SHOULDER SURFING SECURITY THREAT PREVENTION USING SHIFTING DIRECTIONS

TEY BOON HAU

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY UNIVERSITY OF MALAYA KUALA LUMPUR

2018

SHOULDER SURFING SECURITY THREAT PREVENTION USING SHIFTING DIRECTIONS

TEY BOON HAU

DISSERTATION SUBMITTED IN PARTIAL

FULFILMENT OF THE REQUIREMENTS FOR

THE DEGREE OF MASTER OF COMPUTER SCIENCE

FACULTY OF COMPUTER SCIENCE AND

INFORMATION TECHNOLOGY

UNIVERSITY OF MALAYA

KUALA LUMPUR

2018

UNIVERSITY MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **TEY BOON HAU**

Name of Degree: **MASTER OF COMPUTER SCIENCE**

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"): **SHOULDER SURFING SECURITY THREAT PREVENTION USING SHIFTING DIRECTIONS**

Field of Study: **COMPUTER SCIENCE**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:

Subscribed and solemnly declared before,

Witness's Signature Date:

Name:

Designation:

Abstract

In this research work, a graphical method using shifting directions is proposed. The proposed method is based on knowledge-based indirect image selection method to perform authentication. A user needs to use the registered images and shifting direction to identify the pass-images used in each challenge set. A uniform randomization algorithm was used to ensure the images used were randomly allocated within the grid cell for every challenge set. Only users who have the knowledge of both registered images and the registered shifting direction can derive the pass-images. Therefore, it is impossible for the attacker to gain the user registered images although the whole login session was recorded. A user study was carried out to assess the feasibility of the proposed method in resisting shoulder-surfing attack. The results shown that the proposed method was able to preventing video recorded, and direct observation shoulder-surfing attacks.

Keywords: graphical password, shoulder-surfing attack, shifting directions

Abstrak

Dalam kerja penyelidikan ini, satu kaedah grafik yang menggunakan arah peralihan telah dicadangkan. Kaedah yang dicadangkan adalah berdasarkan kaedah pemilihan imej tidak langsung berasaskan pengetahuan untuk melakukan pengesahan. Seseorang pengguna perlu menggunakan imej berdaftar dan arah peralihan untuk mengenal pasti pas-imej untuk log masuk bagi setiap set cabaran. Algoritma rawak seragam digunakan untuk memastikan imej diedarkan secara rawak dalam sel grid untuk setiap set cabaran. Hanya pengguna yang mempunyai pengetahuan mengenai imej berdaftar dan arah peralihan berdaftar sahaja dapat menghasilkan pas-imej. Oleh itu, tidak mustahil bagi penyerang untuk mengetahui imej berdaftar pengguna walaupun keseluruhan sesi log masuk direkodkan. Satu kajian pengguna telah dilaksanakan untuk menilai kemungkinan kaedah yang dicadangkan untuk mencegah serangan pelayaran bahu. Hasil kajian menunjukkan bahawa kaedah yang dicadangkan dapat menghalang kedua-dua keadaan sama ada melalui rakaman video, atau pemerhatian langsung.

Kata kunci: kaedah grafik, pelayaran bahu, arah peralihan

Acknowledgement

First of all, I would like to thank my parents and family members for their support and encouragement. Then, I would like to express my sincere gratitude to my supervisor, Dr. Por Lip Yee. Without his guidance, advices and encouragement, I could not have been completed this research. Special thanks go to my colleagues who took part in the user study. Thank you for the time and suggestions given for improving the proposed method. Last but not least, I would like to thank all the participants who took part in the study.

Table of Contents

List of Figure

List of Table

List of Abbreviation

DAS	:	Draw-A-Secret
FOA	:	Frequency of Occurrence Analysis
IRR	:	Information Retention Rate
NIST	:	National Institute of Standards and Technology
PDS	:	Password Diversity Score
TAC	:	Transaction Authorization Code
WYSWYE	:	Where You See is What You Enter

List of Appendices

Chapter 1 Introduction

1.1 Background

Password authentication is essential to protect resources from unwanted intruders. Systems such as automated teller machines, online social media, cell phones, and computers need password before they can be accessed. There are many types of password. Text based password is one of the commonly used authentication methods for most of the systems (Gokhale & Waghmare, 2014). Text based password uses the combination of alphabets, numbers and special characters to form a password. Guidelines were created and revised by National Institute of Standards and Technology (NIST) from time to time to ensure users are aware and practice strong password (Grassi et al., 2018). Strong passwords are difficult to remember (Tank et al., 2015). Users tend to forget their password when they used strong password. Therefore, graphical password was proposed to help users to remember their passwords (Golar & Adane, 2016).

1.2 Problem Statement

Even though graphical password is able to improve users to remember their password, but most of the current graphical passwords are still wild exposed to shoulder-surfing attack (Simha, 2017). Shoulder-surfing attack is a security threat, which an attacker can steal the password of a legitimate user via direct observing or video recording method during an authentication process (Khedr, 2018). There are several graphical password systems were proposed to prevent shoulder-surfing attack. For example, in Convex Hull Click System (Wiedenbeck et al., 2006), the authors used non-register icons to confuse attackers from identifying the correct pass-icon used in every challenge set. During enrolment procedure, a user needs to register three icons. During authentication procedure, the user has to click any icon inside the convex hull area that formed by the

registered icons. According to the authors, their method could resist shoulder-surfing attack.

In "Where You See is What You Enter" (WYSWYE) System (Khot et al., 2012), the author used partial password method to prevent shoulder-surfing attack. During enrolment procedure, a user needs to register several images. During authentication procedure, some of the registered images are randomly selected. The user needs to click the registered images in sequence to login. In each challenge set, the selection of the registered images are varies. Therefore, the authors believed such method could resist shoulder-surfing attack.

(Por et al., 2017) proposed a method that uses diagraph substitution method to prevent shoulder-surfing attack. In this method, a user needs to understand and remember the three digraph substitution rules that set by the authors. During authentication procedure, the user needs to identify the pass-images based on the registered images and the three digraph substitution rules. The pass-images are random and they can be the registered images or decoy images or the mixture of both. Therefore, the authors believed such method could confuse the shoulder-surfing attackers.

Convex Hull Click System, WYSWYE System, and Por System are able to prevent direct observation shoulder-surfing attack but these systems are vulnerable to video recorded shoulder-surfing attack because attackers are able to reveal the password by observing multiple video recorded login session. For example, in Convex Hull Click System, users will never click on the registered icons to login. Therefore, attackers can use multiple video recorded login session to filter out the icons that is not selected by the users. In WYSWYE System, users must select the registered images in sequence

before they can login. Attackers can use multiple video recorded login session to determine the sequence of the images based on user's selection. Moreover, the attackers can filter out those non-selected images, as they can never be the registered images. In Por System, the registered images are always located within the same row or column of the pass-images. Therefore, attackers can use multiple video recorded login session to analyze and make an intelligent guess to gain access into the system. After analyzing the weaknesses of the existing systems, it shows that there are rooms of improvement especially in proposing a graphical password method to prevent shoulder-surfing attack. As such, this dissertation was conducted with the objective to address both video recorded and direct observation shoulder-surfing security threats.

1.3 Objective

The following are the objectives of this research work:-

1. To propose a graphical password method that is able to prevent video recorded and direct observation shoulder-surfing attacks.
2. To design and implement the proposed method.
3. To test and evaluate the feasibility of the proposed method in resisting video recorded and direct observation shoulder-surfing attacks using user study.

1.4 Scope of Research

Due to the time constraint, this research work only focus on recognition based graphical password. Other graphical passwords, biometric based password, token based password, text based password are not within the scope of this research work. Moreover, this research work only focus on proposing a method to prevent video recorded and direct

observation shoulder-surfing attacks. Other security threats such as brute force, dictionary, and phishing attacks are not included in this study.

1.5 Significant of Research

A method that uses shifting direction was proposed to prevent video recorded and direct observation shoulder-surfing attacks. This method was proposed to trick attackers from identifying the correct pass-image used. Only users who have the knowledge of both registered images and registered shifting direction can derive the pass-image. The pass-images can be decoy images or registered images. As such, it is impossible for the attackers to obtain the pass-images even though the whole login session was recorded.

A value added feature was added in the proposed method to prevent Frequency of Occurrence Analysis (FOA) attack. During authentication process, the grid cell is filled up with the registered and decoy images using uniform randomization algorithm. The leftover images are bound with the user's identification permanent and those images will not appear in the subsequence authentication challenge sets. As a result, this feature enables the proposed method to use the same images in every challenge set and it is able to prevent FOA attack.

1.6 Dissertation Organization

This dissertation consists of six chapters. In this chapter, the dissertation background, problem statement, research objective, project scope, significant of research and the organization of the dissertation were discussed.

Chapter two begins with the discussion of the type of authentication systems followed by shoulder-surfing security threat. Several recognition based authentication systems

were discussed in term of their method used, strength and weakness before the chapter summary is presented.

Chapter three discusses the methodology used to achieve the goal for the dissertation. The details of data gathering and analysis, system design, testing and evaluation are discussed in this chapter before it ended with a chapter summary.

Chapter four describes the design and implementation of the proposed system. The beginning of this chapter is discussion of the proposed user authentication system. After that, the details of the proposed method are deliberated. The system file is discussed in this chapter before it ended with a chapter summary.

Chapter five discusses the system testing and evaluation of the proposed method. The procedure used, result obtained, and analyses that have been carried out in this user study are discussed in detail. The comparison of the related work is presented before the chapter summary is deliberated.

Chapter six discusses the objective accomplished in this study. The contribution of this dissertation is highlighted and the future work is presented at the end of chapter.

Chapter 2 Literature Review

2.1 Introduction

The first part of this chapter is the discussion of the type of authentication systems followed by shoulder-surfing attack. Several recognition based authentication systems were discussed in term of their method used, strength and weakness before the chapter summary is presented.

2.2 Type of Authentication System

There are three types of authentication methods – biometric based, token based, and knowledge based authentications (Zviran & Erlich, 2006). Token based authentication uses physical or software based password that a user possesses such as bank cards and Transaction Authorization Code (TAC) to perform authentication. Biometric based authentication uses unique biological characteristic such as fingerprint, facial recognition, and iris scan of an individual to perform authentication. Knowledge based authentication uses what a user knows for example text password and graphical password to perform authentication. This study only focuses on graphical password. Therefore, other authentication methods are not discussed further in this chapter.

Graphical password uses images as password to perform authentication. According to the literature, graphic can improve human in remembering and recalling their password better (Golar & Adane, 2016). There are three types of graphical password – recognition based, recall based and cued recall based (Bhanushali et al., 2015). In recognition based graphical password, users authenticate to the system by recognizing and identifying the registered images. Passface™ is an example of the system that uses such authentication method. For recall based graphical password, a user is required to reproduce the registered password during the enrolment procedure without any hint/clue given. Draw-

A-Secret (DAS) is an example of the system that uses such authentication method. In cued recall based graphical password, user is given clues to help them to reproduce the registered password. Cued Click Point is an example of the system that uses such authentication method.

2.3 Shoulder-surfing Security Threat

There are many security threats for example guessing attack, social engineering attack, brute force attack, dictionary attack and shoulder-surfing attack encountered by graphical password. Due to the time constraint, this research work only focus on shoulder-surfing security threat. Other security threats are not discussed further in this chapter.

Shoulder-surfing attack is an act of observing victim's information over a victim's shoulder (Lashkari et al., 2009). An attacker can then use the observed information to login to a secure system as a legitimate user. The common ways to perform the shoulder-surfing attack are via direct observation, video recording and sound recording (Eiband et al., 2017). These attacks normally are carried out in a public crowded area.

2.4 Related Work

Due to the time constraint, this research work only focus on recognition based graphical password. Thus, other authentication methods are not discussed further in this chapter. The following is the review regarding the selected recognition based graphical passwords.

2.4.1 Déjà Vu

Dhamija and Perrig (2000) developed this system using "random art" images (see Figure 2.1). These images are generated using Andrej Bauer's Random Art. During enrolment procedure, a user needs to register five images. During authentication procedure, twenty-five images are given and the user needs to select the registered images to login. According to the authors, using "random art" images can make users harder to describe, share and write down their password (Dhamija and Perrig, 2000). However, this system is vulnerable to direct observation shoulder-surfing attack. Attackers can shoulder-surf which images selected by a user and used the similar images to login.

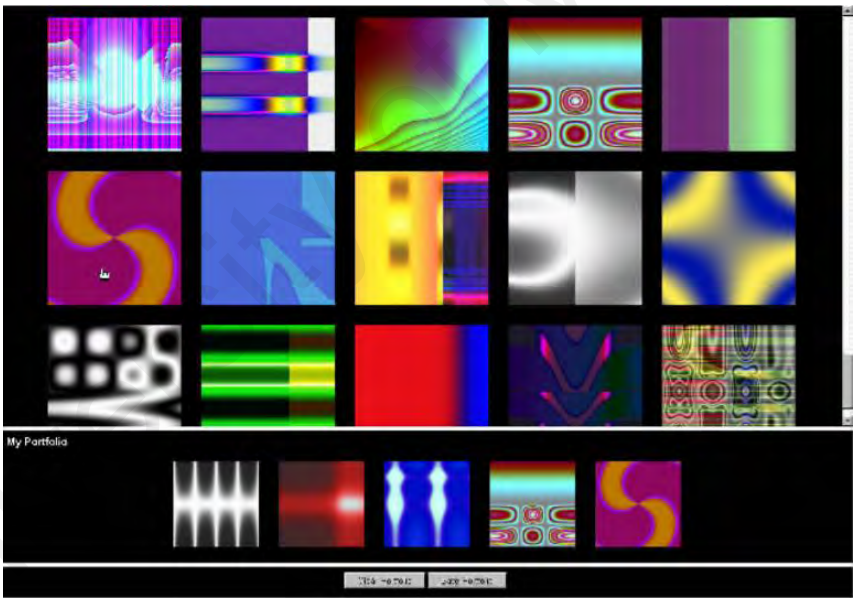

Figure 2.1 Déjà Vu (Dhamija and Perrig, 2000)

2.4.2 Passfaces™

Passfaces™ was proposed by Davis et al. (2004). This system uses human faces as images (see Figure 2.2). During enrolment procedure, a user needs to register four images. During authentication procedure, users need to identify the registered images for four rounds before they can login. According to the authors, Passface ™ can help users to remember their password better compared to text password. However, Passface ™ is vulnerable to shoulder-surfing attack because attackers can shoulder-surf which images selected by a user and used the similar images to login.

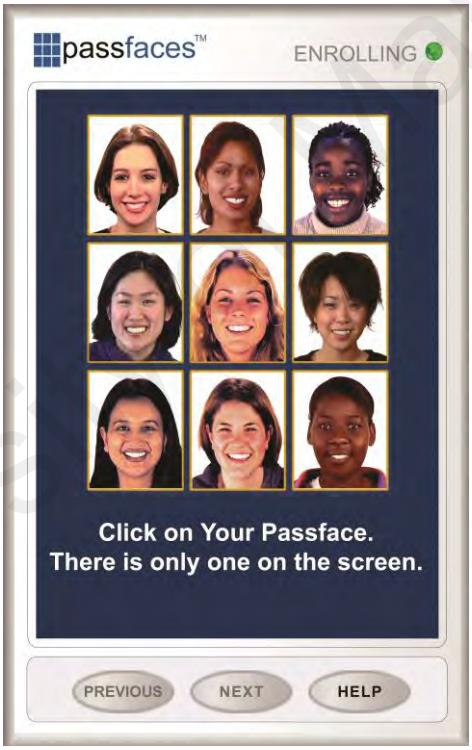

Figure 2.2 Passfaces™ (Davis et al., 2004)

2.4.3 Convex Hull Click

Convex Hull Click was proposed by Wiedenbeck et al. (2006). During enrolment procedure, a user needs to register three icons. During authentication procedure, the user needs to visualize an area (convex hull) that formed by the three registered icons. The user has to select any one of the icons inside the convex hull area to login (see Figure 2.3). The authors believed this method can prevent direct observation shoulder-surfing attack because the pass-icon used to login is a decoy icon and the user can choose the same decoy icon or other decoy icons to login as long as these decoy icons are within the convex hull. Since the pass-icon used can never be the registered icons, thus, an attacker can filter out the clicked/used pass-icons by using multiple video recorded shoulder-surfing sessions. Therefore, this method is exposed to video recorded shoulder-surfing attack whereby the registered icons will be known after attackers performing multiple video recorded shoulder-surfing sessions.

Figure 2.3 Convex Hull Click (Wiedenbeck et al., 2006)

2.4.4 WYSWYE

"Where You See is What You Enter" was proposed by Khot et al. (2012). During enrolment procedure, a user needs to register N images. During authentication procedure, the user needs to eliminate the row/column, which does not have the registered images (Figure 2.4). To login, the user has to do the same elimination process until no more rows or columns can be eliminated. The authors believed this method can prevent direct observation shoulder-surfing attack because the user is not revealing any information about the registered images. However, this method actually reveals the registered images in the final form of the elimination processes. The attackers can filter out the images by using multiple video recorded shoulder-surfing sessions. To obtain the registered images information, the attackers can compare the eliminated images with the final form of the left over images. Therefore, this method is exposed to video recorded shoulder-surfing attack.

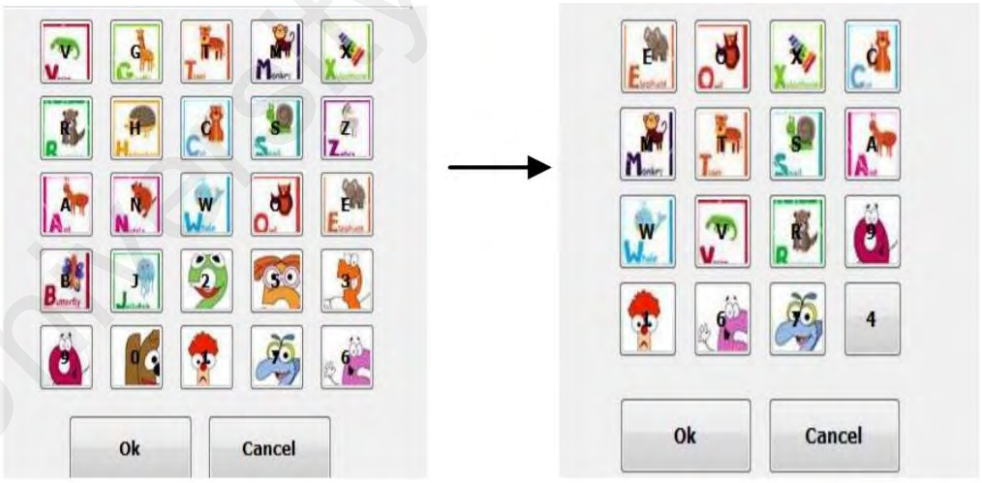

Figure 2.4 WYSWYE (Khot et al., 2012)

2.4.5 Sonal

Sonal et al. (2015) had proposed a graphical authentication system in 2015. During enrolment procedure, a user needs to register several characters and a color. During authentication, the user needs to rotate the color sector to the places that have the registered characters (see Figure 2.5). The authors believed this method can prevent direct observation shoulder-surfing attack because the user is not revealing any information about the registered characters and color. However, an attacker can filter out the color sector and the characters that each of the color contains when the user stop rotating. Therefore, by using multiple video recorded shoulder-surfing sessions, the attacker might be able to know the registered color as well as the registered characters. Hence, this method is vulnerable to video recorded shoulder-surfing attack.

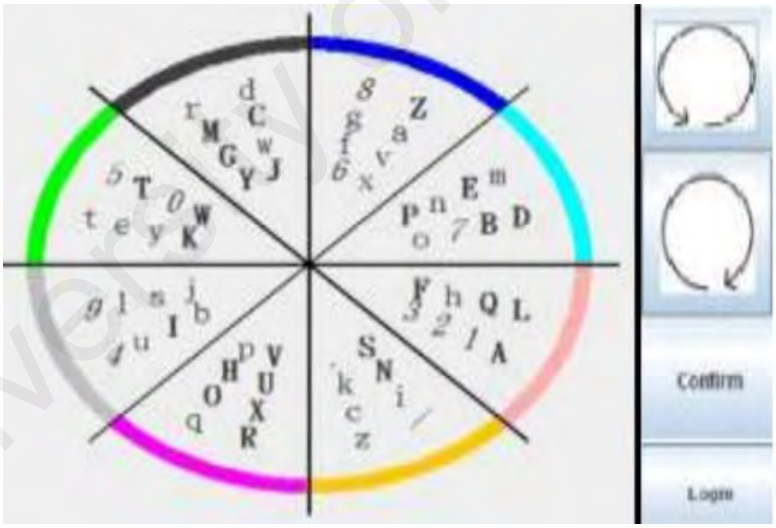

Figure 2.5 Sonal (Sonal et al., 2015)

2.4.6 Kolay

Kolay et al. (2017) had proposed a graphical authentication system using image segmentation method. During enrolment procedure, a user needs to register an image. The registered image is segmented into grid. During authentication procedure, the segmented images in a jumbled order are given (see Figure 2.6). The user needs to click the correct segmented images and reproduce the registered image. The authors believed this system is easy for the users to remember and recall their registered image. However, this method is vulnerable to shoulder-surfing attack because attackers can observe the segmented images selected by a user and used the similar segmented images to login.

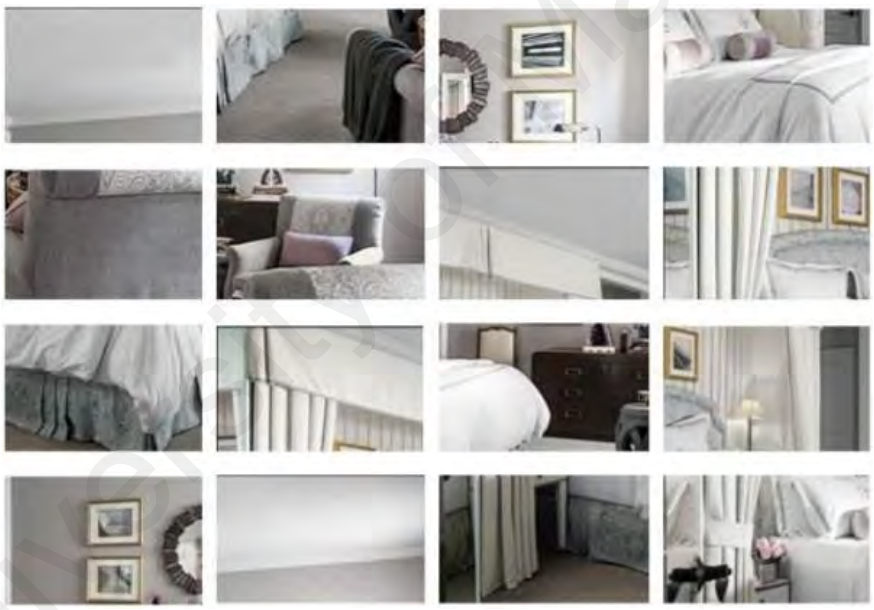

Figure 2.6 Kolay (Kolay et al., 2017)

2.4.7 Por

Por et al. (2017) had proposed a graphical authentication system that uses digraph substitution rule. During enrolment procedure, a user has to register a username and two images. During authentication procedure, the user is required to identify the pass-images based on the registered images and the three digraph substitution rules (see Figure 2.7). The authors believed this method can resist direct observation shoulder-surfing attack because the pass-images are random and they can be the registered images or the decoy images or the mixture of both. An attacker requires the knowledge of the digraph substitution rules and the registered images information to derive the pass-images. However, there is a drawback of the proposed digraph substitution rules because the pass-images produced will always fall together with the registered images either within the same row/column. Therefore, the registered images can still be revealed by using multiple video recorded login sessions. Hence, this method is vulnerable to video recorded shoulder-surfing attack.

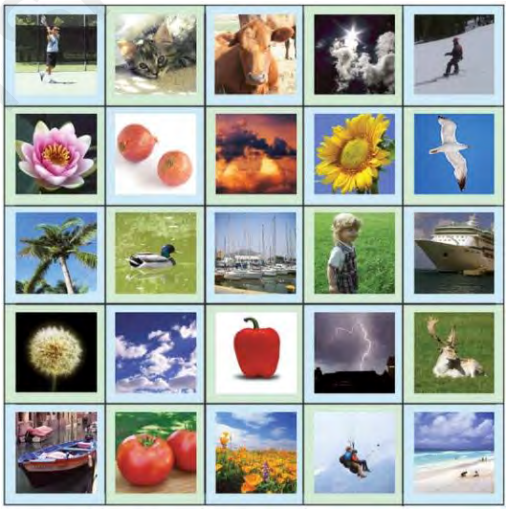

Figure 2.7 Por (Por et al., 2017)

2.4.8 Dhandha

Dhandha & Parekh (2017) proposed a graphical password system in 2017. During enrolment procedure, a user needs to register the username and several images. During authentication procedure, the user is required to identify the registered images and the string associated with the registered images. To login, the user has to enter the strings with the correct sequence based on the registered images (see Figure 2.8). According to the authors, this method can prevent direct observation shoulder-surfing attack because only part of the registered images will be selected for authentication purposes. Moreover, the string associated with the registered images will be varies every time the login page is refreshed. Even so, this system is exposed to video recorded shoulder-surfing attack. An attacker can filter out the decoy images, which are not selected by the user. After that, the attacker can map the string entered by the user with the images given. With multiple video recorded shoulder-surfing sessions, the registered images can be revealed.

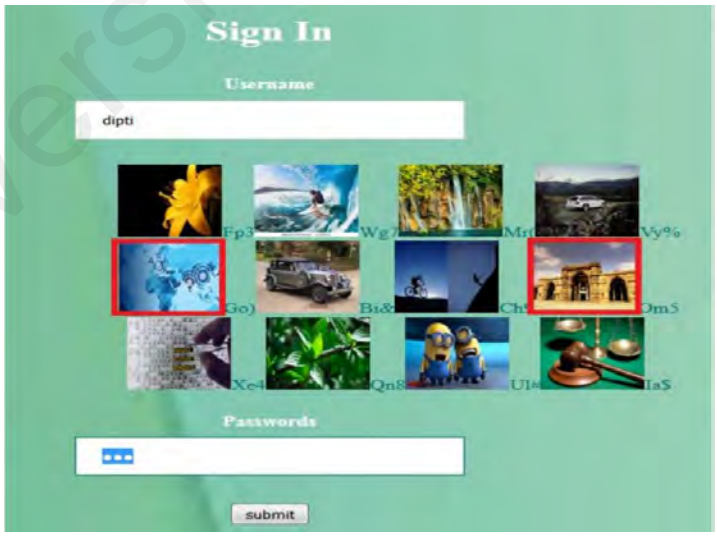

Figure 2.8 Dhandha (Dhandha & Parekh, 2017)

2.4.9 EvoPass

EvoPass was proposed by Yu et al. (2017). During enrolment procedure, a user needs to register four images. During authentication procedure, the registered images and decoy images in sketches form are given (see Figure 2.9). To login, the user needs to click the correct sketches that represent the registered images. According to the authors, EvoPass can prevent direct observation shoulder-surfing attack because this method implements Password Diversity Score (PDS) and Information Retention Rate (IRR) in the process of generating sketches images. EvoPass images will gradually degrading. Thus, this method can prevent direct observation attack even though part of the sketches may have been exposed. However, an attacker can reveal the registered images using video recorded shoulder-surfing sessions. Attacker can analyze the characteristic of the clicked sketches images and used the similar images to gain the access. Hence, this method is vulnerable to video recorded shoulder-surfing attack.

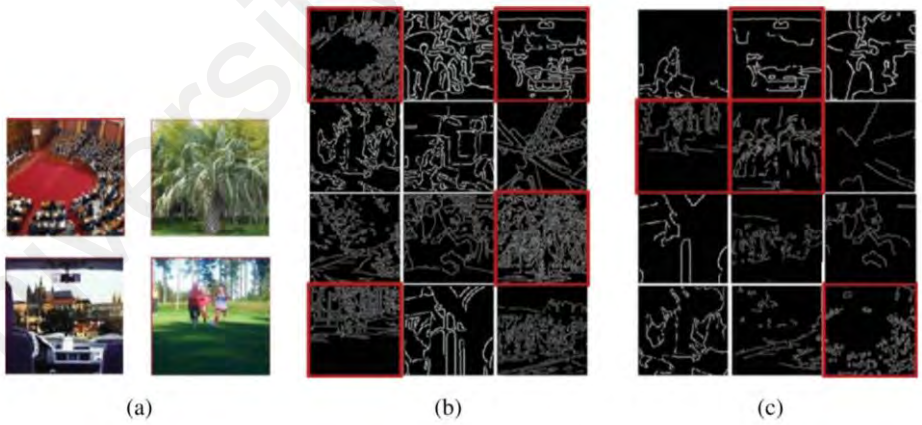

Figure 2.9 Evopass (Yu et al., 2017) – (a) Registered Images (b) Sketches Images Generated (c) Evolving Version of Sketches Images. The Red Borders Highlighted the Registered Images In Sketches Form

Table 2.1 Recognition Based Authentication Method

Method	Year	Strength	Weakness	Evaluation Method	Methodology
Déjà Vu	2000	▪ Able to prevent user from selecting predictable images. ▪ Able to prevent user from writing down and share the password.	▪ Vulnerable to direct observation shoulder-surfing attack. ▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	User study
Passfaces™	2004	▪ Easy to remember.	▪ Vulnerable to direct observation shoulder-surfing attack. ▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	N/A
Convex Hull Click	2006	▪ Able to prevent direct observation shoulder-surfing attack.	▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	Simulation study
WYSWYE	2012	▪ Able to prevent direct observation shoulder-surfing attack.	▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	N/A
Sonal	2015	▪ Able to prevent direct observation shoulder-surfing attack.	▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	N/A
Kolay	2017	▪ Easy to remember.	▪ Vulnerable to direct observation shoulder-surfing attack. ▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	N/A
Por	2017	▪ Able to prevent direct observation shoulder-surfing attack.	▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	User study
Dhandha	2017	▪ Able to prevent direct observation shoulder-surfing attack.	▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	N/A
EvoPass	2017	▪ Able to prevent direct observation shoulder-surfing attack.	▪ Vulnerable to video recorded shoulder-surfing attack.	Case study	User study

A summarize of the selected recognition based graphical passwords is presents in Table 2.1. According the table, Convex Hull Click, WYSWYE, Sonal, Por, Dhandha, and EvoPass are able to prevent direct observation shoulder-surfing attack but these systems are vulnerable to video recorded shoulder-surfing attack because attackers can reveal the password by observing multiple video recorded shoulder-surfing sessions. Other systems such as Déjà Vu, Passfaces™, and Kolay are vulnerable to both video recorded and direct observation shoulder-surfing attacks. Déjà Vu, Por, and EvoPass used user study as the methodology. Convex Hull Click used simulation study as the methodology. Methodology used by other systems such as Passfaces™, WYSWYE, Sonal, Kolay and Dhandha are not mention in their publications. From the summary, it shows that there are rooms of improvement especially in proposing methods to resist shoulder-surfing attack. As such, this study was carried out with the objective to address both video recorded and direct observation shoulder-surfing attacks.

2.5 Summary

The type of the authentication systems and shoulder-surfing security threat have been discussed in this chapter. Several recognition based graphical passwords have been present in term of their method, strength, and weakness. The analysis of the related work shows that most of the recognition based graphical passwords are vulnerable to shoulder-surfing attack. Some of the graphical passwords can prevent direct observation shoulder-surfing attack, but those systems are vulnerable to video recorded shoulder-surfing attack. After analyzing the weaknesses of the existing systems, it shows that there are rooms of improvement especially in proposing a graphical method to prevent shoulder-surfing attack. As such, this dissertation was conducted to address both video recorded and direct observation shoulder-surfing security threat in graphical password. Next, the methodology used for this research will be discussed.

Chapter 3 Research Methodology

3.1 Introduction

This chapter describes the methodology applied to achieve the goal for the dissertation. The details of data gathering and analysis, system design, testing and evaluation are discussed in this chapter before it ended with a chapter summary.

3.2 Research Methodology

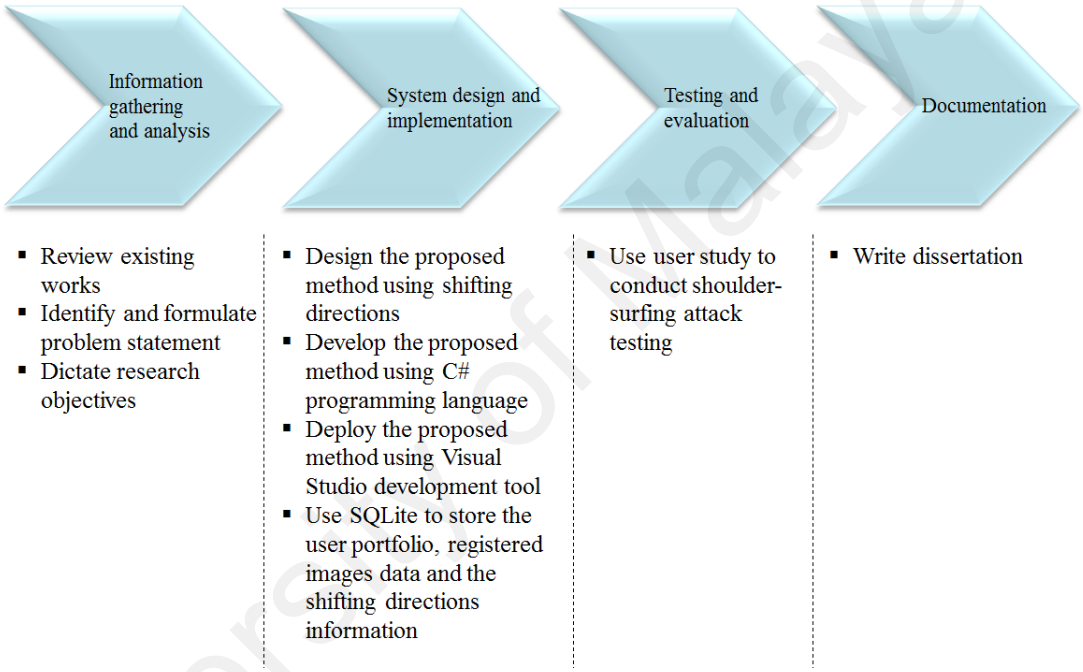

Figure 3.1 Research Methodology

Figure 3.1 presents the methodology used in this study. The proposed methodology contains four phases – information gathering and analysis, system design and implementation, testing and evaluation, and documentation. The details of each phase will be explained in the following sub-sections.

3.2.1 Information Gathering and Analysis

Several existing recognition based graphical passwords were selected and analyzed in terms of their features, strengths and weaknesses. The information regarding the selected recognition based graphical passwords was gathered from articles such as journal, conference and white paper. Problem such as recognition based graphical passwords are still exposed to shoulder-surfing attack was identified although there are methods have been proposed to prevent shoulder-surfing attack. To fill in the research gap, this research was carryout to address the video recorded shoulder-surfing attack and direct observation shoulder-surfing attack.

3.2.2 System Design and Implementation

Three objectives have been formulated. To accomplish the first objective, a method that uses shifting directions is proposed to prevent video recorded and direct observation shoulder-surfing attacks. To test on the proposed method, a proposed system was developed. The proposed method is based on knowledge-based indirect image selection method to perform authentication. A user needs to use the registered images together with the shifting directions to identify the pass-image used in each challenge set. The pass-image can be the registered image or a decoy image. A uniform randomization algorithm is used to ensure that the images were randomly assigned to the grid cells every time a user wants to login. To obtain the correct pass-image, an attacker must have the knowledge of both registered images and the shifting directions. Therefore, an attacker is not possible to know the correct pass-image to use in each challenge set even the login process was shoulder-surfed or recorded.

To achieve the second objective, the proposed method is transformed into a workable prototype. To test the feasibility of the proposed method in resisting both direct

observation and video recorded shoulder-surfing attacks, a proposed authentication system was developed. The proposed authentication system was deployed using Visual Studio and the proposed method was developed using C# programming language. SQLite was used as the database to store the user portfolio, registered images data and the shifting directions information.

3.2.3 Testing and Evaluation

In order to accomplish the third objective of this research, the proposed system was tested and evaluated using a user study. The user study was conducted to assess the feasibility of the proposed system in resisting the shoulder-surfing attack. Due to budget and geographical constraints, the user study was conducted at a company named Public Bank Berhad that located at Bangi, Selangor, Malaysia. This company is an international company and it has approximately 500 employees. 102 participants were invited to perform the evaluation. The confidence interval (margin of error) of this user study is approximately 8.62% based on the 95% confidence level, sample size of 102, population size of 500, and 50% of population proportion. Confidence level indicates the percentage of the target population will provide answer within the confidence interval. If the confidence level is 95%, it express that 95% of the certainly the target population will select the answer within the confidence interval. The most common used of confidence level by the researcher is 95%. To baseline with the other graphical passwords, this research also selects 95% as the confidence level.

There were four phases in the evaluation process. In phase 1, a pre-survey was conducted to explore the exposure and knowledge of the participants regarding graphical password and shoulder-surfing attack. Six questions were asked and the questions were stated in Table 3.1. The first three questions are used to gather the

personal information of the participant. Question four is used to understand the participant's knowledge about a graphical-based password. Question five and six are used to measure the participant's experience towards graphical-based password and to determine participant's knowledge about shoulder-surfing attack respectively.

Table 3.1 Pre-survey Question

No.	Question
1	Name
2	Gender
3	Age
4	Do you know what graphical password is?
5	Have you login using graphical password before?
6	Do you ever heard about shoulder-surfing attack?

In phase 2, a demonstration of the proposed authentication system was presented to the participants. Participants were guided to undergo the registration and authentication phases so that they can familiar themselves with the proposed system. The participants then were requested to create their own graphical password and used the registered password to log in. Ten successful login times were recorded by the system. The purpose of recording the login time is to study the average time take by the users so that in future the proposed method can be further improved to achieve better usability aspect.

In phase 3, a successful login video was presented to the participants. The participants were given unlimited trials to log in.

In the last phase, a post-survey was conducted to gather the participants' feedback after they have conducted shoulder-surfing attack. Four questions were asked and the questions are shown in Table 3.2.

Table 3.2 Post-survey Question

No.	Question
1	Were you successful login via shoulder-surfing attack?
2	What strategy attempted to perform shoulder-surfing attack?
3	Do you agree that the proposed method is able to resist shoulder-surfing attack?
4	What would you suggest to improve this proposed graphical password authentication method?

Question one and three are closed-ended questions and the others are open-ended questions. Question one was used to determine whether the proposed authentication system is vulnerable to shoulder-surfing security threat. Question two was used to explore the strategy/method used by the participants when they performed shoulder-surfing attack. Question three was used to gather information of whether the participants agreed that the proposed method was feasible to prevent shoulder-surfing attack. The last question was used to gather the suggestion/idea from the participants to further improve the proposed method if there is any.

3.2.4 Documentation

In this stage, the procedure used to conduct the research; the detailed of the proposed method and the results obtained from the survey were documented. The future

enhancement and research summary were also discussed and documented in this dissertation.

3.3 Summary

This chapter presented the research methodology applied to achieve the dissertation objectives. The methodology used to identify the research problem was explained. The instruments used for gathering and analyzing the data were discussed in details. To achieve the research objectives, a method that used shifting algorithm was proposed to prevent shoulder-surfing attack. Visual Studio and C# programming language were used to deploy and develop the proposed method respectively. A user study was carried out to test the feasibility of the proposed method in resisting both video recording and direct observation shoulder-surfing attack. The proposed method required users to use a pass-image that derived from the registered images and the shifting direction to log in. Therefore attackers that without both information are unable to login. Next chapter discusses the system design and implementation of the proposed method.

Chapter 4 System Design and Implementation

4.1 Introduction

This chapter discusses the design and implementation of the proposed system. It starts with the discussion of the proposed user authentication system. After that, the details of the proposed method are deliberated. The system file is discussed before the chapter summary is presented.

4.2 Proposed User Authentication System

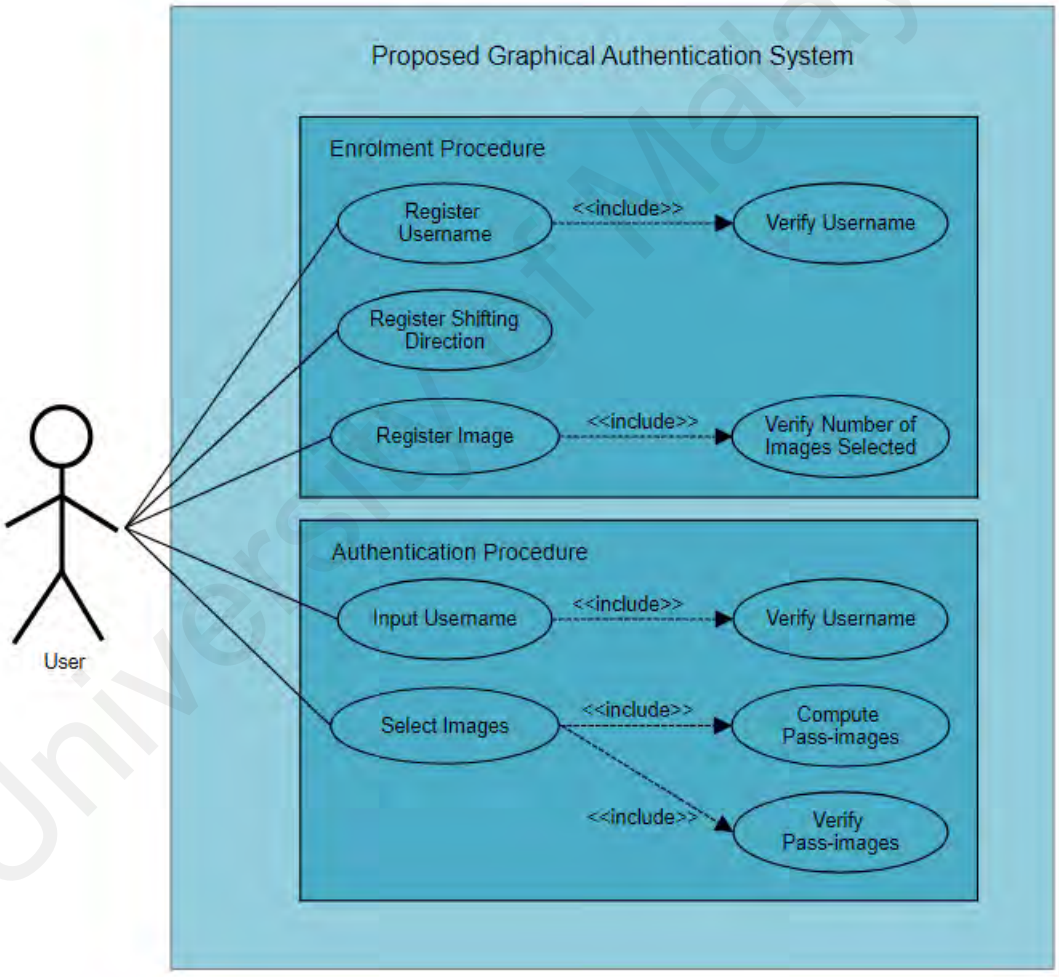

Figure 4.1 Use Case Diagram

A use case diagram of the proposed authentication system is shown in Figure 4.1. To test on the proposed method, the proposed authentication system was developed. The

proposed authentication system consists of two main procedures: enrolment and authentication procedures.

4.2.1 Enrolment Procedure

The enrolment procedure involves three processes: –

- Username registration
- Shifting direction registration
- Image registration

4.2.1.1 Username Registration

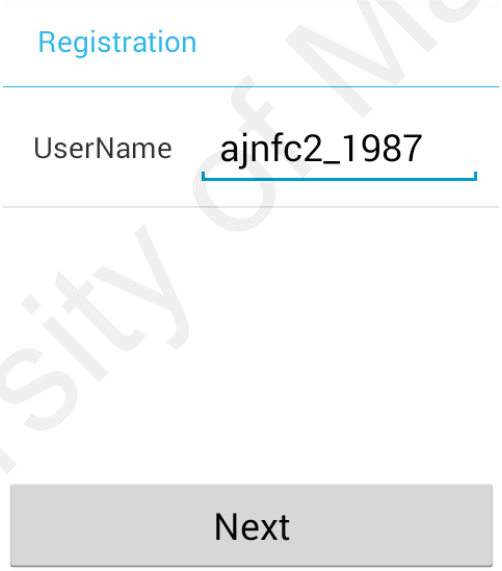

Figure 4.2 Username Registration Interface

Figure 4.2 shows the username registration interface. Users are required to register a unique username. A warning dialogue window will display if the user has input an invalid data (see Figure 4.3). The system will save the username into a temporary variable once the user clicks on the "Next" button. The pseudo-code of the username registration process is shown in Figure 4.4.

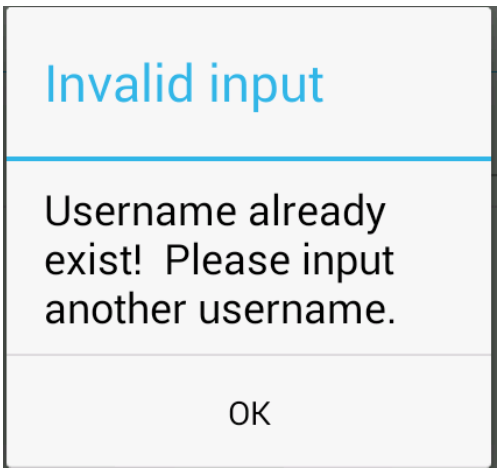

Figure 4.3 Username Verification Interface

```
Registration

SET login ID = user input username string

CHECK database

        IF login ID found THEN
                LAUNCH warning username been used
        ELSE IF null entry
                LAUNCH warning null entry
        ELSE
                LAUNCH shifting registration page
```

Figure 4.4 Pseudo-code of the Username Registration Process

4.2.1.2 Shifting Direction Registration

Thereafter completing the username registration process, the user is directed to a new window where he/she has to register a shifting direction. The user has to select one of the shifting directions given – vertical shift and horizontal shift (see Figure 4.5).

Vertical Shifting Horizontal Shifting

Figure 4.5 Shifting Direction Interface

There are five positions given (0 until 4) in each direction shifting. The "0" position is a default setting selected for user. To benchmark with (Por et al., 2016), the same grid size is used (5 x 5). This is also the reason why the proposed system only allowed the user to shift five positions. The proposed system will save the chosen options into a temporary variable once the user clicks on the "Next" button. The pseudo-code of the shifting direction registration process is shown in Figure 4.6.

```
Shifting Movement Registration

SET shift vertical = user SELECT number of vertical movement

BUTTON 0
        NULL no shifting
BUTTON Down1 OR UP4
        SHIFT to down direction for 1 unit
BUTTON Down2 OR UP3
        SHIFT to down direction for 2 unit
BUTTON Down3 OR UP2
        SHIFT to down direction for 3 unit
BUTTON Down4 OR UP1
        SHIFT to down direction for 4 unit
BUTTON Next
        LAUNCH to horizontal shift selection interface

SET shift horizontal = user SELECT number of horizontal movement

BUTTON 0
        NULL no shifting
BUTTON Right1 OR Left4
        SHIFT to right direction for 1 unit
BUTTON Right2 OR Left3
        SHIFT to right direction for 2 unit
BUTTON Right3 OR Left2
        SHIFT to right direction for 3 unit
BUTTON Right4 OR Left1
        SHIFT to right direction for 4 unit
BUTTON Next
        LAUNCH to graphical password selection interface
```

Figure 4.6 Pseudo-code of the Shifting Direction Registration Process

4.2.1.3 Image Registration

After completing the shifting direction registration process, the user is directed to another new window where he/she needs to select at least 8 images (repeated image is counted as another image). There are 26 images given (A to Z) (see Figure 4.7). The user can only select a maximum up to 25 unique images. A dialogue window will prompt out if the user has selected less than 8 images or more than 25 unique images (see Figure 4.8). The reason of allowing the user to select only 25 unique images is because the proposed system only has 5 x 5 grid cells (the same grid to benchmark with (Por et al., 2016)). The sequence of the selected images is important. The user has to

remember the sequence. The proposed system has an indicator to keep track of the number of images that clicked by the user. The user can use the “reset” button to reset his clicks. The user is required to click on the “Next” button if he/she satisfies with the selected images. A confirmation dialogue window will display after that (see Figure 4.9). Once the user has clicked the “Yes” button, the username, shifting direction and the selected images information will be stored in a database. The user can redo the image selection process again by clicking the “No” button. The pseudo-code of the image registration process is shown in Figure 4.10.

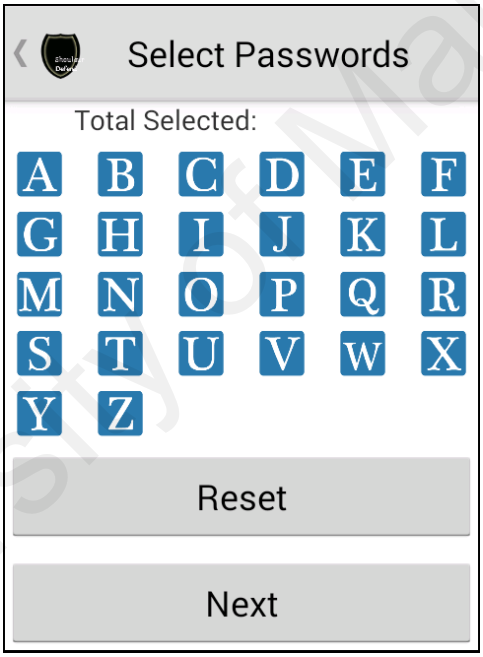

Figure 4.7 Image Registration Interface

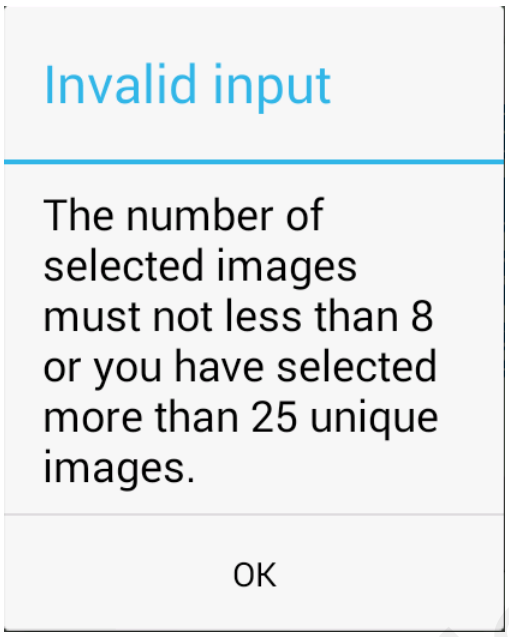

Figure 4.8 Exception Handling Interface of Image Selection Process

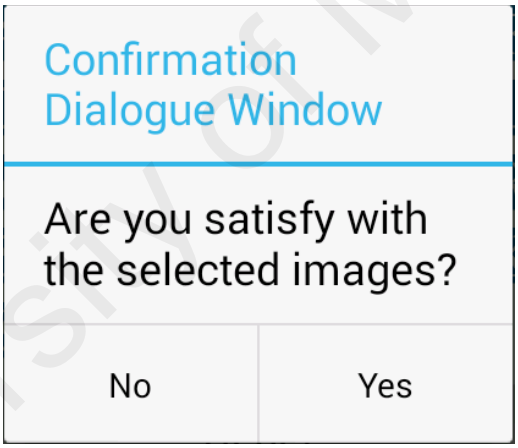

Figure 4.9 Confirmation Dialogue Window

```
SET coorx = interger list for x-coordinates
SET coory = interger list for y-coordinates
SET count = 0
SET passwordlist = null

ADD coorX = image's x-coordinates
ADD coorY = image's y-coordinates
count INCREMENT by 1
passwordlist = ADD image

IF count EQUAL 0
        LAUNCH warning no image selected
ELSE IF count MORE THAN 25
        LAUNCH warning maximum images selected
ELSE
        CREATE user ID, shift vertical, shift horizontal, passwordlists
```

Figure 4.10 Pseudo-code of the Image Registration Process

4.2.2 Authentication Procedure

The authentication procedure consists of two stages:

- Username verification
- Pass-images verification

4.2.2.1 Username Verification

Firstly, the user has to enter the correct username. An error dialogue window will be displayed if the username does not match with the registered username. The user has to repeat the username verification process. Otherwise, the user will direct to the pass-images verification process.

4.2.2.2 Pass-images Verification

After completing the username verification process, the user is directed to a challenge set which consists of 25 images in a 5 x 5 grid cell (see Figure 4.11). Initially, the grid cell is filled up with the registered images using a uniform randomization algorithm. After that, the grid cell is filled up with the decoy images using a uniform randomization algorithm. To address the frequency of occurrence analysis (FOA) attack

mentioned by (Por, 2013), the leftover image is bound with the username permanent and it will not show in the subsequence authentication challenge sets.

During the pass-images verification process, the user needs to identify the correct pass-images using the proposed method. A successful login message will be displayed if the user manages to identify the correct pass-images. An error message will be displayed for an invalid login. If an unsuccessful attempt detected, user will be given a brand new challenge set. The same images are used in every challenge sets, but the images position would be difference. The images are randomly allocated within the grid cell using a uniform randomization algorithm.

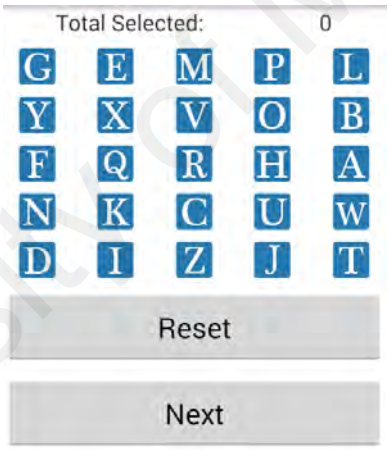

Figure 4.11 Pass-images Verification Interface

A block username feature is implemented. If system detected three failed login attempts, the account will be suspended. This password policy is followed from banking systems. The suspended account can only be unlocked by the system administrator. However, this feature is disabled during the user study testing so that attackers can have unlimited trials. An assumption is made whereby the attackers will not be able to discover the correct pass-images to login as if the user's registered images and the knowledge of

shifting direction during the enrolment procedure are secured from attackers when storing into a database.

4.2.2.2.1 Proposed Method

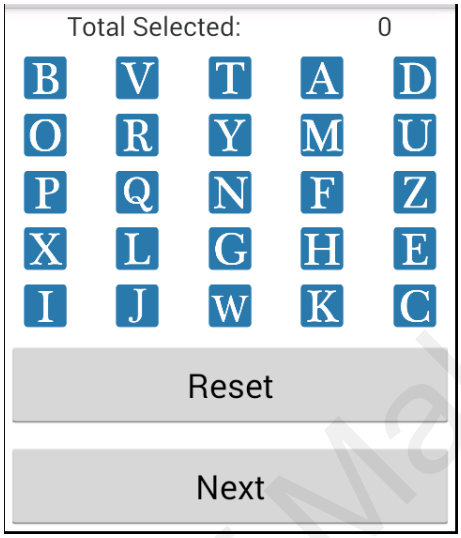

Figure 4.12 A Challenge Set Sample

An example of a single challenge set is shown in Figure 4.12. Assuming the registered images and the shifting direction of a user are as follows:–

- Registered Images: RAMBUTAN
- Vertical Shifting Direction: Down3
- Horizontal Shifting Direction: Right1

Firstly, the user needs to identify the position of the first registered image (“R”) in a challenge set. After that, the user has to apply the registered shifting direction (three steps down and one step right) to determine the first pass-image (“W”). The black arrows are used to indicate the direction for determining the pass-images (see Figure 4.13). To determine the second pass-image and the subsequence pass-images, the same process is used.

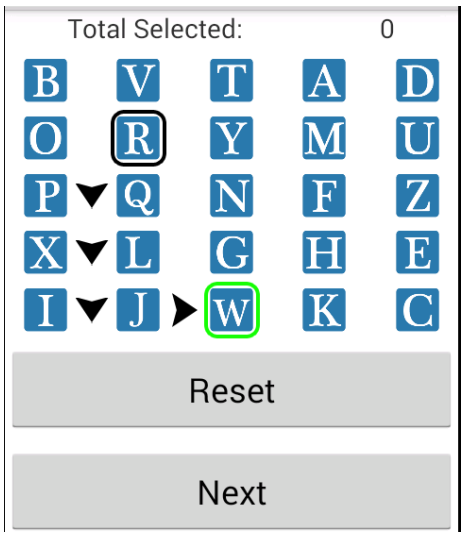

Figure 4.13 Normal Case

There is a special case for determining the fifth pass-image. To obtain the fifth pass-image, the user has to move three steps downward from the registered image ("U"). After moving three steps down, the user has to move one wrapped around step to the left side of the row of "C". Therefore, the fifth pass-image for "U" is "I" (see Figure 4.14).

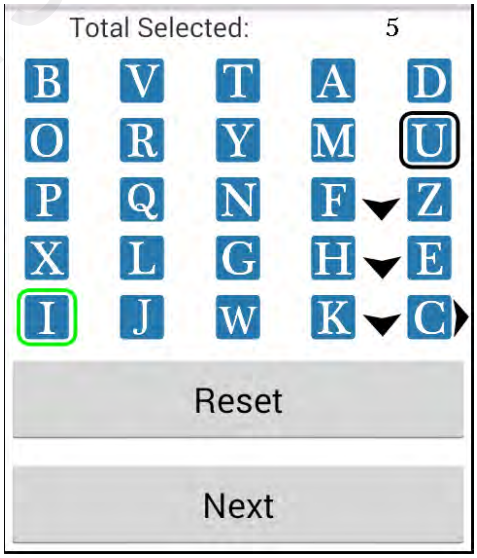

Figure 4.14 Special Case – Image Located at the Right/Left Edge of the Grid

There is another special case for determining the last pass-image. To obtain the last pass-image, the user has to move three steps down and one step right from the last registered image ("N"). After moving two steps downward, the user has to move one wrapped around step to the up side of the column of "W". Therefore, the last pass-image for "N" is "A" (see Figure 4.15).

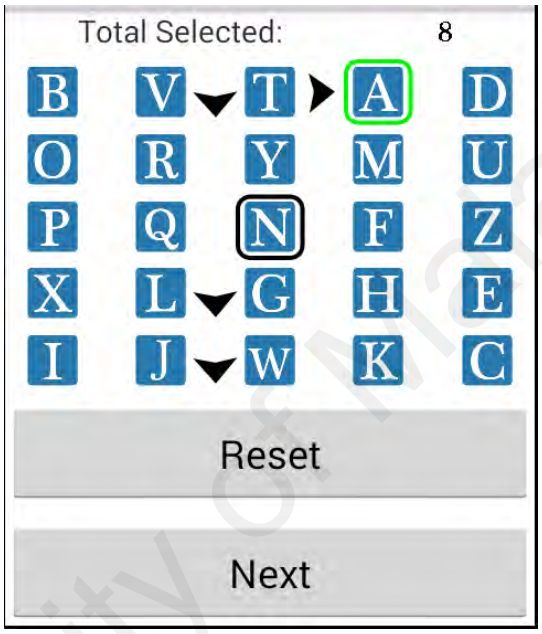

Figure 4.15 Special Case – Image Located at the Top/Bottom Edge of the Grid

The user has to click on the pass-images (WECLIHEA) in sequence and press the "Next" button to perform password validation. User can click the "Reset" button to reset the clicks. The pseudo-code of the proposed algorithm is shown in Figure 4.16.

```
Login

SET login ID = user input username string

CHECK database
        IF login ID found THEN
                LAUNCH password authentication window
        ELSE
                LAUNCH warning user ID not found

SET login coorX = image's X-coordinates
SET login coorY = image's Y-coordinates
SET count = password list count

ADD login coorX = images's SELECTED X-coordinates
ADD login coorY = images's SELECTED Y-coordinates
ADD images into login list
INCREMENT count

SET TemppassX = coorX ADD shift horizontal
SET TemppassY = coorX ADD shift vertical

IF RESET
        count = null
        login list = null
ELSE
        FOR list
                If list TemppassX AND TemppassY EQUAL list login coorX & login coorY
                        LAUNCH successful login window
                else
                        LAUNCH warning wrong password inserted
```

Figure 4.16 Pseudo-code of the Authentication Procedure

4.3 File Storage System

Figure 4.17 shows the database used by the proposed system. SQLite database was selected because it does not require any complicated configuration and it is easy to maintain. There are three tables used in the proposed system and they are PasswordPicture, User and Login Attempt tables. PasswordPicture table is used to store the images used in the proposed system. This table has four fields – Id, UserId, PictureId and SequenceNumber. Id is an auto-increment that works as a unique identifier to keep track of each record in this table. UserId is a foreign key and it is used as a reference to the User table. PictureId and SequenceNumber are used to store the registered images and its sequence selected by a user respectively.

User table is used to record users registered information. There are seven fields in this table – Id, UserId, IsLock, FailedAttemptCount, SecretShiftHorizontal, SecretShiftVertical and SecretCount. Id is an auto-increment that works as a unique identifier to keep track of each record in this table. UserId is used to store a unique username keyed in by a user. FailedAttemptCount is used to record the number of unsuccessful login attempts. SecretShiftHorizontal and SecretShiftVertical are used to store the horizontal and vertical movement shifting information chosen by a user respectively. SecretCount is used to store the number of images chosen by a user.

Login Attempt table is used to record user login attempts. There are six fields in this table – Id, UserId, ChallengeSet, IsSuccessful, IsLocked and FailedAttempt. Id is an auto-increment that works as a unique identifier to keep track of each record in this table. UserId is a foreign key and it is used as a reference to the user table. ChallengeSet is used to store the 25 images information used by each user during the authentication procedure. IsSuccessul and IsLocked are used to record the login attempt result and the user account status. FailedAttempt is used to store the unsuccessful login attempts. Zero is assigned as a default value assigned to this field. The user account will be locked if the value reaches three. This value will reset to zero for every successful login.

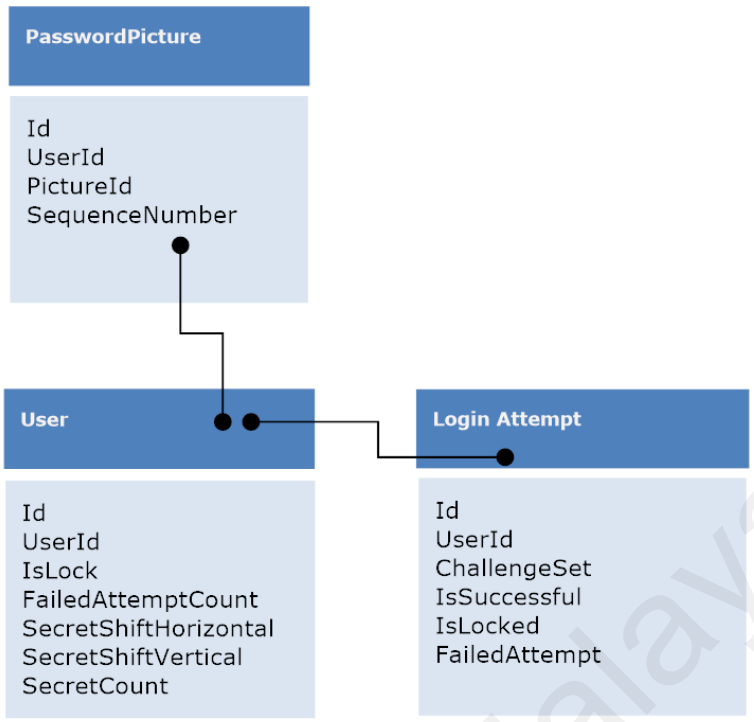

Figure 4.17 File Storage Database Tables

4.4 Summary

The proposed user authentication system, which consists of enrolment and authentication procedures, was presented in this chapter. The proposed system used alphabets (A to Z) as images. A user was required to register minimum of eight images during the enrolment procedure. Similar image is allowed to register more than one time. However, the user was allowed to register up to twenty-five unique images due to the number of grid size used. To prevent FOA attack, the unused image was bound with the username permanent and it will not show in the subsequence authentication challenge sets. During authentication procedure, the user needs to identify the correct pass-images using the proposed method. The proposed method used shifting direction to resist shoulder-surfing attack. The details of the proposed method were presented in the authentication procedure. The end of this chapter had discussed the storage method used for the proposed system. The system testing and evaluation of the proposed method will be discussed in the next chapter.

Chapter 5 System Testing and Evaluation

5.1 Introduction

This chapter discusses the system testing and evaluation of the proposed method. The procedure used, results obtained, and analyses that have been carried out in the user study are discussed in details. The comparison of the related work is presented before a chapter summary is deliberated.

5.2 User Study

Due to budget and geographical constraints, the user study was conducted at a company named Public Bank Berhad that located at Bangi, Selangor, Malaysia. This company is an international company and has approximately 500 employees. There are 102 participants involved in this user study. 64 of the participants were males and another 38 of them were females. 6% of the participants were below 20 years old; 51% of them were from the age group of 21-30 years old; another 33%, 7% and 3% of the participants were from the age group of 31-40, 41-50 and more than 50 years old respectively. The confidence interval (margin of error) of this user study is approximately 8.62% based on the 95% confidence level, sample size of 102, population size of 500, and 50% of population proportion.

5.2.1 Procedure, Results and Analysis of the User Study

There are four phases involved in this user study. In phase 1, participants were requested to provide their personal information and answer a questionnaire that consists of six questions (see Appendix A). The objective of this survey is to understand whether the participants have the knowledge and exposure to graphical password and shoulder-surfing security threat.

The phase 1 survey results show that 79% of the participants knew about graphical password and only 21% of them do not know about graphical password. Among all of the participants, only 40% of the participants have never come across of using any graphical password while others have experience in using graphical password. In terms of shoulder-surfing exposure, 42% of the participants know about shoulder-surfing attack and the remaining 58% have zero knowledge about shoulder-surfing attack. From the data that have been gathered, it shows that most of the participants have experienced in using graphical password, but a majority of them do not aware that these graphical authentication systems can be shoulder-surfed by attackers until we have demonstrated the shoulder-surfing testing to them.

In phase 2, a demonstration regarding the steps used in the proposed method to perform the enrolment and authentication procedures were shown to the participants via a notebook. After the demonstration, the participants were requested to register their images and log in using the registered images for ten successful attempts. The login time were recorded by the proposed system. The purpose of recording the ten successful login time is to study the average time taken by the users so that in future the proposed method can be further improved to achieve better usability aspect.

Figure 5.1 shows the mean time for 10 successful logins recorded by the proposed system. From the graph, the login time decreases from the first login attempt until the tenth login attempt. This phenomenon shows that the participants were familiarized themselves with the proposed method used after they have tried several times. From the data that have been gathered, the shortest time required for a successful login was 29 seconds and the longest time required was 80 seconds. On average, the login time used for the participants to login into the proposed system is about 42 seconds. Due to time

constraint, the usability aspect is not cover in this research work therefore it will not be discussed further in this chapter.

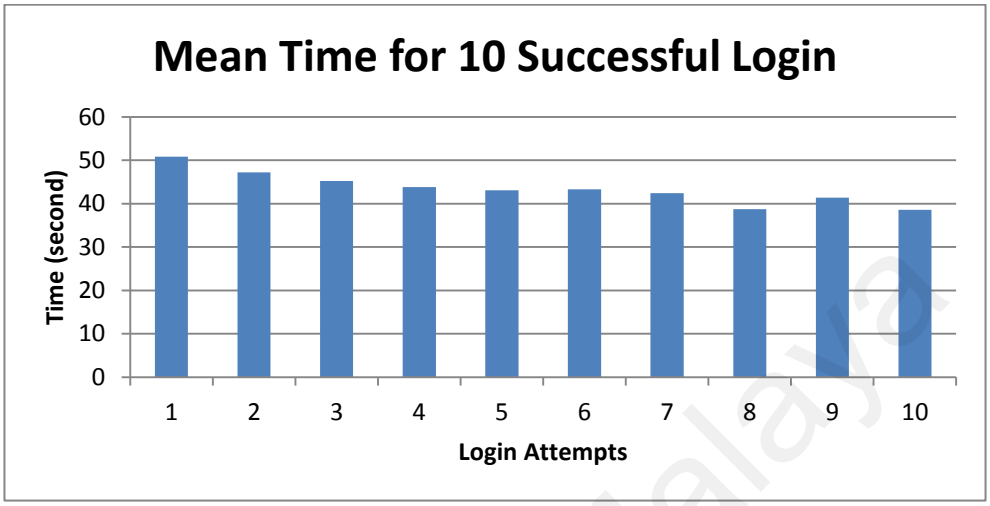

Figure 5.1 Mean Time for 10 Successful Login

In phase 3, a video that recorded a successful login session was shown to the participants. The participants were given unlimited trials to guess the pass-images used based on the information shown in the video. The participants were allowed to access and watch the video any time. The shoulder-surfing testing results show that no participant is able to guess the pass-images used based on the information shown in the demonstration video.

In phase 4, the participants were required to answer a survey (see Appendix A). The objective of the survey is to gather the participant's feedback regarding the proposed method used in resisting shoulder-surfing attack and the strategies they uses during the shoulder-surfing testing. The feedback regarding the proposed method used in resisting shoulder-surfing attack was gathered. 72% and 28% of the participants were strongly agreed and agreed that the proposed method used was able to resist shoulder-surfing

attack respectively. This result implies that the proposed method can resist shoulder-surfing attack.

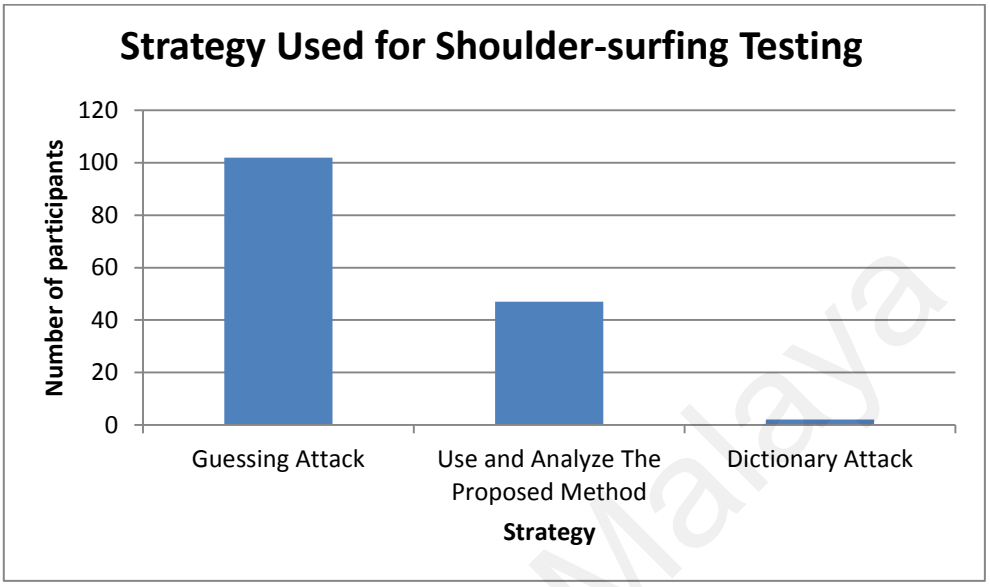

Figure 5.2 Strategy Used for Shoulder-surfing Testing

The strategies used by the participants during the shoulder-surfing testing are shown in Figure 5.2. All participants used guessing attack method; while 47 of them used the proposed method to log in, and 2 participants used the dictionary attack to log in. The proposed method uses shifting directions (vertical shift and horizontal shift) to delude the attackers from obtaining the correct pass-images used. A uniform randomization algorithm was used to ensure the images used were randomly allocated within the grid cell for every challenge set. Moreover, the leftover decoy images are bound with the username permanently and it will not show in the subsequent challenge sets. Therefore, it is impossible for the attackers to gain the user registered images although the attackers knew how the proposed method works. Thus, this result implies that the proposed method can resist both direct observation and video recorded shoulder-surfing attacks.

5.3 Comparison of the Related Work

Table 5.1 Comparison of the Related Work

Graphical Authentication System	Resist Shoulder-surfing Attack	
	Direct Observation	Video Recorded
Déjà Vu (Dhamija and Perrig, 2000)	No	No
Passfaces™ (Davis et al., 2004)	No	No
Convex Hull Click (Wiedenbeck et al., 2006)	Yes	No
WYSWYE (Khot et al., 2012)	Yes	No
Sonal (Sonal et al., 2015)	Yes	No
Kolay (Kolay et al., 2017)	No	No
Por (Por et al, 2017)	Yes	No
Dhandha (Dhandha & Parekh, 2017)	Yes	No
EvoPass (Yu et al., 2017)	Yes	No
Proposed Method	Yes	Yes

Table 5.1 presents the comparison of the proposed authentication system and the selected recognition based graphical passwords which discussed earlier in Chapter 2. As shown in the table, the proposed authentication system is the only system that can resist both direct observation and video recorded shoulder-surfing attacks. Convex Hull Click, WYSWYE, Sonal, Por, Dhandha, and EvoPass are able to prevent direct observation shoulder-surfing attack but these systems are vulnerable to video recorded shoulder-

surfing attack because attackers are able to reveal the password by observing multiple video recorded shoulder-surfing sessions. Other systems such as Déjà Vu, Passfaces™, and Kolay are vulnerable to both direct observation and video recorded shoulder-surfing attacks.

5.4 Summary

This chapter discussed the system testing and evaluation of the proposed system. A user study was conducted to test the feasibility of the proposed system in resisting shoulder-surfing attack. The shoulder-surfing testing results show that no participant can shoulder-surf and obtain the pass-images used based on the information shown in the demonstration video. In the other words, the proposed method that uses shifting directions (vertical shift and horizontal shift) is able to trick attackers from identifying the correct pass-images used. Moreover, the images used are randomly allocated within the grid cells for each challenge set, therefore, it is impossible for shoulder-surfing attackers to gain the user registered images although the whole login session was recorded. A comparison between the proposed method and the related works was presented. The proposed method is the only one that can prevent both direct observation and video recorded shoulder-surfing attacks. The next chapter presents the conclusion of this dissertation.

Chapter 6 Conclusion

6.1 Introduction

This first part of this chapter is the discussion of the objective accomplished in this study. The contribution of this dissertation is highlighted and the future work is presented at the end of the chapter.

6.2 Objective Accomplished

The objectives of this research work are as follows:-

1. To propose a graphical password method that is able to prevent video recorded and direct observation shoulder-surfing attacks.
2. To design and implement the proposed method.
3. To test and evaluate the feasibility of the proposed method in resisting video recorded and direct observation shoulder-surfing attacks using user study.

To accomplish the first objective, a graphical method that uses shifting directions was proposed to prevent video recorded and direct observation shoulder-surfing attacks. The proposed method is based on knowledge-based indirect image selection method to perform authentication. A user needs to use the registered images and shifting direction to identify the pass-images used in each challenge set. A uniform randomization algorithm was used to ensure the images used were randomly allocated within the grid cell for every challenge set. Moreover, the leftover decoy images are bound with the username permanently and it will not show in the subsequent challenge sets. Therefore, it is impossible for the attacker to gain the user registered images although the whole login session was recorded.

In order to attain the second objective, the proposed method was transformed into a workable prototype. The proposed system was developed in order to test the feasibility in preventing both direct observation and video recorded shoulder-surfing attacks. The proposed system was developed using C# programming language and the system was deployed using Visual Studio. SQLite was used as the database to store the user portfolio, registered images data and the shifting direction information.

To accomplish the third objective, the proposed system was tested and evaluated using a user study. There are four phases in the evaluation process. In phase 1, a pre-survey was conducted to explore the exposure and knowledge of the participants towards graphical password and shoulder-surfing security threat. A demonstration of the proposed system was presented to the participants in phase 2. The participants were guided to undergo the enrolment process and using the proposed system to login. In phase 3, a user study was carried out to assess the feasibility of the proposed method in resisting shoulder-surfing attack. A successful login video was shown to the participants. The participants were given an unlimited trial to login to the proposed system. In phase 4, a post-survey was conducted to gather the participants' feedback after they have conducted the shoulder-surfing attack. The results were gathered and analyzed.

6.3 Contributions

A proposed method that uses shifting directions was proposed to trick attackers from identifying the correct pass-images used. This method required users to register their password images as well as to choose the shifting direction based on their preferences. Users were needed to use the proposed method to determine the correct pass-image before they can login. Only users who have the knowledge of both registered images and the registered shifting direction can derive the pass-images. The pass-images used

to login for every challenge set can be the registered images or decoy images. Hence, it is impossible for the attacker to gain the pass-images used even though the whole login session was recorded.

A user study was carried out to assess the feasibility of the proposed method in resisting shoulder-surfing attack. The shoulder-surfing test results shown that, the proposed method was able to preventing shoulder-surfing attack. An analysis between the proposed method and the related works was conducted. The comparison result shown that the proposed method was the only method that can prevent both direct observation and video recorded shoulder-surfing attacks.

As a value added feature, the proposed system used auto filtering method to ensure the same images appear in every challenge set to prevent Frequency of Occurrence Analysis (FOA) attack mentioned by (Por, 2013). During the authentication phase, the grid cell is filled up with the registered images using a uniform randomization algorithm. After that, the grid cell is filled up with the decoy images using a uniform randomization algorithm. To prevent FOA attack, the leftover image is bound with the username permanent and it will not show in the subsequence authentication challenge sets.

6.4 Future Enhancement

Usability is an aspect that can be considered for future research. Methods that can help or improve the users to remember and recall their password will be the future work for this research. As if a method can be very secure but it must not burden the users to memorize or recall their password. Moreover, the time required for users to gain access into the system should be reasonable. If the time required for the users to login is too long, the users might lose interest to use the propose method or system.

References

Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., & Bhogle, P. (2015). Comparison of Graphical Password Authentication Techniques. *International Journal of Computer Applications*, 116, 11-14. doi:10.5120/20299-2332.

Bianchi, A., Oakley, I., & Kim, H. (2016). PassBYOP: Bring Your Own Picture for Securing Graphical Passwords. *IEEE Transactions on Human-Machine Systems*, 46(3), 380-389. doi:10.1109/THMS.2015.2487511.

Dave, K. T. (2013). Brute-force Attack "Seeking but Distressing". *International Journal of Innovations in Engineering and Technology (IJIET),* 2(3), 75-78.

Davis, D., Monrose, F., & Reiter, M. K. (2004). On user choice in graphical password schemes. Paper presented at the *Proceedings of the 13th conference on USENIX Security Symposium*, 11-11, Berkeley, CA, USA.

Dhamija, R., & Perrig, A. (2000). Deja Vu: A User Study Using Images for Authentication. Paper presented at the In *Proceedings of the 9th USENIX Security Symposium*, 45-58, Denver, Colorado, USA.

Dhandha, D., & Parekh, C. (2017). Enhancement of Password Authentication System Using Recognition based Graphical password for web Application. *International Journal of Advanced Research in Computer Science*, 8(5), 1135-1138.

Eiband, M., Khamis, M., Zezschwitz, E. v., Hussmann, H., & Alt, F. (2017). Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. Paper presented at the *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 4254-4265, Denver, Colorado, USA.

Gokhale, A., & Waghmare, V. (2015). A Study of Various Passwords Authentication Techniques. *International Journal of Computer Applications*, 1-5.

Golar, P. C., & Adane, D. S. (2016). Critical analysis of 2-dimensional graphical authentication systems. Paper presented at the *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, 150-155, Pune, India.

Golofit, K. (2007). Picture Passwords Superiority and Picture Passwords Dictionary Attacks. *Journal of Information Assurance and Security 2*, 179-183.

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., & Richer, J. P. (2018). Digital Identity Guidelines. *NIST Special Publication* 800-63B. doi:10.6028/NIST.SP.800-63b.

Khedr, W. I. (2018). Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol. *Journal of Information Security and Applications*, 39, 41-57. doi:10.1016/j.jisa.2018.02.003.

Khot, R. A., Kumaraguru, P., & Srinathan, K. (2012). WYSWYE: Shoulder surfing defense for recognition based graphical passwords. Paper presented at the *Proceedings of the 24th Australian Computer-Human Interaction Conference*, 285-294, Melbourne, VIC, Australia.

Kolay, R., Vora, A., & Yadav, V. (2017). Graphical Password Authentication Using Image Segmentation. *International Research Journal of Engineering and Technology (IRJET)*, 4(3), 1694-1698.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22(C), 113-122. doi:10.1016/j.jisa.2014.09.005.

Lashkari, A. H., Farmand, S., Zakaria, O. B., & Saleh, R. (2009). Shoulder Surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security*, 6(2), 145-154.

Li, Y., Wang, H., & Sun, K. (2016). A study of personal information in human-chosen passwords and its security implications. Paper presented at the *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 1-9, San Francisco, CA, USA.

Passfaces Corporation. (2004). The Science behind Passfaces. Retrieved from White paper URL: http://www.realuser.com/published/ScienceBehindPassfaces.pdf.

Por, L. Y., Ku, C. S., Islam, A., & Ang, T. F. (2017). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. *Frontiers of Computer Science*, 11(6), 1098-1108. doi:10.1007/s11704-016-5472-z.

Simha, T. S., & Srinivasulu, D. (2017). Pass Matrix checks for Login Authentication. *International Journal of Computer Science Trends and Technology (IJCST)*, 5(6), 5-13.

Sonal, G., Poonam, K., Ketaki, M., & Bhagyashri, S. (2015). Shoulder Surfing Resistant Graphical Password Scheme. *International Journal for Scientific Research & Development*, 3(8), 291-294.

Tank, H., & Harsora, V. (2015). A Survey on Secure Virtual Password and Phishing Attack. Paper presented at the Conference: *4th International Conference on Computer Science and Information Technology (ICCIT 2015)*, 25-29, Gujarat, India.

Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.-C. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. Paper presented at the *Proceedings of the working conference on Advanced visual interfaces*, 177-184, Venezia, Italy.

Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W. T., & Song, L. (2017). EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security*, 70, 179-198. doi:10.1016/j.cose.2017.05.006.

Zviran, M., & Erlich, Z. (2006). Identification and Authentication: Technology and Implementation Issues. *Communications of the Association for Information Systems*, 17, 90-105.