSR

The chart above shows that six out of ten participants were able to successfully login into test account by performing shoulder-surfing attacks. They spend some effort by taking pictures all every attempt and compare it to analyze the real password because the real password must be in the same row or column of the pass-image clicked in the video so they were still able to successfully login into the account after they find out the real pass-image. This prove that DSR system is more vulnerable to multiple shoulder-surfing attack and still can be break through if attacker analyzed the password of every attempt.

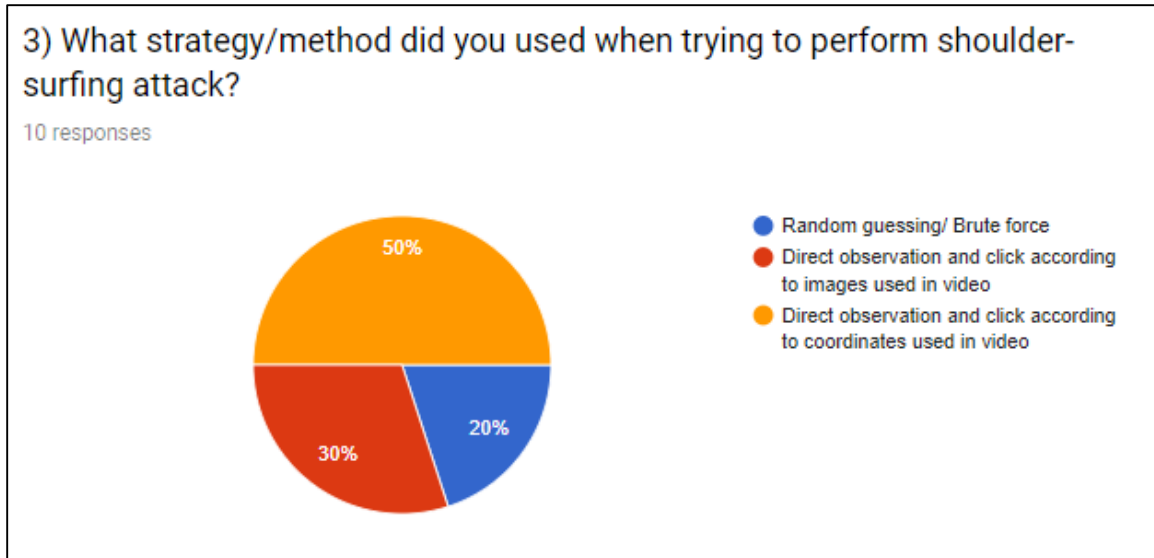


Figure 5.2.2.11 Chart of participants' attack method for DSR

From the chart above, half of the participants used method of direct observation according to coordinates used in video to find out their real pass-image. Another half might fail to login so they used other method.

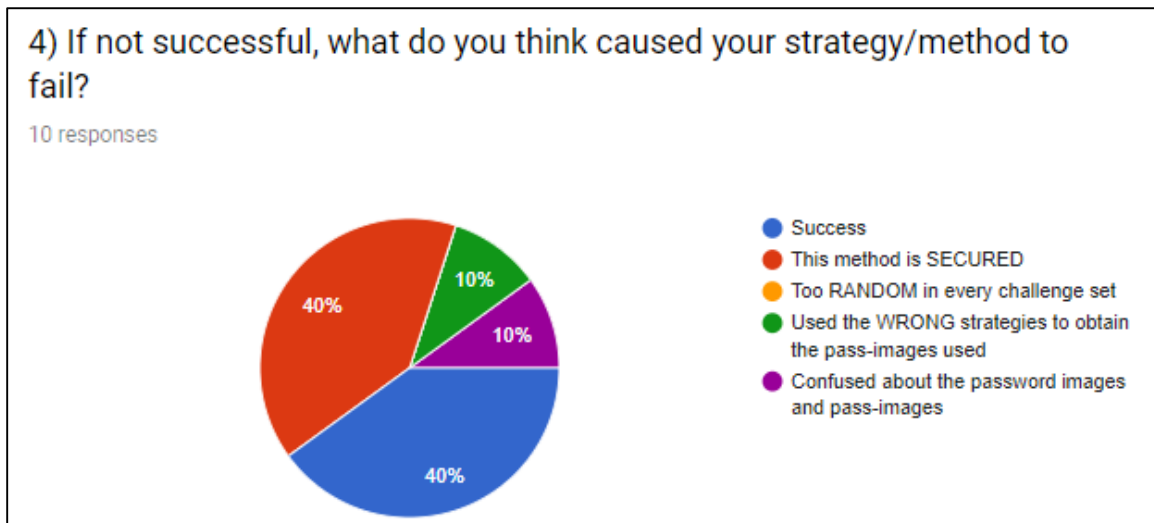


Figure 5.2.2.12 Chart of reason of unsuccessful login

The chart above shows that four of them are able to successfully login into the account while four of them think that DSR system is secured while another two of them is other reasons.

5.3 Accuracy

After finish fill up the survey form and learn all three different systems of how to user and login. Participants had to perform login for the proposed system for five days with at least five successful login attempt each days. The login time for each pass-image, total time and success rate is recorded inside the database. Only successful login will be count as successful attempt. The system accuracy can be determined by the number of successful login attempts out of total number of login attempts including successful and fail attempts. The formula to calculate the system accuracy is defined as below:

$$\text{Accuracy} = \frac{\text{Successful login Attempts}}{\text{Total Login Attempts}} \times 100$$

Proposed system Accuracy:

$$\text{Accuracy} = \frac{300}{312} \times 100$$

Total Login Attempts: 312

Total Successful Login Attempts: 20x (5x3) =300

System	Accuracy (%)
Proposed System	96.15%

Table 5.3.1 Proposed System Accuracy

Table above show that the proposed system have accuracy of 96.15%. Only total of twelve fail attempts among twenty participants. One of the reason is they might using forgot password to let them remember password in case they forgot their password so they were not that easily failed. Even once they failed, they will go to forgot password to retrieve their password to successfully login. Most of them are having same images or same directions so they could easier to remember the image and directions. This prove that the proposed system have high accuracy and user are easier to login successfully.

5.4 Usability

To find out the usability of the proposed system, every user login attempts will be recorded including total time, first pass-image time, second pass-image time and third pass-image time. The formula to calculate the average login time is define as below:

$$\text{Average Login Time} = \frac{\text{Sum of login time of total login attempts}}{\text{Total number of login attempts}}$$

Registration Time

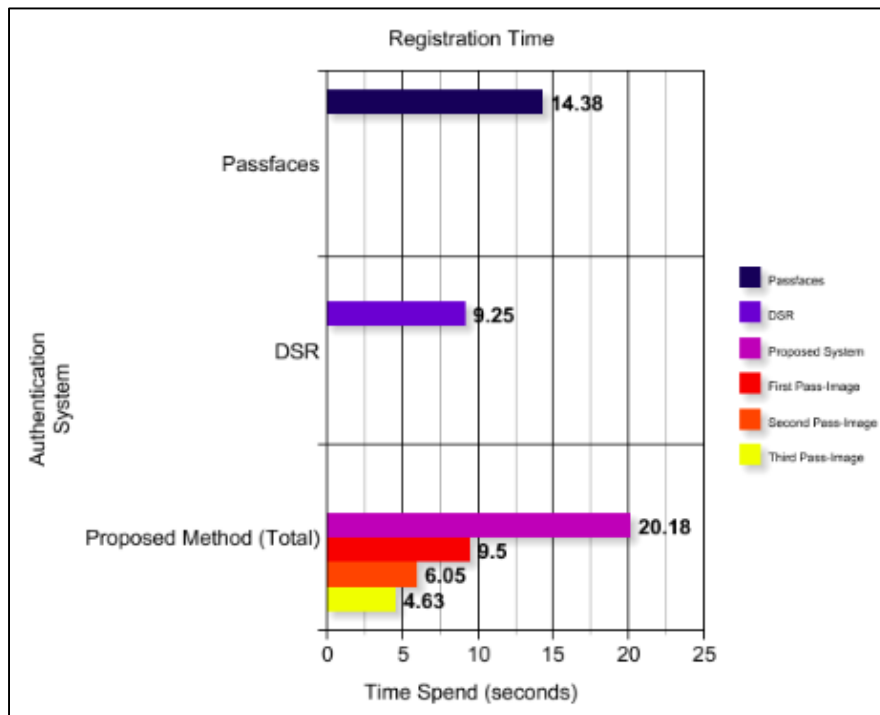


Figure 5.4.1 Registration time of three authentication systems

System	Average Registration Time (seconds)	
Passfaces	14.38	
DSR	9.25	
Proposed System	Total:	20.18
	First Pass-Image:	9.5
	Second Pass-Image:	6.05
	Third Pass-Image:	4.63

Table 5.4.1 Registration time of three authentication systems

From chart and table above shown that the shortest time needed to register an account is DSR because DSR system only need to select two images and one choice so that is faster compared to other two systems. While Passfaces has average register time of 14.38 seconds which higher registration time than DSR but still lower than the proposed system because user will need to first identify the faces then carefully pick the faces that they easier to remember and easy to be recognize during login. Proposed system is the highest average registration time to register an account, the reason is proposed system required user to register three images and three directions which like six things to be remember and it cause the registration time to be longer than other system. Although users are allowed to register same image or same directions so some of them would be faster while register for second and third pass-image.

Login Time

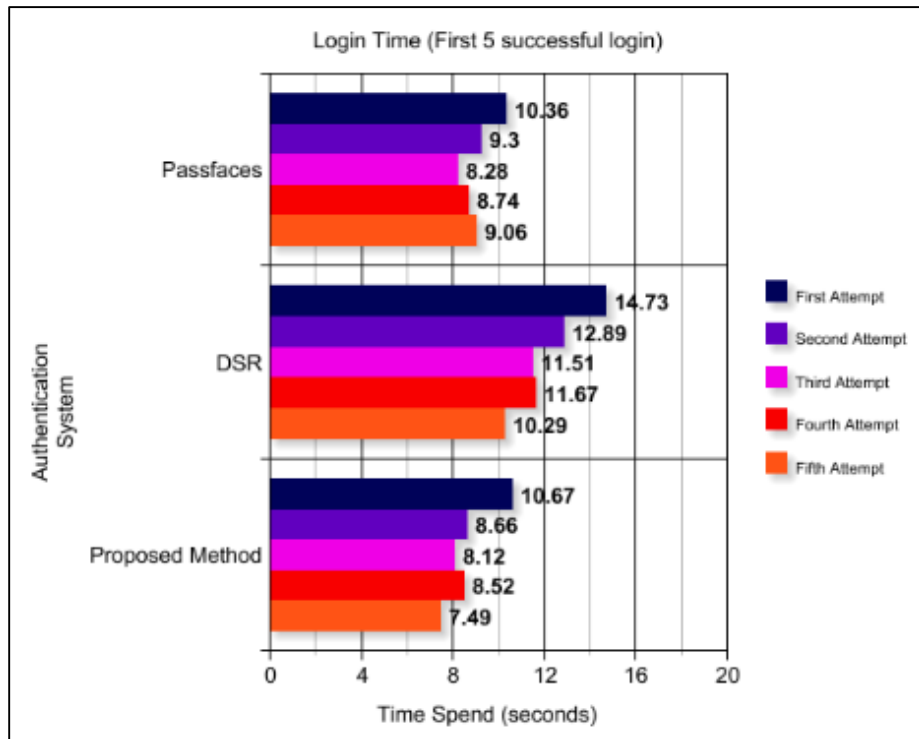


Figure 5.4.2 Login time of three authentication systems on first day

System	Average Login Time (seconds)				
	First	Second	Third	Fourth	Fifth
Passfaces	10.36	9.3	8.28	8.74	9.06
DSR	14.73	12.89	11.51	11.67	10.29
Proposed Method	10.67	8.66	8.12	7.52	7.49

Table 5.4.2 Login time of three authentication systems on first day

For the login time at the first day user learn how to use the three authentication systems and after they register an account. Every login attempts of first five time is recorded to make a comparison between three systems. The chart shows that DSR system is the highest average of login time in every attempt of all attempts are above ten seconds. It is because the rules of DSR system is quite complicated and user are harder to find the pass-image so they need to spend more time during login. Passfaces and proposed system are having some similar average login time and proposed system are slightly shorter time than Passfaces. The reason is user had to spend some time in recognize twenty-five different face to find their pass-image and human faces are not much different compared to proposed system which using twenty-five different images including animals, human and other things which easier to recognize.

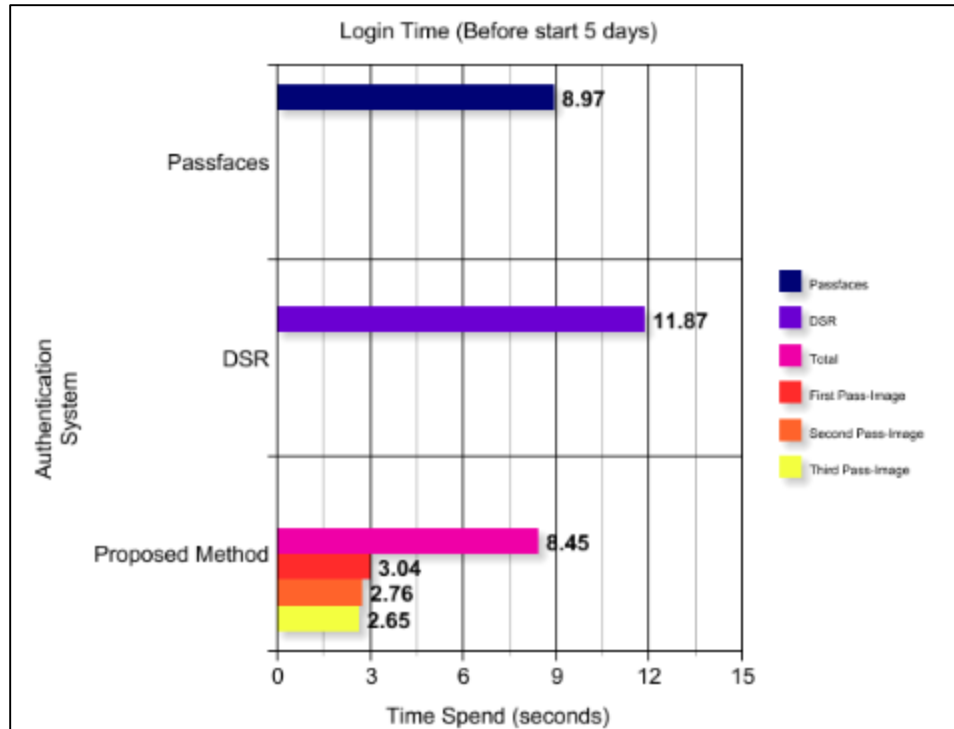


Figure 5.4.3 Average Login Time of three systems on first day

System	Average Login Time (seconds)	
Passfaces	8.97	
DSR	11.87	
Proposed System	Total:	8.45
	First Pass-Image:	3.04
	Second Pass-Image:	2.76
	Third Pass-Image:	2.65

Table 5.4.3 Average Login Time of three systems on first day

Chart and table above shows average login time of three systems on first day which total of five successful login attempts for each systems. DSR have longest average login time at first day while Passfaces have average login time of 8.97 seconds and proposed method only slightly less than Passfaces which only had average login time of 6.45 seconds. The reason is same as last chart mentioned.

Login Time (Start of five day)

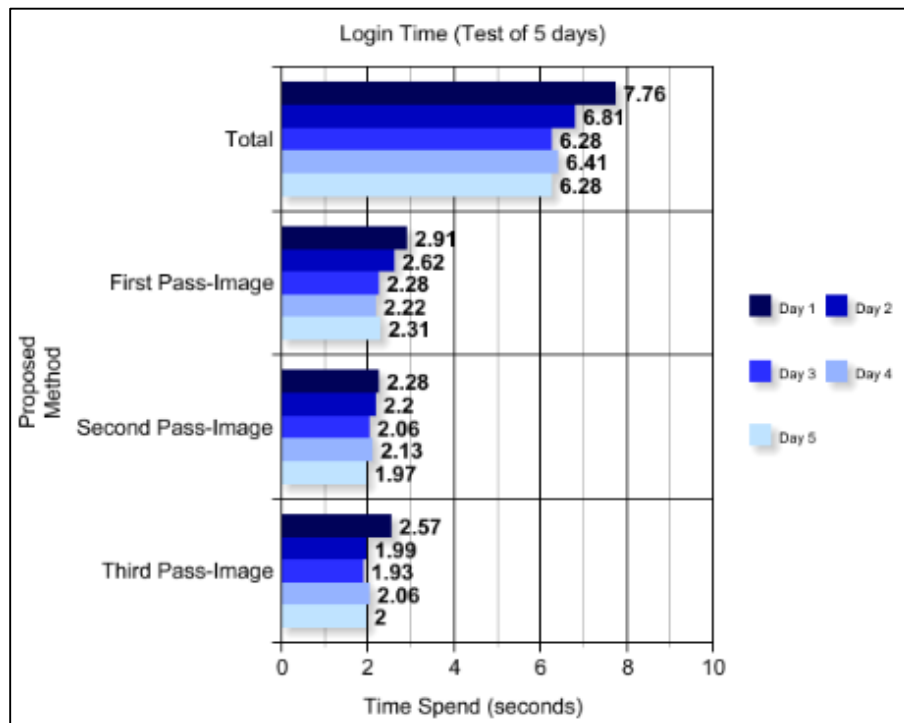


Figure 5.4.4 Average Login time of proposed system for total five days

Pass-Image	Average Login Time (seconds)				
	Day 1	Day 2	Day 3	Day 4	Day 5
Total	7.76	6.81	6.28	6.41	6.28
First	2.91	2.62	2.28	2.22	2.31
Second	2.28	2.2	2.06	2.13	1.97
Third	2.57	1.99	1.93	2.06	2.00

Table 5.4.4 Average Login time of proposed system for total five days

Chart and table above shows average login time of twenty participants in five days. At first day, the average of total login time is 7.78 seconds and it drops to around 6.28 seconds from day 1 to day 5. First Pass-Image login time was drop from 2.91 seconds on day 1 to around 2.31 at day 5. First pass-image will be slightly longer than second and third pass-image because participants might have to consider a while to remember their password

before click the image. Second and third pass-image are having similar range of times which it start drop to around 2.2 seconds from day 2 to around 2 seconds in day 5.

The participants will be separated into two groups of group test 1 and group test 2 with each contain of ten participants. Group test 1 will login into the system for five consecutive days, while group test 2 will login into the system every other day.

Group Test 1

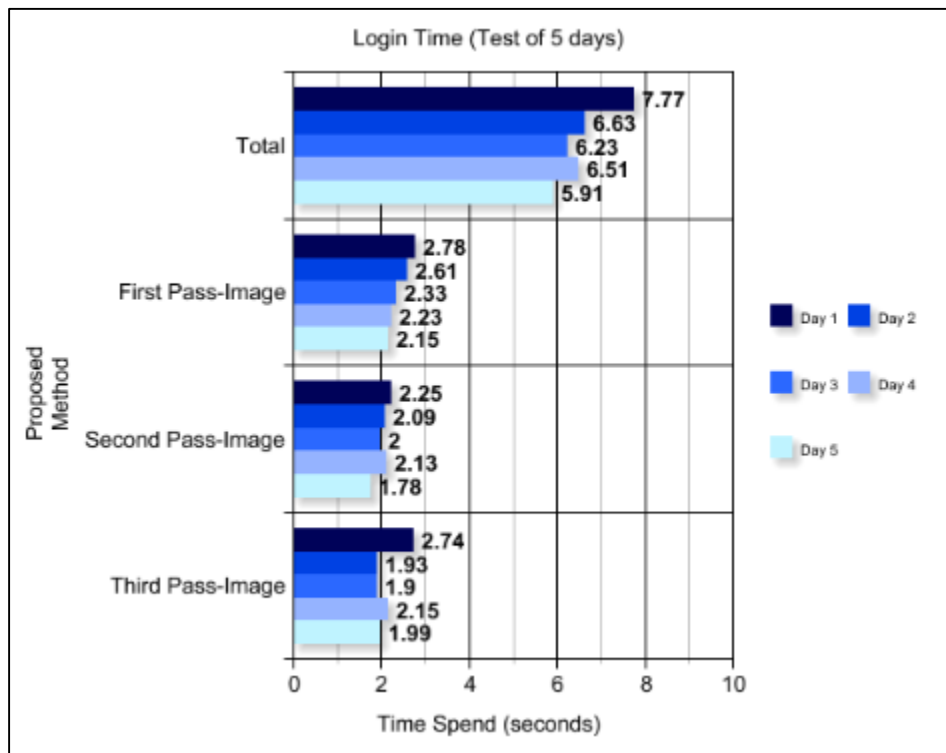


Figure 5.4.5 Average Login time of proposed system for total five days (Group 1)

Pass-Image	Average Login Time (seconds)				
	Day 1	Day 2	Day 3	Day 4	Day 5
Total	7.77	6.63	6.23	6.51	5.91
First	2.76	2.61	2.33	2.23	2.15
Second	2.25	2.09	2.00	2.13	1.78
Third	2.74	1.93	1.9	2.15	1.99

Table 5.4.5 Average Login time of proposed system for total five days (Group 1)

Group Test 2

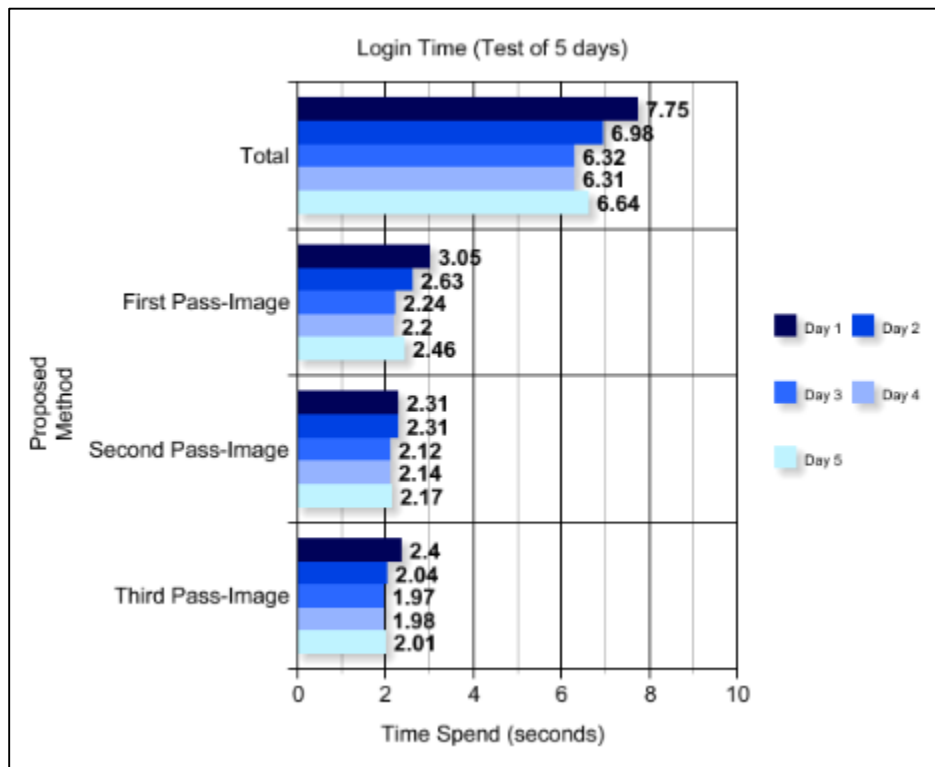


Figure 5.4.6 Average Login time of proposed system for total five days (Group 2)

Pass-Image	Average Login Time (seconds)				
	Day 1	Day 2	Day 3	Day 4	Day 5
Total	7.75	6.98	6.32	6.31	6.64
First	3.05	2.63	2.24	2.2	2.46
Second	2.31	2.31	2.12	2.14	2.17
Third	2.4	2.04	1.97	1.98	2.01

Table 5.4.6 Average Login time of proposed system for total five days (Group 2)

From the chart and table from group test 1 and 2, it shows that there is not much different during Day 1. Then the difference start to become bigger from Day 2 which group test 1 only have 6.63 seconds of average total login time while Day 2 of group test 2 have average

total login time of 6.98 seconds. Although both looks similar in Day 3, the biggest difference will be at Day 4 and Day 5. At Day 5, the average total login time of group test 1 which is only 5.91 seconds while group test 2 have 6.64 seconds which longer than before. The reason is if participants in group test 1 are login into the system with five consecutive days, they will not easily forget their password and will have better password memorability because they have to login everyday so they have shorter login time. While participants in group test 2 will have interval of one empty day in each of five days so they will have weaker password memorability because they will only have to login every 2 days and they will have longer time spend to login into the proposed system.

5.5 Security Analysis against Shoulder Surfing Attack

Shoulder-surfing attack is a common attack we can see nowadays in everywhere because it can be easily trigger by any strangers to perform attack. In this project, three different graphical authentication system are being compared to test its vulnerability to shoulder-surfing attack including Passfaces, DSR and proposed system. For Passfaces, almost all of the participants are able to crack the password to login into user account while DSR have almost half of them are able to login into the test account after perform multiple shoulder-surfing attack and analyze the real pass-image. Some of them are taking pictures to compared it or record the video to find out the real pass-image. For the case of Passfaces, participants only need to remember the faces clicked by user in video to find out the pass-image. While DSR have more complex algorithm so participants will harder to crack the password but still able to crack it after they willingly to put much effort into it, so it's only can say that it is partially invulnerable to shoulder-surfing attack. For the proposed system, it can completely prevent shoulder-surfing attack if attacker only see one attempt of user login but if the attacker perform multiple shoulder-surfing attack and compare many attempts together then they could easily find out the real pass-image. It still can be say that it can avoid shoulder-surfing attack but not multiple shoulder-surfing attack.

Chapter 6 Discussion

Ability to Achieve Project Objective

This project manage to achieve all the project objective stated above. The proposed method is able to resist to shoulder-surfing attack by its own algorithm. This can be prove through the shoulder-surfing test results that shows no one can crack the password of proposed system. User can easily learn the algorithm or the proposed system and they also can easily understand how it works and how to use. Although the data collected above shows that most of user spend more time in register their account because it's including three image and three directions to be choose by user and it should need more time to register. But there is balance between security of system and password memorability. If the password is too simply, then the system security will also be weaken. So to increase the security of system, the difficulty of password memorability will also be increased.

Limitations of the System

There are some limitation of this proposed system in the project. The first limitation of the system is it using SQLite which only implemented for local data storage instead of online firebase. The reason why I code it as offline because it was easier compared to online which more complex, harder and take more time for me to research and learn the code. Although this is not convenience to the user if I want to collect the data of login attempt after five days from the participants. For the shoulder-surfing test, I can see that most of them are unable to perform attack to my proposed system if they only see the login once, I found that if they see more than twice it could be more easier to know the real pass-image used to login into the system which vulnerable to attack that can compared different login session.

Future Works

For future works, the proposed system can be implemented through online server and database instead of offline database in this project as enhancement. By using online implementation, all data will be keep on online databases in server and will be easier to manage and collect data to be analyze. The proposed system will also add a reset password function which will send a reset password confirmation to the e-mail registered by user to reset their password in case they forgot their pass-image.

Chapter 7 Conclusion

As a conclusion, this project development is developed a mobile application with proposed graphical authentication system to prevent shoulder-surfing attack and to evaluate user's memorability for password. This proposed system is recognition-based authentication system which will need user to remember which image they choose as their password. Other than shoulder-surfing attack, this proposed system is also resist to other attacks such as direct observation, dictionary attack and brute force attack. The proposed method is design with a rules that user need to indirectly click the other image as password instead of the image they choose during registration. So this system is strong resist against shoulder-surfing attack.

This proposed authentication system also can prove to other people that graphical password authentication system is not only clicking the pass-image to proceed, it can be included with some specific rules or algorithm to resist other attacks. It also can protect the info inside user's account with this proposed authentication system. This system also be designed as easier for user to learn and memorize their password.

BIBLIOGRAPHY

Aravindh, B., Ambeth Kumar, V.D., Harish, G., and Siddarth, V.(2017) "A novel graphical authentication system for secure banking systems", 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp. 177-183.

Bahrack, H.P. (1984) "semantic memory content in permastore: Fifty years of memory for Spanish learned in school". *Journal of Verbal Learning and Verbal Behavior* 14, pp. 1-24.

Chee Yeung, A. L. *et al.* (2015) 'Graphical password: Shoulder-surfing resistant using falsification', in *2015 9th Malaysian Software Engineering Conference (MySEC). 2015 9th Malaysian Software Engineering Conference (MySEC)*, Kuala Lumpur, Malaysia: IEEE, pp. 145–148. doi: 10.1109/MySEC.2015.7475211.

Gao, H.C., Liu, X.Y., Wang, S.D., Liu, H.G. and Dai, R.Y. (2009) "Design and Analysis of a Graphical Password Scheme", 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC), pp. 675-678.

Jermyn, I., Mayer, A., Monroe, F., Reiter, M.L., Rubin, A.D. (1999), "The Design and Analysis of Graphical Passwords." Available from: https://www.unisex.org/legacy/events/sec99/full_papers/jermyn/jermyn.html/ (Accessed 8 August 2018)

Por, L. Y. *et al.* (2017) 'Graphical password: prevent shoulder-surfing attack using digraph substitution rules', *Frontiers of Computer Science*, 11(6), pp. 1098–1108. doi: 10.1007/s11704-016-5472-z.

Purushothaman, G.R. and Ashwini, K. (2016) “A Novel Two Step Random Colored Grid Process: Graphical Password Authentication System”, *International Journal of Computer Networks and Communications Security*, pp. 52-55.

Towhidi, F., Masrom, M. and Manaf, A. A. (2013) ‘An Enhancement on Passface Graphical Password Authentication’, p. 7.

Wright, N., Patrick, A.S. and Biddle, R. (2012) Do You See Your Password? Applying Recognition to Textual Passwords [online]. Available from: https://cups.cs.cmu.edu/soups/2012/proceedings/a8_Patrick.pdf (Accessed 8 August 2018)

Appendices

FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

Trimester, Year:	Study week no.:
Student Name & ID:	
Supervisor:	
Project Title:	

<p>1. WORK DONE [Please write the details of the work done in the last fortnight.]</p>
<p>2. WORK TO BE DONE</p>

3. PROBLEMS ENCOUNTERED
4. SELF EVALUATION OF THE PROGRESS

Supervisor's signature

Student's signature

3. PROBLEMS ENCOUNTERED
4. SELF EVALUATION OF THE PROGRESS

Supervisor's signature

Student's signature

3. PROBLEMS ENCOUNTERED
4. SELF EVALUATION OF THE PROGRESS

Supervisor's signature

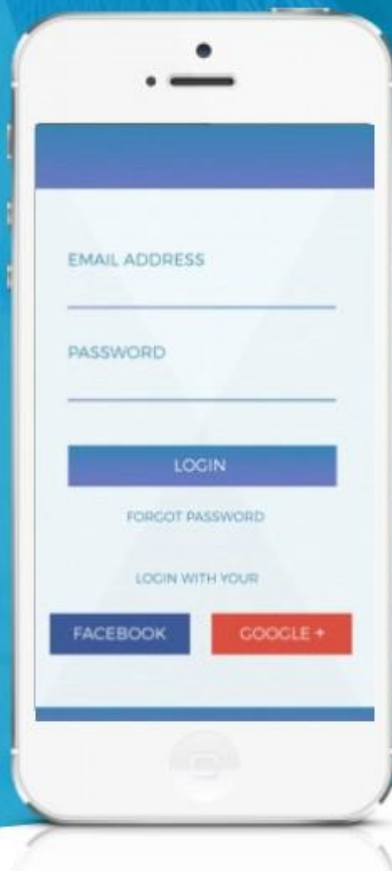
Student's signature

POSTER

Picture-Based Password Scheme

INTRODUCTION

This project introduces a proposed graphical authentication system which using an algorithm of only required user to click the image on the direction of his real paa-image.



OBJECTIVES

- To develop a picture-based authentications scheme to resist shoulder-surfing attacks
- To provide more effective method for user easier to memorize their password while also strengthen the system.

METHODOLOGY

- It is recognition-based graphical authentication system.
- Developed in mobile application with using local database to store user data.

CONCLUSION

- The proposed system is able to resist to shoulder-surfing attack.
- People easier to remember images than textual as passwords.

Plagiarism Check Result

Feedback Studio - Google Chrome
 ev.turnitin.com/app/carta/en_us/?s=&u=1086308340&lang=en_us&o=1104458485&student_user=1

Seow Yang Jiin | Final Year Project 2 Report

Match Overview

11%

1	B. Aravindh, V.D. Ambet... <small>Publication</small>	1%	>
2	ima.ac.uk <small>Internet Source</small>	1%	>
3	Lip Yee Por, Chin Soon ... <small>Publication</small>	1%	>
4	en.wikipedia.org <small>Internet Source</small>	1%	>
5	Submitted to University... <small>Student Paper</small>	1%	>
6	Susan Wiedenbeck, Ji... <small>Publication</small>	1%	>
7	Submitted to Manchest... <small>Student Paper</small>	<1%	>
8	Andrew Lim Chee Yeun... <small>Publication</small>	<1%	>

preferences

Originality Report

Document Viewer

Processed on: 21-Aug-2019 20:11 +08
 ID: 1104458485
 Word Count: 11475
 Submitted: 2

Final Year Project 2 Report

By Seow Yang Jiin

Similarity Index	Similarity by Source
11%	Internet Sources: 4% Publications: 7% Student Papers: 9%

include quoted include bibliography excluding matches < 8 words mode: show matches one at a time Change mode

Chapter 1 Introduction 1.1 Project Inspiration Nowadays, many authentication systems are suffering from many weaknesses. Textual password is very vulnerable to guessing, key loggers, shoulder-surfing, hidden camera and spyware attacks. There are some new techniques has been introduced to overcome the limitations of text-based password such as two-factor authentication and graphical password. Graphical Password is an authentication system that works by letting users to select pictures in a specific orders and it had to present in a graphical user interface (GUI). It also known as graphical user authentication (GUA). Most people are easier to remember graphical password than a text-based password. Graphical password is using several pictures to represent a user's password instead of using text as password. During the login process, user need to select the same pictures in correct orders that has been set during account registration to access into the system. The advantage of graphical password is to prevent hacker from stealing passwords if they had implanted some key loggers such as Trojan in order to capture the text-based passwords. For these authentication system also had some vulnerability too, applications and input devices such as mouse and touch-screen that allow hackers using spyware to record the graphical authentication process, that is why it also

vulnerable to shoulder-surfing attacks too. Generally, graphical passwords

techniques are classified

- 2% match (student papers from 11-May-2011)
[Submitted to University of Malaya](#)
This is source #9 in the cumulative report. This source is partially hidden by one or more sources in the cumulative report.
- 1% match (publications)
[B. Aravindh, V.D. Ambeth Kumar, G. Harish, V. Siddarth, "A novel graphical authentication system for secure banking systems". 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials \(ICSTM\), 2017](#)
This is source #1 in the cumulative report. This source is partially hidden by one or more sources in the cumulative report.
- 1% match (student papers from 05-Jul-2017)
[Submitted to Vel Tech University](#)
This source is completely hidden by one or more sources in the cumulative report.
- 1% match (student papers from 29-Apr-2016)
[Submitted to Laureate Higher Education](#)

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1 of 1



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Seow Yang Jiin
ID Number(s)	16ACB07612
Programme / Course	IB
Title of Final Year Project	Picture-Based Password Scheme

Similarity	Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)
Overall similarity index: <u>11</u> % Similarity by source Internet Sources: <u>4</u> % Publications: <u>7</u> % Student Papers: <u>9</u> %	
Number of individual sources listed of more than 3% similarity: <u>0</u>	
Parameters of originality required and limits approved by UTAR are as Follows: (i) Overall similarity index is 20% and below, and (ii) Matching of individual sources listed must be less than 3% each, and (iii) Matching texts in continuous block must not exceed 8 words <i>Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.</i>	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

Signature of Supervisor

Signature of Co-Supervisor

Name: _____

Name: _____

Date: _____

Date: _____



UNIVERSITI TUNKU ABDUL RAHMAN

**FACULTY OF INFORMATION & COMMUNICATION
TECHNOLOGY (KAMPAR CAMPUS)**

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	16ACB07612
Student Name	Seow Yang Jiin
Supervisor Name	Mr. Ku Chin Soon

TICK (✓)	DOCUMENT ITEMS
	Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
	Front Cover
	Signed Report Status Declaration Form
	Title Page
	Signed form of the Declaration of Originality
	Acknowledgement
	Abstract
	Table of Contents
	List of Figures (if applicable)
	List of Tables (if applicable)
	List of Symbols (if applicable)
	List of Abbreviations (if applicable)
	Chapters / Content
	Bibliography (or References)
	All references in bibliography are cited in the thesis, especially in the chapter of literature review
	Appendices (if applicable)
	Poster
	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)

*Include this form (checklist) in the thesis (Bind together as the last page)

<p>I, the author, have checked and confirmed all the items listed in the table are included in my report.</p> <p>_____</p> <p>(Signature of Student)</p> <p>Date:</p>	<p>Supervisor verification. Report with incorrect format can get 5 mark (1 grade) reduction.</p> <p>_____</p> <p>(Signature of Supervisor)</p> <p>Date:</p>
--	--