

The copyright © of this thesis belongs to its rightful author and/or other copyright owner. Copies can be accessed and downloaded for non-commercial or learning purposes without any charge and permission. The thesis cannot be reproduced or quoted as a whole without the permission from its rightful owner. No alteration or changes in format is allowed without permission from its rightful owner.



**TOWARDS AN EFFECTIVE RECOGNITION GRAPHICAL  
PASSWORD MECHANISM BASED ON  
CULTURAL FAMILIARITY**

**ABDULLAH IBRAHIM SHABAN**



**UUM**  
Universiti Utara Malaysia

**MASTER OF SCIENCE (INFORMATION TECHNOLOGY)  
UNIVERSITI UTARA MALAYSIA  
2017**

## **Permission to Use**

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:



Dean of Awang Had Salleh Graduate School of Arts and Sciences  
UUM College of Arts and Sciences  
Universiti Utara Malaysia

06010 UUM Sintok

## Abstrak

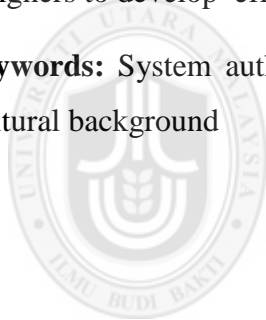
Kata laluan berasaskan teks untuk pengesahan adalah terdedah kepada serangan kamus kerana pengguna cenderung untuk mencipta kata laluan yang lemah supaya mudah diingat. Apabila berurusan dengan pengesahan pengguna, gambar adalah lebih mudah diingat berbanding dengan perkataan. Oleh itu, kajian ini bertujuan menentukan jenis gambar yang mungkin dipilih berdasarkan latar belakang kebudayaan pengguna. Ia juga mengkaji hubungan antara pilihan kata laluan dan kebiasaan budaya serta juga kesan Kata Laluan Grafik (GP) terhadap keselamatan dan kebolehgunaan. Senarai garis panduan telah dicadangkan bagi pengiktirafan kata laluan grafik. Ia dipercayai boleh meningkatkan keselamatan dan juga kebolehgunaan. Seramai 40 orang pelajar telah mengambil bahagian untuk membina pangkalan data GP. Kemudian, penilaian telah dijalankan untuk mengkaji kebiasaan dan keupayaan pengguna mengenali gambar dari pangkalan data dengan menggunakan 30 responden yang lain. Kadar login yang Berjaya adalah 79.51% dan ini menunjukkan bahawa GP berdasarkan kebudayaan telah meningkatkan kebiasaan responden dengan menggalakkan daya ingatan mereka. Responden yang memilih GP biasa mempunyai kadar cubaan meneka yang lebih tinggi berbanding responden yang memilih gambar yang tidak biasa. Kesimpulannya, sebanyak 8 garis panduan telah di bentuk berdasarkan aspek pilihan pengguna untuk memilih dan memproses GP. Garis panduan ini boleh digunakan oleh pereka sistem GP untuk membangunkan sistem GP yang berkesan..

**Kata kunci :** Pengesahan sistem, Kata laluan grafik, Serangan keselamatan, Kebolehgunaan, Latar belakang kebudayaan

## Abstract

Text-based passwords for authentication are exposed to the dictionary attack as users tend to create weak passwords for easy memorability. When dealing with user's authentication, pictures are more likely to be simply remembered in comparison with words. Hence, this study aimed to determine the types of pictures in accordance to users' cultural background. It also investigated the relationship between the choices of password and the cultural familiarity along with the effect of Graphical Password (GP) on security and usability. A list of guidelines was proposed for the recognition of graphical passwords. This is believed to increase the security as well as usability. A total of 40 students were recruited to build a GP database. Further, an evaluation was conducted to investigate users' familiarity and recognition of the GP from the database using 30 other respondents. The results showed that the 30 participants positively responded to the familiar pictures in accordance to their cultures. The result of successful login rate was 79.51% which indicates that cultural-based GP has increased the respondents' familiarity by promoting their memorability. Further, the respondents who chose familiar GP had higher guessing attack rate than the unfamiliar GP. Finally, a total of 8 guidelines were established based on the aspects that correspond to the users' preferences for choosing and processing GP. These guidelines can be used by graphical password system designers to develop effective GP systems.

**Keywords:** System authentication, Graphical password, Security attack, Usability, Cultural background



UUM  
Universiti Utara Malaysia

## Acknowledgement

First and foremost, all praise is for Allah, Who enlightened us with faith and knowledge, and who is lightening my way throughout the completion of this thesis.

I would like to express my deep appreciation to Dr. Nur Haryani Zakaria, my supervisor, for her valuable assistance, enthusiastic encouragement and for her patient guidance to help me to achieve my goal. Without her valuable support, my thesis would not have been possible.

I would like to extend my appreciation to AP Dr. Azham and AP Hatim, for graciously reviewing this work and giving valuable suggestion and comments on my work.

I would like to express my gratitude to the greatest parents in this world. Thank you so much for everything you have done for me and I hope my prayers and good deeds will return a little from the many you gave to me. You always being everything to me thanks for every moment you spent watching over me. Thanks for the everlasting prayers, tenderness, support, and care. To both of you, I submit this work. May Allah bless you with happiness.

To my wife, I express special thanks for her valuable support, encourage and for always being everything to me. For my lovely daughters, Mariam, Elaf and Tasneem, thank you so much for your patient while I was not beside you. Without you all, this degree would have been so hard. May Allah bless my family.

Finally, I would like to thank all of my friends for their support and encouragement throughout my study.

## Table of Contents

Permission to Use.....	I
Abstrak .....	II
Abstract .....	III
Acknowledgement.....	IV
Table of Contents .....	V
List of Tables.....	X
List of Figure.....	XI
List of Abbreviations.....	XIII
<b>CHAPTER ONE INTRODUCTION .....</b>	<b>1</b>
1.1 Background of the Study .....	1
1.2 Problem Statement.....	4
1.3 Research Questions.....	6
1.4 Research Objectives.....	6
1.5 Significance of the Study.....	7
1.6 Scope of the Study .....	7
1.7 Overview of the Thesis.....	8
<b>CHAPTER TWO LITERATURE REVIEW .....</b>	<b>10</b>
2.1 Authentication Methods.....	10
2.2 Knowledge Based .....	12
2.2.1 Traditional Text-Based Passwords .....	12
2.2.2 Graphical-Based Passwords.....	13
2.3 Existing Studies on Graphical Password .....	17
2.4 Security of Graphical Password.....	29
2.4.1 Guessing Attack .....	29
2.4.2 Dictionary Attack.....	30
2.4.3 Brute Force (Exhaustive) Attack .....	30

2.4.4	Spyware Attack.....	31
2.4.5	Shoulder Surfing Attack .....	32
2.4.6	Social Engineering Attack .....	32
2.5	Usability of Graphical Passwords.....	33
2.6	Current Utilization of Graphical Passwords .....	34
2.7	Types of Pictures Used for Recognition-Based Graphical Passwords .....	35
2.8	Challenge Set Designs for Recognition-Based Graphical Passwords .....	38
2.9	Recognition-Based Graphical Passwords Methods (RBGP).....	39
2.9.1	Passface Scheme Passwords .....	39
2.9.2	Dejavu Scheme (Random Art Passwords).....	40
2.9.3	Triangle Scheme (Object Passwords) .....	42
2.9.4	Story Scheme .....	43
2.9.5	Comparison of Typical Recognition-Based Graphical Password .....	44
2.10	Comparison of Typical Recognition-Based Schemes Resistance Against Possible Attacks .....	45
2.11	Culture .....	47
2.12	Cultural Images.....	48
2.13	Cultural Images in Graphical Passwords .....	48
2.14	National Images .....	50
2.15	Cultural Effects on Usability and Security of Recognition-Based Graphical Password Authentication.....	51
2.16	Cultural Models .....	52
2.17	Overview of Literature Review .....	54
2.18	Summary.....	55
<b>CHAPTER THREE RESEARCH METHODOLOGY .....</b>		<b>56</b>
3.1	Introduction.....	56
3.2	Research Methodology .....	56
3.3	Research Design .....	57



3.4	Phase One : Identification of the Problem.....	59
3.5	Phase Two : Collecting Pictures .....	59
3.6	Phase Three : Construction Database and Prototype.....	60
3.6.1	Construct Database and Prototype .....	60
3.6.2	Registration in the System .....	61
3.7	Phase Four : Experiment.....	61
3.7.1	Security Aspects .....	62
3.7.2	Usability Aspect.....	62
3.8	Phase Five : Data Analysis .....	63
3.9	Phase Six : Discussion .....	63
3.10	Data Collection Procedures .....	64
3.11	Sampling Technique and Study Sample .....	64
3.12	Research Instruments.....	66
3.13	Pilot Test.....	66
3.13.1	The Importance of Pilot Study.....	67
3.13.2	The Goal of a Pilot Study .....	68
3.13.3	Validity and Reliability.....	69
3.13.4	Face Validity.....	70
3.13.5	Population Distribution of the Pilot Study.....	70
3.13.6	Pilot Test Results (Appendix A).....	71
3.13.7	Pilot Test Results (Appendix B,C and D).....	73
3.14	Summary.....	73
<b>CHAPTER FOUR CULTURAL FAMILIARITY’S IMPACT ON CHOOSING PICTURES FOR RECOGNITION-BASED GRAPHICAL PASSWORDS .....</b>		<b>74</b>
4.1	Introduction.....	74
4.2	The Aims of the Experiment 1.....	75

4.3	The Design and Method of Experiment 1.....	76
4.4	The Procedure of Experiment 1.....	76
4.5	Results of the Experiment 1.....	77
4.5.1	Respondent Profile Appendix (A) .....	77
4.5.2	Pictures Database .....	79
4.6	The Aim of Experiment 2.....	81
4.7	The Design of Experiment 2.....	81
4.8	The Method of Experiment 2.....	85
4.9	The Procedure of Experiment 2.....	86
4.10	Results of the Experiment 2.....	88
4.10.1	Respondent Profile Appendix (B,C and D) .....	88
4.10.2	Number of Familiar Pictures Selected .....	90
4.11	Discussion.....	91
4.12	Summary.....	92
<b>CHAPTER FIVE User Guidelines based on Cultural Familiarity's</b>		
<b>Impact on the Security and Usability of Recognition- Based</b>		
<b>Graphical Passwords .....</b>		<b>94</b>
5.1	Introduction.....	94
5.2	Participants of Experiment .....	95
5.3	Reliability Test for Appendix (B,C and D) .....	95
5.4	Security Evaluation ( Experiment 3 ) .....	96
5.4.1	The Aim of Experiment 3 .....	96
5.4.2	Educated guessing attack .....	97
5.4.3	The Method of Experiment 3.....	98
5.4.4	The Design of Experiment 3.....	99
5.4.5	The Procedure of Experiment 3 .....	100
5.4.6	The Result of Experiment 3 .....	101

5.4.7	Post-questionnaire (Appendix C) Results for Experiment 3 .....	102
5.4.8	Discussion of Experiment 3 .....	104
5.5	Usability Evaluation ( Experiment 4 ) .....	106
5.5.1	The Method of Experiment 4.....	106
5.5.2	The Procedure of Experiment 4 .....	107
5.5.3	Results of Experiment 4.....	109
5.5.4	Discussion of Experiment 4.....	112
5.6	The Aim of Experiment 5 .....	114
5.7	The Method of Experiment 5.....	115
5.8	The Procedure of Experiment 5 .....	115
5.9	The Results of Experiment 5 .....	116
5.10	Summary.....	119
<b>CHAPTER SIX CONCLUSION AND FUTURE WORKS .....</b>		<b>120</b>
6.1	Introduction.....	120
6.2	Discussion.....	121
6.3	Research Contributions.....	122
6.4	Limitations of the Study .....	123
6.5	Future work.....	123
<b>References .....</b>		<b>124</b>
<b>Appendix A .....</b>		<b>135</b>
<b>Appendix B .....</b>		<b>136</b>
<b>Appendix C .....</b>		<b>137</b>
<b>Appendix D .....</b>		<b>138</b>
<b>Appendix E .....</b>		<b>139</b>

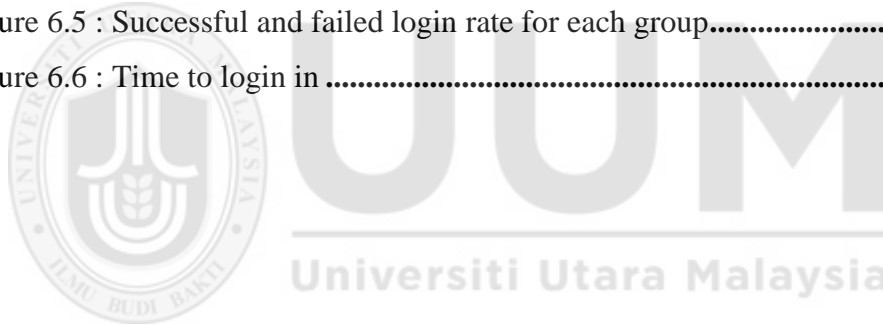
## List of Tables

Table 2.1 : Summary of Authentication methods .....	10
Table 2.2 : Comparison of different graphical password mechanisms in previous studies.....	27
Table 2.3 : Comparison of Typical Recognition-Based Graphical Password .....	44
Table 2.4 : Comparison of typical recognition-based schemes.....	46
Table 3.1 : Questionnaires.....	66
Table 3.2 : Gender Distribution of the Pilot Study .....	71
Table 3.3 : Course Level Distribution of the Pilot Study.....	71
Table 3.4 : Time to finish the questionnaire of the Pilot Study .....	72
Table 3.5 : Reliability Testing Result .....	73
Table 5.1 : Familiar pictures based on the participants' preferences.....	84
Table 6.1 : Number of participants for each group in the study .....	95
Table 6.2 : Comparing the main with the pilot test results .....	96
Table 6.3 : GSR for culturally familiar and unfamiliar pictures .....	102
Table 6.4 : Login attempts among groups.....	109
Table 6.5 : Descriptive results for the usability test.....	112
Table 7.1 : Agreement rate among participants when registered for GP .....	117

## List of Figure

Figure 1.1 : General structure of the thesis .....	9
Figure 2.1: Classification of the Existing Graphical Passwords (Almuairfi, Veeraraghavan, & Chilamkurti, 2013).....	14
Figure 2.2 : Graphical Password Interface Used in Experiment (Weidenbeck et al., 2005).....	15
Figure 2.3 : Grid Selection: A User Selects a Drawing Grid in Which to Draw their Password (Thorpe and Van Oorschot, 2004) .....	16
Figure 2.4: Registration Stage for a Recognition-Based Graphical Password (English, 2012).....	17
Figure 2.5 : GO-pass (Tao 2006) .....	19
Figure 2.6 : User identification system (Syukri, Okamoto, and Mambo, 1998).....	20
Figure 2.7 : Graphical input displays (Jermyn, Mayer, Monroe, Reiter, and Rubin, 1999).....	21
Figure 2.8 : Inkblot example (Stubblefield and Simon, 2004).....	22
Figure 2.9 : Image recall example (Jansen, 2004) .....	23
Figure 2.10: Graphical password system framework (Eljetlawi, 2008).....	24
Figure 2.11: A graphical password scheme using culturally related pictures (Aljahdali and Poet, 2014c).....	25
Figure 2.12 : The human–computer interface for a user to enter his or her graphical password (Chang et al., 2012).....	25
Figure 2.13 : Passfaces .....	40
Figure 2.14 : déjà vu (Touraj, 2015) .....	41
Figure 2.15 : Triangle Scheme (Sobrado, 2002) .....	42
Figure 2.16 : Story Scheme (Farnaz, 2009). .....	43
Figure 2.17: Comparison of typical recognition schemes (Angeli et al. 2005) .....	45
Figure 2.18 : A Malaysian famous building called “PETRONAS Twin Towers .....	51
Figure 2.19 : Literature review Map .....	54
Figure 3.1 : Overall phases of research design .....	58
Figure 4.1 : The gender distribution of the respondents .....	77
Figure 4.2 : The academic degree distribution of the respondents .....	78
Figure 4.3 : The age distribution of the respondents.....	78
Figure 4.4 : The nationality distribution .....	79

Figure 4.5 : The number of pictures for each category .....	81
Figure 5.1 : : User interface for the first attempt.....	83
Figure 5.2 : Show the stored related information about the participants .....	86
Figure 5.3 : Show familiarity question.....	87
Figure 5.4 : The gender distribution of the respondents .....	88
Figure 5.5 : The academic degree distribution of the respondents .....	89
Figure 5.6 : The age distribution of the respondents.....	89
Figure 5.7 : Schools of the participant .....	90
Figure 5.8 : Number of pictures selected from Malaysia culture for creating graphical passwords .....	90
Figure 6.1 : Shows the security attack similarity with GP.....	99
Figure 6.2 : Relationship with victims	Figure 6.3 : Educational Background
.....	103
Figure 6.4 : Reasons behind guessing .....	103
Figure 6.5 : Successful and failed login rate for each group.....	110
Figure 6.6 : Time to login in .....	111



## **List of Abbreviations**

DAS Draw A Secret

GP Graphical Password

GPG Graphical Password Guideline

GSR Guessing Success Rate

RBGP Recognition Based Graphical Password

SR Successful login Rate

TL Time Login



# CHAPTER ONE

## INTRODUCTION

### 1.1 Background of the Study

The latest advances in networked computing bring a number of advantages to the security of applications along with possible chances for becoming a target to numerous online threats. As such, the application of computer security, which is viewed as complex paradigm, is now the main area for researchers to secure and enhance its current security mechanisms for the benefit of organizations and individuals (Colella & Colombini, 2012; Vacca, 2013). This include the constant upgrades to the security services which lay behind the need for protecting end-users against theft or damage of one's electronic resources. Even with today's security parameters, it become difficult for users to attain these updates (Cavalcante et al., 2012), which, in turn, led to raising the needs for adequate and simple security features that users can easily memorize and keep.

However, the actual ubiquity regarding graphical interfaces for applications, and input devices such as touch-screen devices that permit in addition to typed input, has opened the doors for developing various graphic user authentication approaches (e. g., (Bellare, Ristenpart, & Tessaro, 2012; Khanh Dang & Tri Dang, 2013; Mihajlov & Jerman-Blažič, 2011; Salim, Reid, & Dawson, 2015)). Graphical authentication approaches were initially introduced to suit devices which do not allow typewritten input. Furthermore, current graphical authentication approaches present the possibility for offering a kind of authentication which is closely more robust than text passwords (Renaud, Mayer, Volkamer, & Maguire, 2013). These efforts were based



on the authentic related issues which literature revealed to be the actual distribution regarding text security passwords chosen simply by end users (Nicholson, Dunphy, Coventry, Briggs, & Olivier, 2012).

The security settings behind such approaches are still lacking of the entropy to overcome large weakness regarding user authentication. Given the fact that pictures are likely to be more simply remembered in comparison with texts, it will be conceivable that humans can remember more robust passwords of the graphical nature (Umar, Rafiq, & Ansari, 2012).

Furthermore, it has become obvious that the key aspect in security measures research along with practice is the ability to provide reliable authentication, the dedication of no matter if a user should be permitted to entry to a presented system or perhaps resources (Werner & Hoover, 2012). Typically, alphanumeric passwords are commonly used for authentication. Nowadays other techniques, including biometrics along with smart cards, are among feasible alternatives.

Nonetheless, passwords will certainly remain as a dominant option for a while because of its high association with ongoing drawbacks connected with reliability, security measures, and cost of different technologies.

With the current moves for developing an effective mechanism for securing end-users information, graphical password is appeared to be just about the alternative conditions for alphanumeric code, as it is very time consuming process to consider alphanumeric code (Raza, Iqbal, Sharif, & Haider, 2012). When any application applies user-friendly authentication, it helps user to learn the instructions given easily and work with that request (Prasad, Prasad, Chakravarthy, & Avadhani, 2012). One with the major reasons for this procedure is based on psychological research on

human mind in which it reveals the feasibility for user to remember pictures than alphabets or digits (Gurav, Gawade, Rane, & Khochare, 2014).

Meanwhile, the current applications of graphical code are proposed as a substitute to text-based techniques that is motivated on the point that humans may easily remember images more efficiently than text (Dhanake, Korade, Shitole, Kedar, & Lomte, 2014). However, it is obvious that images are usually simpler to be remembered than text. The difference from the possible code space concerning graphical and textual passwords provides level of resistance against text related attacks (Chang, Tsai, & Lin, 2012). Having this in mind, there is a growing involvement of research in graphical code scheme. Besides recognition, centered graphical code authentication method should promote users to consider the use of strong passwords that can easily be recalled or remembered (Ku et al., 2012). This led to the development of brand-new ideas such as graphical passwords (Ragavendra, 2015).

The current graphical password guidelines do not provide learning hints for usability-enhanced features (Catuogno & Galdi, 2014; Chaturvedi & Sharma, 2015; Prasanth, Azarudeen, Kabeer, & Mohamed, 2014). Along with this, Jali, Furnell, and Dowland (2011) highlighted the current gap associated with research on formalizing users' guideline of such schemes, which usually shows the necessity to improve users ability to construct and use graphical password effectively.

Despite this, the existing available methods for constructing password are actually proposed by several researchers to produce unique variations of techniques where each of them has specific requirements for the recognition of structured graphical password. Graphical password can be categorized into three dimensions: (a) cued-

recall, (b) natural recall (c) identification or recognition. This led to the need to consider providing effective Graphical Password Guidelines (GPGs) based on the users' related features.

## **1.2 Problem Statement**

Graphical password techniques have been proposed as a substitution to text-based passwords simply because of the reason that humans may perform better and easily remember images rather than text (Dhanake et al., 2014). The difference in the possible password space between graphical and textual passwords provides resistance against dictionary attacks citing (Suresh, 2014). Due to these characteristics, there is a rising interest in the graphical password schemes. The main problem of this study concerns about the current techniques of graphical password to which it revealed a number of weaknesses and drawbacks in terms of memorability and security related aspects (Sun, Chen, Fang, & Chang, 2012).

As mentioned in literature, among the three categories of graphical password; recognition-based is commonly associated with the task of recognizing pictures (Meng, 2013). These pictures are considered as users' password. Thus, the issue with password selection becomes critical which determines the security of the systems (Olukayode, Ithin, & Ogunnusi, 2014). Others researchers (Sun, Chen, Fang, & Chang, 2012; Yadav & Mohod, 2013; Zangoeei, Mansoori, & Welch, 2012)) acknowledged the need for more efforts to simplify the memorization procedure by linking graphical elements into users' cultural familiarity or context. The actual motivating concept is the use of photographs that relates to the users background due to familiarity aspects will result in greater memorability in addition to decrease the

actual tendency to settle on insecure accounts (Ávila, Menezes, & Braga, 2013), which will subsequently increase total password stability (Kawale & Patil, 2014).

With regards to familiarity aspects, users usually rely on several aspects. Cross-cultural studies in the fields of Information Technology and Computer Science reveal that cultures represent individual background which relates to familiarity aspects (Aljahdali, 2014a; Noiwan, 2006). Studying the impact of cultural differences in creating graphical passwords will lead to a better understanding of the suitable types of pictures used in graphical password authentication. This will increase the level of security and usability of recognition based graphical-password authentication (Biddle, Chiasson, & Van Oorschot, 2012; Sarohi & Khan, 2013).

Another issue was also found in the recognition technique which allows users to predict their password randomly without customising the various features for forming the picture identity. Such practices were found to lead user to select pictures that he or she likes without receiving any specific guidelines (Sarohi & Khan, 2013). It is also time consuming in which users are required to spend long time to browse and create image portfolios necessary for forming their graphical password (Biddle, Chiasson, & Van Oorschot, 2012; Sarohi & Khan, 2013). The above scenario happens due to currently there is lack of guidelines focusing on recognition-based passwords specifically and graphical passwords generally. Unlike traditional text-based passwords, proper guidelines are prompt to users during the process of passwords construction (Aljahdali & Poet, 2014a, 2014b).

Therefore, this study aims to improve the security and usability of recognition-based graphical passwords by further investigating the influence of cultural familiarity in their password selections. This study also intends to propose a guideline for

recognition-based graphical password that could be used to assist users during password construction process.

### **1.3 Research Questions**

This research is conducted in order to answer the following research questions identified from the current research background and problem on the needs for an effective GP among users:

- 1) What are the pictures that the people will choose to reflect their culture?
- 2) What is the relationship between the choices of passwords and the cultural familiarity?
- 3) What is the effect of password choice that can affect security and usability?
- 4) What are the possible guidelines for the recognition-based graphical password?

### **1.4 Research Objectives**

This research concerns about achieving the following objectives:

- 1) To collect pictures that the people will choose to reflect their culture.
- 2) To investigate the relationship between the choices of password and the cultural familiarity.
- 3) To analyze the effect of password choice that can affect security and usability.
- 4) To suggest possible guidelines for the recognition-based graphical password to improve its security and usability.

## **1.5 Significance of the Study**

This research would provide several advantages associated with enhancing users' memorization and recognition of password elements using graphical password. This study can also provide an effective mechanism for organizing graphical elements that fall within users' preferences. Also, it focuses on providing necessary supports for implementation and improving the usability effectiveness for users through providing guidelines for both user and developer. In addition, for studying the cultural effects on different kinds of recognition-based graphical password techniques, it is suggested to discover the suitable method to improve the existing graphical-password techniques so as to make them more secure and practical.

It can also serve as a reference for future studies in which considering aspects related to human racial can add new insights to the field of computer security from the perspective of Human-Compute Interaction (HCI).

## **1.6 Scope of the Study**

With the current authentication and recognition procedures, it becomes difficult for users to recall lengthy passwords and provide necessary interactive hints to remember it (Gao, Haichang, et al.2008). As such, the researcher in the present study is mainly concern about featuring this study in the Malaysian context as a way for building effective graphical passwords according to their culture. This is because most Asian people share relevant practices among them (Luvaas, 2013). Thereby, the effect of cultural on creating graphical password has been investigated on UUM post/undergraduate students. This study was broadly included students in UUM. The educating guessing attacks and usability related aspects in terms of ease of use, login

time, memorability, satisfaction, etc., would be covered and investigated in this study.

## **1.7 Overview of the Thesis**

The main structure of this thesis is divided into three main parts: background, data collection and analysis, and conclusion and future work. The background consists of two main sections, the first of which reviews Graphical Password (GP) techniques and provides information about usability with security attacks (Chapter 2) and the second of which discuss the research method that involves in this thesis (Chapter 3).

The data collection and analysis is presented in Chapters (3 and 4). Chapter 4 presents the culturally-familiar picture database that is the basis of this thesis. Chapter (4) also presents the effect of cultural familiarity on users' choice of GP pictures.

The effect of cultural familiarity on the usability of GPs is presented in (Chapter 5), while the effect of educated guessing attacks when using GP pictures that are either culturally familiar or unfamiliar at the same chapter. The suggest guidelines to overcome the weakness that appear through the previous chapter are discuss in the same chapter.

The conclusion is presented in Chapter 6, discussing the main results of the thesis and recommendations for future work in RBGP authentication. Figure 1.1 shows the general structure of the thesis.

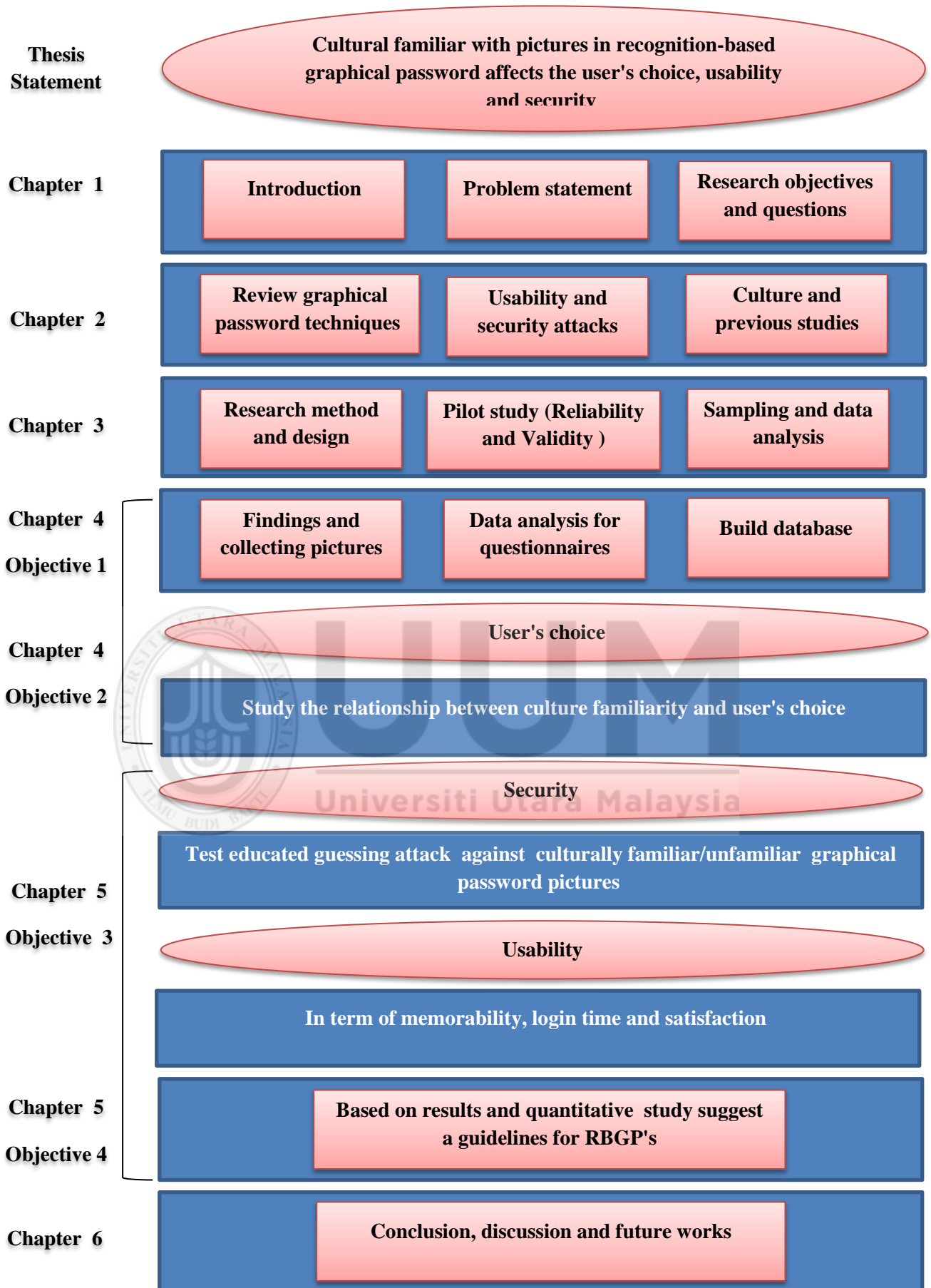


Figure 1.1: General structure of the thesis



## CHAPTER TWO

### LITERATURE REVIEW

#### 2.1 Authentication Methods

With the recent spectacular growth of Ecommerce, the need for the highest-security environment possible on the Internet has become nothing less than urgent. Any such environment requires some sort of user authentication protocols. Monroe and Reiter (2005) state that the purpose of user authentication is to “confirm the claimed identity of a human user”. In other words, user authentication is a manner of identifying users who want to login to a system by questioning him or her for some piece or pieces of information to prove their identity.

Authentication methods are divided into three main categories, i.e., token-based, knowledge-based, and biometric authentication (Suo et al., 2005). Table (2.1) summarizes those methods along with their advantages and disadvantages.

Table 2.1: Summary of Authentication methods (Suo et al., 2005)

	Knowledge-based	Token-based	Biometric
<b>Method</b>	<ul style="list-style-type: none"> <li>➤ It requires information to prove user's identity.</li> <li>➤ This information is in two forms: text-based form or graphical-based.</li> </ul>	<ul style="list-style-type: none"> <li>➤ It requires official identifications (passport, bank card, etc.)</li> <li>➤ Usually, it is used in combination with knowledge-based authentication</li> </ul>	<ul style="list-style-type: none"> <li>➤ It requires the physiological or behavioral information of users.</li> <li>➤ This information include fingerprints, voice, ear shape, etc.</li> </ul>
<b>Advantages</b>	<ul style="list-style-type: none"> <li>➤ Most commonly used.</li> <li>➤ Easy to apply and use.</li> </ul>	<ul style="list-style-type: none"> <li>➤ High level of security.</li> <li>➤ Two-factor</li> </ul>	<ul style="list-style-type: none"> <li>➤ Suitable for places such as airports or courts.</li> <li>➤ Their cost continues to</li> </ul>

	authentication.	drop.
<b>Disadvantages</b>	<ul style="list-style-type: none"> <li>➤ It is quite difficult to remember more than one complex alphanumeric password.</li> <li>➤ This difficulty led many users to create simple password or to write it down or to use the same one several times.</li> </ul>	<ul style="list-style-type: none"> <li>➤ It is hard to use for some internet applications.</li> <li>➤ Risk of losing the bank card, passport, etc.</li> <li>➤ It brings privacy concerns for users.</li> <li>➤ Biometric readers should be highly accurate to avoid authentication delay.</li> </ul>

---

The mechanism of Token-based authentication is done by inquiring from the users for the material objects, for example, bank cards or passports and other forms of official identification. Typically, token-based authentication is employed in combination with knowledge-based authentication to confirm that the ownership is legitimate.

Biometric-based authentication utilizes the physiological or behavioral information of users with the intention of recognizing them (Johnson, 2004). This physiological or behavioral information might include the voice, face, fingerprints, ear shape, etc. Detailed information about how biological information is used in authentication is given in Jain et al. (2006).

The knowledge-based method is the most commonly used technique for authentication (sou et al., 2005). This technique includes the text-based (alphanumeric password) and graphical-based authentications, the latter of which may be split into two sub categories, i.e., recognition-based and recall-based authentications. In recognition-based authentication, the user looks through sets of pictures and then has to recognize the particular picture that he/she selected or made

at the registration stage. Under recall-based authentication, the users are requested to redraw an image, most commonly a signature that he/she has created at the registration process so that to access the system in question. (Suo et al., 2005) Even though most companies exercise text-based authentication, it has many limitations as compared to the graphical-based authentication. Therefore, the research community has started concentration on graphical-based authentication so that to overcome the weaknesses of text-based authentication and make the authentication process more useful while still secure. Since the last two decades, several graphical-based authentication techniques have been proposed and implemented.

According to Monroe and Reiter (2005) and Biddle et al. (2012), graphical-based authentication systems can be divided into three major parts: recognition-based (picture identification); recall-based (drawing); and cued-recall (clicking or picture interpretation).

## **2.2 Knowledge Based**

### **2.2.1 Traditional Text-Based Passwords**

A traditional text-based password is a password which consists of any combination of characters from the ASCII set. These passwords are also referred to as ‘alphanumeric passwords’ or ‘text passwords’. Text passwords remain the most widely used authentication mechanism, instead of the huge amount of available options for several reasons reported in Herley et al. (2009).

They are also inexpensive as well as easy to implement, and most users are familiar with them. Users can select text passwords that do not contain any personal information to authenticate themselves without violating their privacy. Lately, network and computer security has become a formidable technical challenge. One of

the main areas in the research of security is authentication, which determines if users would be allowed to access a particular resource or system. Accordingly, it is common to use a password as an authentication tool even till date, however, at present it is not a very reliable security approach. Studies at present reveal that the key challenges of using passwords are the remembering difficulty and users often use simple passwords that they can recall easily; however, these passwords are often predictable and risky. On the contrary, having a complicated password would mean that it would be difficult to recall (Haichang et al. 2010; Touraj, 2015).

### **2.2.2 Graphical-Based Passwords**

To be able to improve the limitations regarding traditional text-based authentication, graphical passwords methods happen to be proposed as an alternative to text-based passwords based on the psychology reports (e.g., (Biddle et al., 2012; Ploehn & Greene, 2015; Wright, Patrick, & Biddle, 2012) that mental faculties is much better at thinking about how and recognizing images as compared to text (e.g., digital strings). An assumption is established means of reducing one's need to memorize lengthy password, users may produce better passwords via using graphics (e.g., offering much larger password space) as compared to text-based code schemes (Almuairfi, Veeraraghavan, & Chilamkurti, 2013). Normally, graphical password schemes are classified into the following:

- i. Cued recall-based graphic password (clicking)
- ii. Pure recall-based graphic password (drawing)
- iii. Recognition-based graphic password (recognizing)

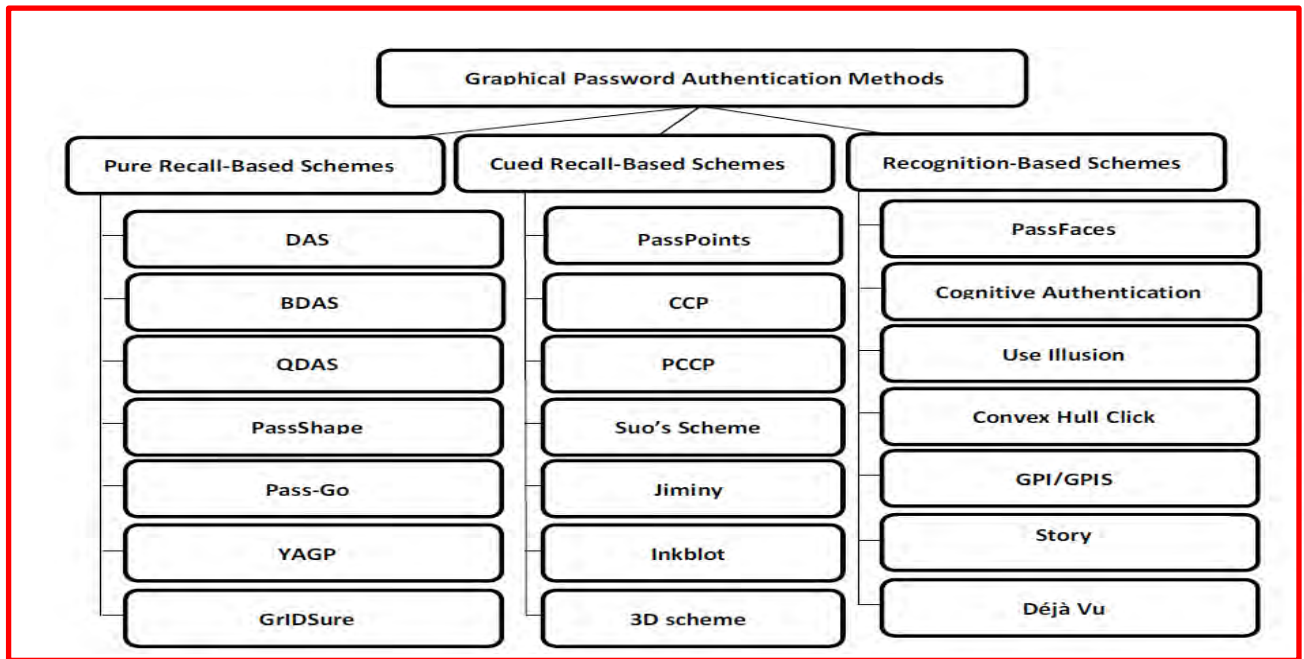


Figure 2.1 : Classification of the Existing Graphical Passwords (Almuairfi, Veeraraghavan, & Chilamkurti, 2013)

### 2.2.2.1 Cued Recall-Based Graphic Password

With the authentication, the Cued recall -based system asks end participants to click on the available images (for example, selecting the things in an image), Weidenbeck, Waters, Birget, Brodskiy, and Memon (2005) highlighted the current issues associated with the use of graphical password as an alternative for current practices in which user needs to click constantly on images rather than typing alphanumeric characters. The authors proposed what they claimed to be a secure graphical password system terms as PassPoints. The working mechanism of this password relied on the use of security characteristics. They also conducted an empirical study to compare the PassPoints to alphanumeric passwords. During the users' practice of the technique, authors noticed that the learnability of users increased with the use of a combination of text and graphical elements over a period of five weeks. The obtained result showed that users assigned under the graphical group spent more time and got errors in learning the password, but that the difference was largely an effect

of just a few graphical participants who had trouble to learn the usage of graphical passwords, as shown in Figure (2.2) one of the used interfaces.

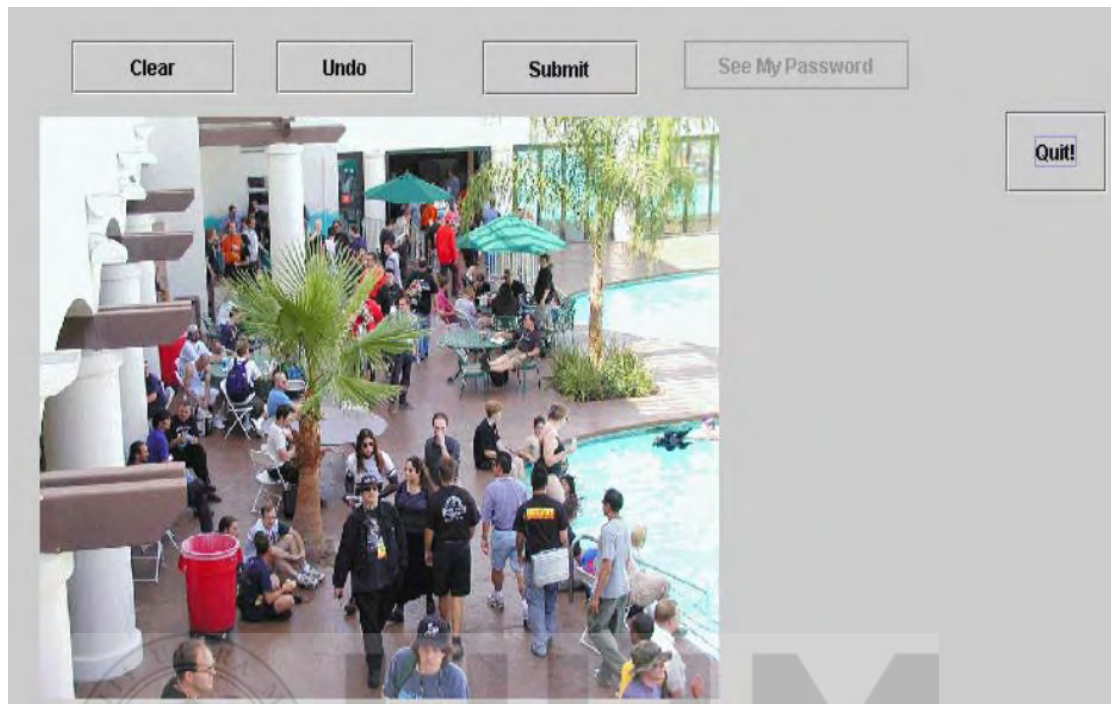


Figure 2.2 : Graphical Password Interface Used in Experiment (Weidenbeck et al., 2005)

#### 2.2.2.2 Pure Recall-Based Graphic Password

This kind of procedure is also known as a drawmetric system (De Angeli et al., 2005). The recall-based method works by asking the user to draw a figure as a GP during the enrolment stage. Thorpe and Van Oorschot (2004) have examined the key determinants for identifying the relationship between the number of grid dimensions, composite strokes, and password length in the DAS password space, as shown in Figure (2.3). The mechanism consists of the usage of a large part from DAS password space based on guessing user preferences while constructing a long password with numerous composite strokes. In the event that user decides to construct a password of 4 or fewer strokes, with passwords of length 12 or less on a  $5 \times 5$  grid, then the size associated with the DAS password is alternatively condensed

to smaller size. Moreover, the authors found analogous decrease when users chose no strokes of length 1. This led Authors to propose a novel scheme in order to help system use additional spaces for containing the password strokes to 16 bits of security. The proposed mechanism found to provide a good variant of size and complexity as compared to other techniques.

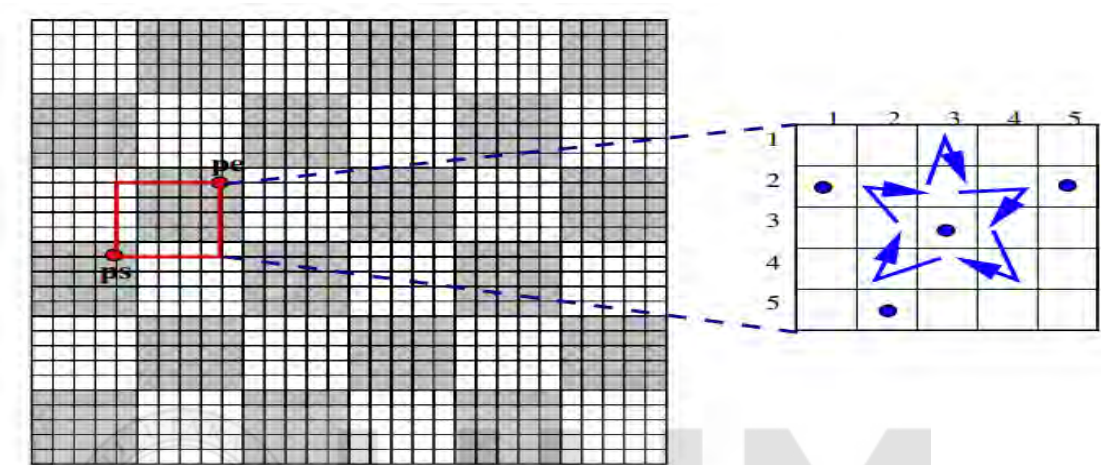


Figure 2.3 : Grid Selection: A User Selects a Drawing Grid in Which to Draw their Password (Thorpe and Van Oorschot, 2004)

### 2.2.2.3 Recognition-Based Graphical Passwords (RBGSs)

Recognition-based systems also called cognometric or searchmertic systems require the users to memorize a portfolio of images at the time of password creation and should be able identify them (their previously seen images) from among decoys to be authenticated (Biddle, 2012). At the time of registration for a recognition-based graphical password (RBGP) method, the customer is offered with a group of images from which he/she selects a number of pass-images to be used for authentication. On the other hand, they will upload their own images. At the time of authentication (when the username is provided) the user is presented with a set of screens that include a grid of images. Each screen consists of at least one pass-image and a number of alternative nonpassimages called distractors. The customer should select

their pass-image from the screen, repeating the method for each of the challenge screen. After successfully selecting the customer's pass-image from each screen, he/she is authenticated.

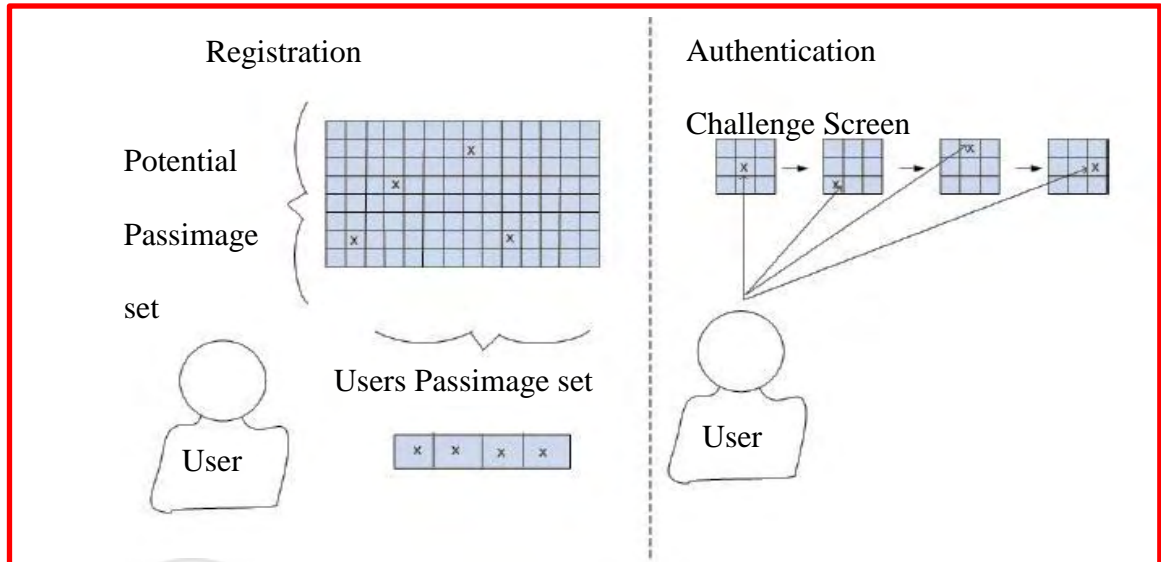


Figure 2.4 : Registration Stage for a Recognition-Based Graphical Password (English, 2012)

This process is demonstrated in Figure( 2.4) above, where in the registration process, a user selecting a subset of the potential pass-images to be their pass-image set is depicted. In the authentication process, the user is provided with a number of challenge screens having one pass-image on each screen. The user selects the correct pass-images to authenticate successfully (English, 2012).

### 2.3 Existing Studies on Graphical Password

Computer security has traditionally devoted to low-level, technological design as well as implementation facts. Security specialists often refer to humans because weakest link within the security cycle, asserting the problem falls not with the security techniques themselves, but having users who are unable as well as unwilling to stick to security protocols. This strategy of distancing system design from



individual behaviour is actually doomed to be able to fail as it ignores the current platform during which security techniques are inevitably used (Chang et al., 2012).

The adjust towards useful security as well as including people factors during system design can be an important one which a direct impact on the security from the system can be achieved. When users misunderstand the best way to use certain security measures mechanisms, circumvent them since they are too obtrusive, or do not even realize the need for this sort of systems, then the particular systems usually are far very likely to provide a reliable security measures regardless of the systems technological needs. Users are always encountering security threats daily, such since physical keys to unlock their account as well as security alarms intended to alert them of threats. With respect to computer security issues, people are generally required to be able to authenticate independently using knowledge-based schemes including passwords.

Because the name suggests, image-based techniques use images, including image graphics, unnatural pictures, or other sort of images as background. This includes showing a number of images in order to build one's access style to the account. As such, graphical password is divided into two sub-classes: single-image techniques and multiple-image techniques. The latter is additionally called a new recognition-based scheme in the previous studies.

Single-image structured schemes use one single image as being a background, and requires from user to repeat many actions through an input product, such since clicking or dragging, in a similar as in the registration period.

Tao (2006) proposed the design of Go-pass as a security solution which enables online users to configure their own graphical password by navigating through an

image, as illustrated in Figure (2.5). The process stated with allowing user to choose a number of images that are associated with his/her preferences. For example, user can choose food, furniture, placement, etc., in a kitchen environment. Other similar settings include dialing a phone number, preparing a meal by selecting and cooking ingredients, and choosing a hand of cards. The author also noted a potential issue in the security of the proposed method, which falls into the length of full password. In addition, a password set by users in short manner can be easily obtained by several tries.

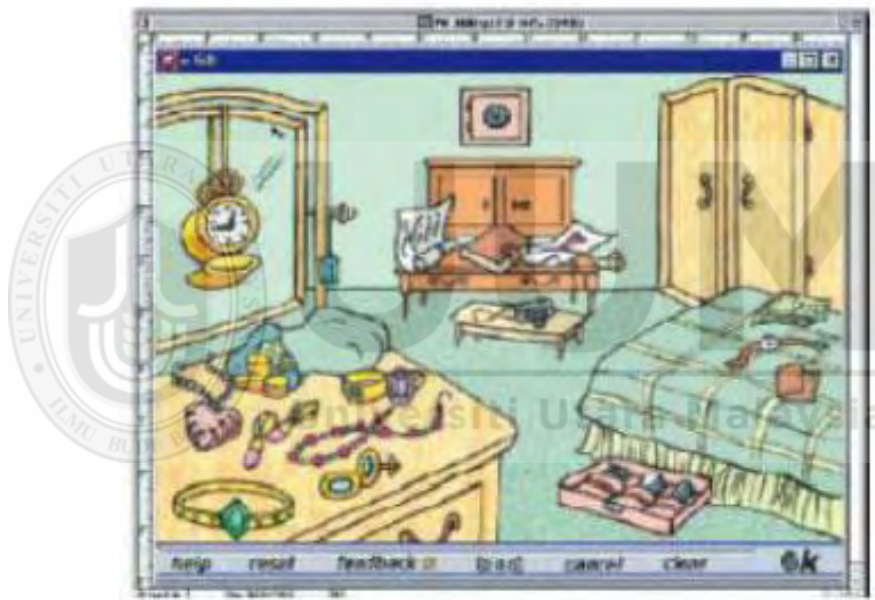


Figure 2.5 : GO-pass (Tao 2006)

Other studies like in Wiedenbeck, Waters, Birget, Brodskiy, and Memon (2005) addressed how computer security authenticates practices to offer a suitable security measures. They emphasized on the current problems related to getting users remembering passwords over time, i.e. a password that is long and random. Such problem leads most online users to prefer using short and insecure passwords. Hence, they offered the use of graphical passwords as a way to help users memorize images rather than typing alphanumeric strings. The authors proposed PassPoints as a secure

graphical password system. It enables users to form their own alphanumeric or graphical password. The result of using such mechanism proved to provide a valid password with fewer difficulties than the alphanumeric users.

Syukri, Okamoto, and Mambo (1998) have addressed the needs for providing a reliable user identification system using mouse, this as a result led them to identify users using a complex figure object, signature as a way for ensuring one's identity as shown in Figure (2.6). They followed the following steps: the normalization of input data, the adoption of new signature writing-parameters, the evaluation of verification data using geometric average means and the dynamical update of database. Then, they utilized the proposed system on number of users for usability related verifications in which the system achieved a rate of 93%.

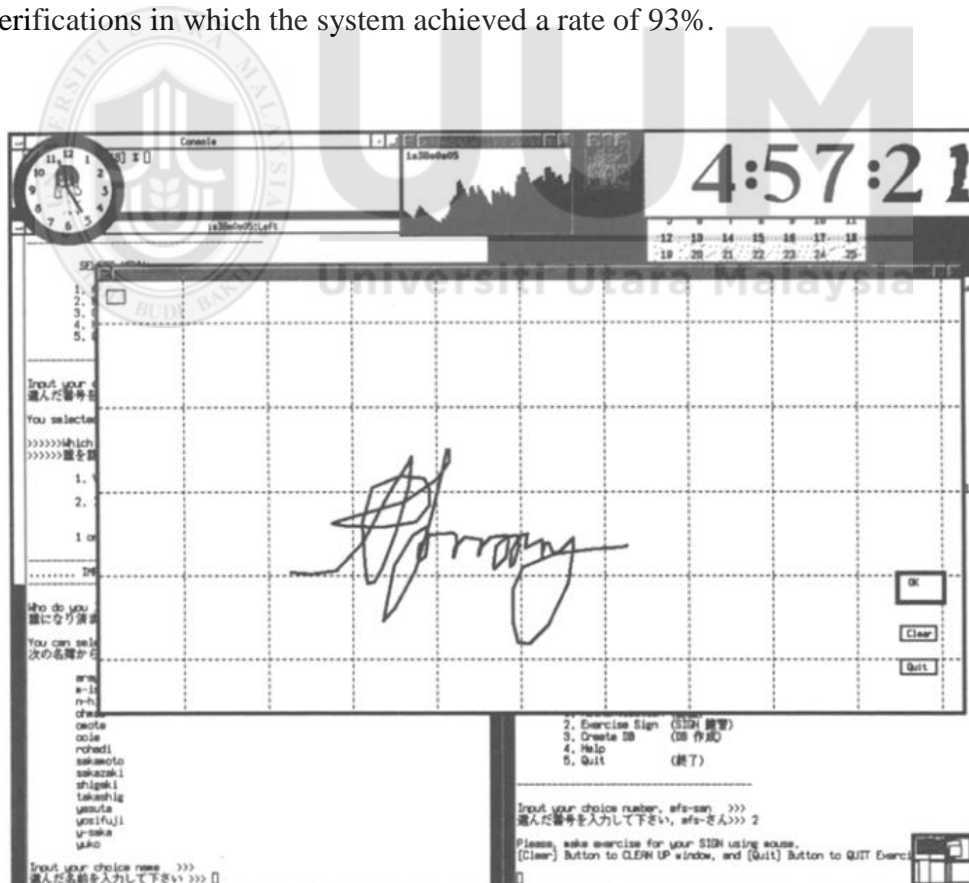


Figure 2.6 : User identification system (Syukri, Okamoto, and Mambo, 1998)

Jermyn, Mayer, Monroe, Reiter, and Rubin (1999) proposed graphical password mechanism for exploiting features of graphical input displays to achieve better security than textbased passwords. The main idea driven by the scholars was favoured by using small size graphical input devices for the aim of allowing user to decouple the position of inputs from the temporal order in which those inputs occur to generate password schemes with substantially larger (memorable) password spaces. They evaluated the suitability of the proposed system shown in Figure (2.7) by capturing a subset of the “memorable” passwords on personal digital assistants (PDAs).

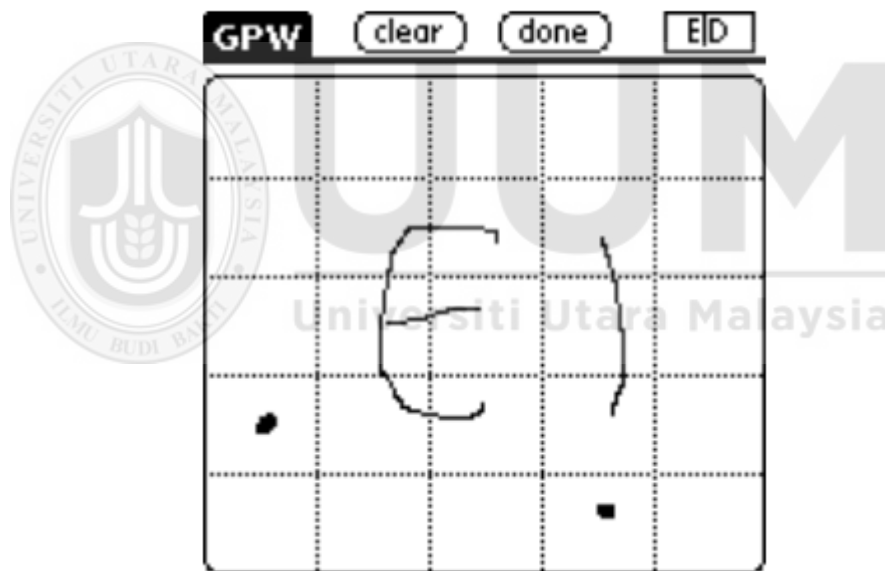


Figure 2.7 : Graphical input displays (Jermyn, Mayer, Monroe, Reiter, and Rubin, 1999)

In multiple-image schemes, on the other hand, multiple images are presented and a user is required to recognize and identify one or more of them, which are previously seen and selected by the user.

Inkblot authentication method proposed by Stubblefield and Simon (2004) takes advantage of the images as a cue for text password entry. During password formation, users are given the chance to select a series of inkblots and to type in the first and last letter of the word/phrase that best describes the inkblot. The authors assume that users after certain period of time can memorize their password and would no longer need to rely on the inkblots as cues as shown in Figure (2.8). The authors assert that inkblot is an effective way to prevent online authentication attacks.



Figure 2.8 : Inkblot example (Stubblefield and Simon, 2004)

Jansen (2004) conducted his study for the aim of providing a simple PIN or password mechanisms and periodically enable users updating their authentication information for authenticating purposes image selection. The author derived his method as a sequence of recalling images that indicates an easy and natural which believed to help reduce the barrier to users' compliance with corporate policy as shown in Figure (2.9). The approach described distinguishes itself from other attempts in this area in

several ways, including style dependent image selection, password reuse, and embedded salting, which collectively overcome a number of problems in employing knowledge-based authentication on mobile devices.

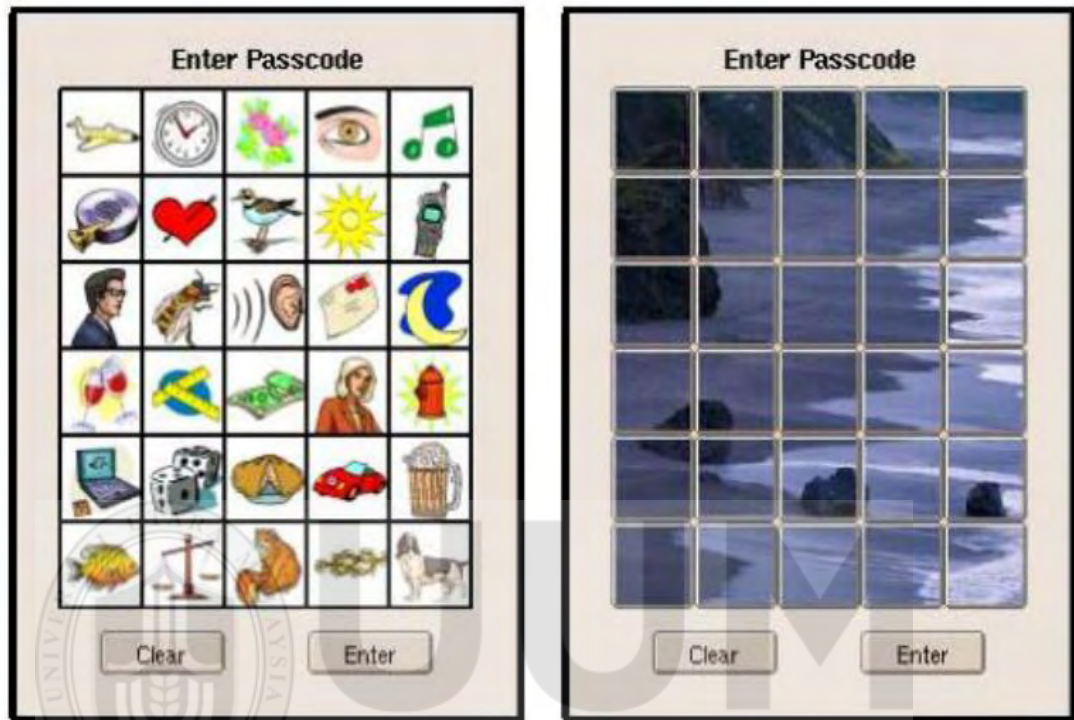


Figure 2.9 : Image recall example (Jansen, 2004)

Eljetlawi (2008) proposed a graphical password system framework for simplifying the current recall experience of graphical passwords. The author relied on new user and existing user stage, in which such consumption was developed into prototype and an evaluation of the prototype usability features has been conducted by questionnaire survey in the UTM (CASE) and Computer Science Faculty students (Johor). The evaluation result showed that the proposed system in Figure (2.10) carries the potential in offering an easy to remember mechanism.





Figure 2.10 : Graphical password system framework (Eljetlawi, 2008)

Aljahdali and Poet (2014c) proposed a graphical password scheme using culturally related pictures based on the result obtained from the interviews conducted with the users of graphical passwords. The comments and feedback obtained from the interviews were used in order to form a certain pictures for their graphical passwords. The system consists of processing successful or failed authentication, main properties of security of graphical passwords, and their general impressions about using graphical passwords instead of alphanumeric ones. Figure (2.11) shows the graphical password proposed by the author for Middle East region.



Figure 2.11 : A graphical password scheme using culturally related pictures

(Aljahdali and Poet, 2014c)

Chang et al. (2012) proposed a new graphical-based password system for touch screen handheld mobile devices. The graphical password enlarges the password space size and promotes the utility in touch screen handheld mobile devices as shown in Figure (2.12).



Figure 2.12 : The human-computer interface for a user to enter his or her graphical password (Chang et al., 2012)



Table (2.2) shows the similarity and differences between different techniques applied in previous studies on graphical password. It can be summated that each study tried to ensure providing a simple and easy to remember graphical password mechanism that could appeal to users' needs. There also a number of weaknesses can be spotted in terms of lack of studies on cultural properties in favouring users' cognitive to create password.



Table 2.2 : Comparison of different graphical password mechanisms in previous studies

	Study	Objective	Technique	Inputs	Device	Weakness
1	Tao (2006)	Enables online users to configure their own graphical password	Allowing users to navigate and select graphical elements through an image	User can choose food, furniture, placement, etc., in a kitchen environment. Other similar settings include dialing a phone number, preparing a meal by selecting and cooking ingredients, and choosing a hand of cards	PC	Textual verification is not considered.
2	Wiedenbeck et al. (2005)	Offer a suitable security measures based on the use of computer security authenticates	Enable user selecting number of places associated with users' characteristics or preferences.	Free selection	PC	There is no indication about the selected places which may lead to invalid verification.
3	Syukri et al. (1998)	Identify users using a complex figure object, signature using geometric average means and the dynamical update of database	Provide a reliable user identification system using mouse	Signature writing- parameters	PC	Possibility of knowing users' signature without security password can simplify accessing their account by others.

4	Jermyn et al. (1999)	Exploit features of graphical input displays to achieve better security than textbased passwords	Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur	Exploit features of graphical input displays	Mobile	Outsiders may access users' account upon a number of trials.
5	Stubblefield and Simon (2004)	Provide an effective way to prevent online authentication attacks	Select a series of inkblots and to type in the first and last letter of the word/phrase that best describes the inkblot.	Inkblots	PC	Users may forget the selected color or shapes.
6	Jansen (2004)	Motivating users to enable simple password mechanisms update	Style dependent image selection, password reuse, and embedded salting.	Image selection	Mobile	Number of selections is limited to certain event.
7	Eljetlawi (2008)	Provide an effective graphical password system framework	Indicate images that are mostly preferred by the user.	Image selection	PC	Number of selections is limited to certain event.
8	Aljahdali and Poet (2014c)	Increase memorability and to facilitate user authentication	Select a number of graphical elements with culturally related nature	Culture related pictures	PC	Lacking of using text ID for each cultural picture.
9	Chang et al. (2012)	Provide an effective graphical password touch screen handheld mobile devices	Keystroke Dynamic-based Authentication (KDA)	Select image 3 times	Mobile	Limited selection of images.

## **2.4 Security of Graphical Password**

The below subsections will cover a broad study concerning the possible attacks on Recognition-based graphical password schemes which was carried out where by the attacks have been identified and fixed on the basis of Common Attack Pattern Enumeration and Classification (CAPEC). The subsections also include the 3 features of a passwords security, which are observability describes an attacker's ability to observe the GP when a user selects it, recordability describes the user's ability or requirement to record the GP, which makes it easier for an attacker to find it" and guessability describes an attacker's ability to guess a user's GP without physical Access" (De Angeli et al., 2005):. Possible attacks are mapped according to the Recognition-based methods found in Table (3) These attacks consist of 6 different types, i.e., spyware, guessing, brute force, dictionary, social engineering, and shoulder-surfing, and they are the currently active forms of attacks in the Recognition-based techniques (Touraj, 2105).

### **2.4.1 Guessing Attack**

In this case the user usually selects his/her password based on some particular data, for example pet name, passport number, family name etc..; the hacker will attempt to guess the password by simply guessing and ruling out the possible password (Arash, 2011). Attacks in this method are generally divided into online password and offline dictionary guessing attacks. In the latter, the attacker searches for the password by managing the inputs through one or more oracles. In contrast, for the online password guessing attack the hacker tries to use a preexisting guessed password by managing the inputs of one or more oracles. Nonetheless, a graphical password may be guessed just as easily as a textual one. For instance, research on the Pass-face

scheme shows that the user is most likely to select an expected and weak graphical password (Arash, 2011 & English, 2012).

#### **2.4.2 Dictionary Attack**

This method is done by attempting to guess the password space using passwords most likely to be selected by the user. By narrowing the amount of predictable guesses it may highly improve the success rate compared to an extensive attack. Dictionary threats may also be fruitful when registered entries are preliminarily used to test the most likely passwords. In this case, graphical-passwords are less susceptible compared to textual passwords because they use a mouse input instead of a keyboard input. Among other current schemes only the Pass-face scheme is not immune to this type of attack.

#### **2.4.3 Brute Force (Exhaustive) Attack**

Exhaustive threats are carried out in a manner similar to the previous one, however every probable password option is created and used for attacking the authentic password. In higher looped threats, priority is given to these types of possibilities in order to decrease the chances of being selected by the users if all the possibilities might be guessed (Towhidi, 2013). This type of attack may be performed both online and offline just like a dictionary threat. The advantage of an exhaustive threat is that there is enough time and computing power to find a match (unless the online threat is identified and terminated before the list is able to expand). However, huge password spaces are not ideal in guessing the password within the whole space. These types of in-depth attacks provide high coverage but require more time or processing power, which is the opposite of a dictionary threat.

The main tool of defense in a brute-force search is to use a huge enough password taking up a lot of space. Textual password has a space of  $94^N$ , where  $N$  is the length of password and 94 is the printable number of characters not including the space. Various graphical-password techniques utilize this same principle or may be even longer. Graphical-password, which is recognition-based, is possible to include a smaller password space compared to the recall-based systems. Attacking a graphical-password by brute-force is much harder compared to that of a textual-password. Attack software is required in order to generate an automatically precise mouse motion to mirror the human inputs, which is rather difficult for the recall-based graphical-password.

#### **2.4.4 Spyware Attack**

In this particular type of attack, software is installed primarily on the users' computer and complex information is recorded. This malware helps to film the movement of every key and mouse then the information is recorded without the users' knowledge and is then sent back outside of the computer. Simply using key logging or key listening spyware may not be efficient enough to crack graphical-passwords since it is not tested if the mouse spyware is effective enough, except for a few cases (Suo, 2006; Towhidi, 2013). Mouse tracking although successfully saved is still inefficient in locating and cracking the graphical password. Additional information is still required in order to accomplish this type of threat, for example, position and size of window, instead of information timing.

#### **2.4.5 Shoulder Surfing Attack**

Here, the attacker will use direct observation or external recording through video cameras as the real user calculates the information in order to gain information of the users' credentials. Shoulder surfing is made possible thanks to the availability of high resolution cameras with scrutiny tools and telephoto lenses which is a key threat if the hacker is targeting the user and knows where the user is located. This is mainly invasive in a public environment but is a more serious threat in a private setting. Both graphical-passwords as well as textual-passwords are susceptible to the shoulder surfing threat. Numerous recognition-based methods are available that are designed for tackling the problem of shoulder-surfing. None of the Recall-based schemes can be considered as resistant to shoulder-surfing (Touraj, 2015).

#### **2.4.6 Social Engineering Attack**

This type of threat includes any scheme that is used to fool a person into revealing their personal data or IDs to unreliable people. Phishing is an example of social engineering used in websites and email, but it may also be carried out via other methods such as “fake phone calls” claiming to be from the unsuspecting users' banks, credit card company, or technical supports. It is so much easier to acquire a password or ID from a sincere user rather than trying to hack into a secured system. In this method it is harder for a user to reveal a graphical password to someone else as opposed to a textual one. For instance, it is virtually impossible for a user to expose a graphical password through a telephone call.

Developing a phishing website just to obtain a graphical-password is ore time consuming (Sarohi, 2013 & Lashkari, 2011).

## 2.5 Usability of Graphical Passwords

Beyond the security of the GP, it must feature user authentication that can be used without significant problems. Usability has been described as the “extent to which a product can be used by specified users to achieve particular goals with effectiveness, efficiency and satisfaction in a specific context of use” (Frøkjær et al., 2000). In the case of GPs, usability measures the effectiveness, efficiency, and user satisfaction when using the GP:

- i. ***Effectiveness***: It measures the exactness and accuracy in which user achieves particular goals. Examples of indicators used to evaluate the effectiveness are error rate and memorability (Frøkjær et al., 2000; Van Welie et al., 1999). As will be shown in the next section, the memorability factor is commonly used to measure the effectiveness of the GP (Biddle et al., 2012). The memorability factor is based on the number of GPs that were remembered and the number of GPs that were incorrectly entered (De Angeli et al., 2005).
- ii. ***Efficiency*** calculates the resources consumed concerning the completeness and accuracy in which the user achieves their goals. Factors such as task learning time and completion time are examples of efficiency indicators (Frøkjær et al., 2000). In the GP context, task completion time should be based on both enrolment-time and authentication-time. Enrolment-time is that time which is needed to create or reset a GP, while the authentication time is the one needed to login successfully using the GP chosen (Wiedenbeck et al., 2005; Renaud and Angeli, 2004). In most studies, however, the authentication time is the only factor used for measuring the efficiency of GPs (Biddle et al., 2012; Dunphy et al., 2008; Weinshall, 2006; De Angeli et al., 2005).



- iii. **Satisfaction** measures both freedoms from distress and optimistic approaches towards the usage of product. User satisfaction can be evaluated using a usability questionnaire at the end of the task. Examples of those questionnaires are the System Usability Scale (SUS) (Brooke, 1996)

## 2.6 Current Utilization of Graphical Passwords

Graphical password potentially might be a well alternative to the standard textual password. Many previous studies stated that images could be memorized as compared to the current practices for using characters and numbers (Gasti & Rasmussen, 2012). Furthermore, images tend to be basically much better for recognition or memorizing instead of words. Additionally, the volume of remembering possible photographs and number of images is actually not well configured. This can compress on the relationship between graphical and textual nature, which are poorly identified in a given context (Duggan, Johnson, & Grawemeyer, 2012). Thus, it helps make better security as a way to variety items instead of words in addition to number inside alphanumeric password schemes. Difficulty of remembering a new textual password is an established problem (Pandey, Motwani, Nayyar, & Bakhtiani, 2013). There tend to be some principles users need to follow to make a solid password, which make it difficult to recall:

- i. The selected password must have at very least 8 figures contains alphanumeric figures.
- ii. Shouldn't be linked to one's personal information.
- iii. Shouldn't be easy to locate by outsiders using simple dictionary or the general public one.

- iv. Need to compress of upper and also lower scenario letters, a minimum of one upper then one lower and may have a minimum of one digit.

Davis, Monroe, and Reiter (2004) asserted that using graphical password can help users with low cognitive abilities to memorize their passwords without a need to recall numerical or textual elements. As such, graphical password has been applied in different domains, such as commerce, healthcare, learning, etc. Khan, Aalsalem, and Xiang (2011) proposed a graphical password for use in smart mobile devices (like smart phones i.e. ipod, iphone, PDAs etc) which are more handy and convenient to use than traditional desktop computer systems. They highlighted the essential role of graphical password in promoting users access through mobile devices. The same was shared by Chang et al., (2012) who also emphasized about the needs for providing a reliable graphical password mechanism on mobile devices. On the other hand, previous researchers mentioned earlier in Table 3 addressed the needs for more effective graphical password to be utilized in a certain environmental conditions associated with users' demographic background. Therefore, this study is conducted in order to propose an alternative graphical password based on cultural related picture along with the use of textual hints for a certain regions.

## **2.7 Types of Pictures Used for Recognition-Based Graphical Passwords**

Recognition-based “Graphical password frameworks” utilize distinctive sorts of pictures as the basis for the “graphical password”. Cases of the photos utilized as “graphical passwords” are close to home pictures referring to Tullis (2005), pictures of ordinary articles referring to Cranor (2005), abstracts referring to Perrig (2000), faces referring to Brostoff (2000), doodles referring to Poet (2009), and Mikons Renaud referring to (2009). Users' works have been led to look at the ease of use

between these sorts of pictures. As per Renaud (2009) directed a longitudinal research to look at the proficiency of three sorts of “graphical password pictures”; Doodle, Random pictures of ordinary items, and individual pictures provided by the users. The outcomes demonstrated the predominance of doodles over both the photos of ordinary articles and the individual pictures. Doodles were essentially more vital than individual and arbitrary pictures. Additionally, individual pictures were marginally more paramount than arbitrary pictures.

The execution favorable position of doodles in the momentousness might have downsides in other ease of use issues, for example, enrollment and login time. For the individual pictures, it appears that users did not try to transfer individual pictures to be utilized as “graphical passwords”. Users should be prompted obviously to give appropriate pictures that have solid connection to them. Results produced by Renaud (2009) demonstrate that 31% of the individual pictures were landscape pictures that were less significant than pictures that portray certain items. For the arbitrary pictures, Renaud (2009), contended that they were less huge in light of the fact that the users had no immediate association with them. As such, the users had no contribution in the creation of the arbitrary pictures. This legitimization may experience the ill effects of the way that there are numerous well known pictures that have solid association with users despite the fact that these were not brought with their respective cameras. Another research work directed by Tullis and Tedesco (2005) look at the ease of use of individual pictures that have been transferred by users (not really brought with their own cameras) and stock pictures (irregular pictures). The outcomes demonstrated better impressiveness execution of the individual pictures over the arbitrary pictures. The contrast between the investigation of Tullis and Tedesco (2005) and Renaud (2009) is such as the users in Tullis and

Tedesco's research have further adaptability to transfer pictures whether taken without anyone else or by another person. Hence, the users in Tullis and Tedesco's (2005) study had more assortments of individual pictures than those in the work of Renaud. This adaptability may be one of the components that brought on the execution benefit for individual pictures to be utilized as “graphical passwords”. Following six years, 12 of 13 members effectively recollected their “graphical passwords” (Thomas, 2011).

Monrose and Reiter (2005) contemplated the momentousness of two “recognition-based graphical password” methods, Story technique (utilizing pictures of ordinary objects) and Face technique (utilizing faces). The outcome demonstrated that the Face system is more paramount than the "Story" technique. The creators' legitimization was that a large portion of the users don't create stories from their “graphical passwords” in order to recall the arrangement of their passwords. It is obvious from the exhibited result that from 236 fizzled endeavors in the "Story" technique, more than 75% of them were precise pictures yet their grouping wasn't right. Another conceivable cause may be the gathering of the photos itself; users may think that it was difficult to choose significant “graphical passwords” since they were new to the accessible accumulation of pictures at the enlistment phase. It was not the circumstance in the Face technique where the outcome demonstrated that the user's grade to select faces from the comparable race for their “graphical passwords” ("race effect"). From the study talked about above, it appears that the arbitrary pictures which are given by the “graphical password” framework are less significant than alternate sorts of pictures. The conceivable motive may be such as the irregular pictures are not ""well known"" to the users/customers which create them difficult to recall (Monrose and Reiter, 2005).

## 2.8 Challenge Set Designs for Recognition-Based Graphical Passwords

Most of the work on the outline of test sets has been centered around the semantic closeness between the graphical passwords and the baits. As indicated by Dunphy, Heiner and Asokan (2010), in graphical passwords, users portray their photos in three ways: (i) semantic sorts (e.g., human photos, scene photos, craftsmanship pictures), (ii) protest piece (e.g., a glass set on a table), (iii) unique semantics (e.g., individuals celebrating, irate man). A few studies have demonstrated that utilizing semantically comparative imitations diminishes the memorability of various graphical password methods, including article and scene photographs Angeli (2005), photos by Dunphy (2010) and (2012), passface Dunphy (2008) and doodles Poet, (2007). The issue with utilizing profoundly comparative pictures for imitations is that individuals can be befuddled between their graphical secret word pictures and the fakes. A similar issue happens on account of discovering recognizable fakes that may be chosen by the users on the off chance that they saw them at the enrollment phase. Giving a test set natural imitations additionally befuddles users about which pictures they chose already amid enlistment.

Now with standing semantic comparability, the impact of the race, engaging quality and gender of the individual in the photo may impact the outline of the test sets for pictures of appearances. In spite of the fact that they didn't allude to the test set outline, Davis, Monroe and Reiter (2004), found that race, allure and gender orientation all influence users' decision of a graphical password utilizing pictures of appearances. These elements may influence the convenience and security of a graphical password utilizing pictures of appearances if the test sets comprised of distractions from a similar race, level of engaging quality, or gender orientation.

## **2.9 Recognition-Based Graphical Passwords Methods (RBGP)**

The RBGSs reported in the existing literature have used various types of images, such as faces, dejavu, story and Triangle. The following subsections will present an overview of the usability of RBGSs, followed by a brief discussion of the some common security vulnerabilities in these systems (Chowdhury, 2004).

### **2.9.1 Passface Scheme Passwords**

Passfaces are the most commonly used choice-based method (Biddle, 2009). Users utilizing this method are required to select from a selection of images of faces for the purpose of authentication as in figure (2.13). This stage of selecting the faces is carried out several times to make sure that the space for the password is sufficiently large. Hlywa (2011) carried out studies in their laboratory and it was documented that Passfaces users could remember their passfaces better than those who used the text-based passwords. They also examined the Passface system and found that the users of the Passfaces took much longer to login in comparison to the normal password users. They found that users did not favor using Passface since the main login elements and the remembrance levels (memorability) and recall levels were the same as those using the normal text-based password.



Figure 2.13 : Passfaces (Hlywa, 2011)

There are some disadvantages attached to this algorithm much like all the other authentication methods. First of all, after a password is chosen using the mouse device, it is easy for those with malicious intent to look at the password. Secondly, it is time taken during the login process, which is long, and during the registration stage which is also a long process which makes the algorithm to be slower compared to the text-based system. Majority of the users want to select faces of folks from the similar race, which can make the Pass-face password anticipated to a certain degree in addition to contain only one form (faces). Some of the displayed faces may not be welcomed by a number of users.

### 2.9.2 Dejavu Scheme (Random Art Passwords)

The déjà vu algorithm was designed by Touraj, 2015 and it starts by authorizing the user to select and remember a subset of pictures selected from a larger sample to

create the group on that they will use. Users should recall pictures of their selected group from a set of decoy pictures to login, refer to figure (2.14).

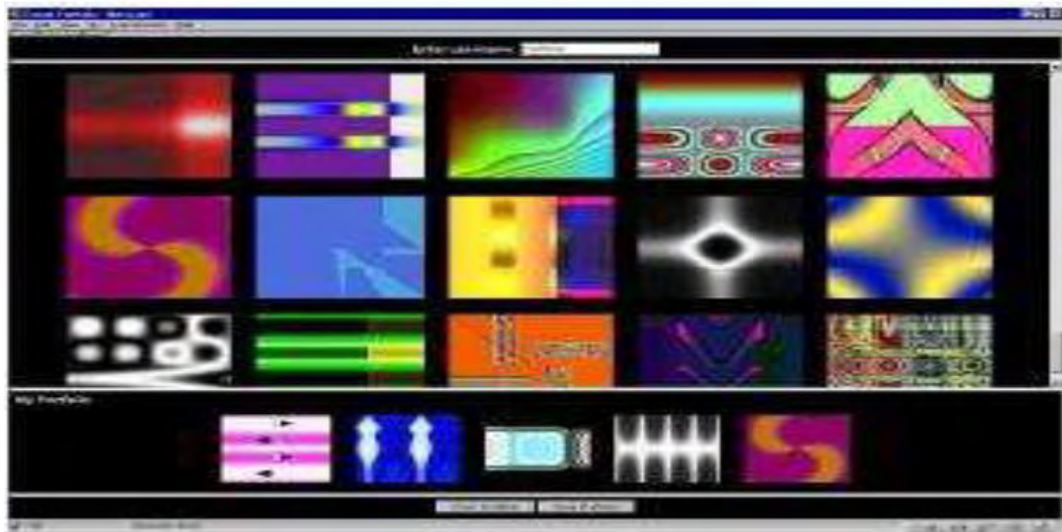


Figure 2.14 : déjà vu (Touraj, 2015)

A group of 25 images is presented in the test system in which 5 belong to the users' portfolio. The user has to recall all his/her portfolio images and display merely one panel. "Randomart" images are chosen because they are difficult for users to jot the password or show it to other people by means of image explanation. The Research community claims that it is ample to utilize a group of fixed 10,000 images; but the good-looking images must be selected precisely to enhance the chances of users selecting the same possible image (Biddle, 2009). The conclusions of their study publicized that 90% of the participants were successful in using this method for authentication while only 70% were successful using PINS and textual-passwords (Lashkari, 2011). Nevertheless, the average time for login is longer than the normal approach; however, its failure rate is much lower. Experiments on the Déjà vu system have revealed undeniable limitations. One of which is that the huge amount of space is used to store pictures on the server, and hence the process of authentication is slower because of the delay caused by network traffic.



The next limitation is that even though the password space size of the Déjà vu is smaller as compared to the text passwords, it doesn't mean that it is simpler to memorize the Déjà vu method (Deja Vu scheme is based on the widely belief that human beings have an excellent memory for images). Another experimental limitation is that the server requires storing the portfolio images' seeds of all the users in the format of plain text. Therefore, the image selection process from the database of pictures might be tedious and time consuming. Finally, to create a password via the Déjà vu system, it takes 60 seconds, but with the text-password, it is done only in 25 seconds (Towhidi, 2009; Biddle, 2009).

### 2.9.3 Triangle Scheme (Object Passwords)

Sobrado (2002) introduced a technique to overcome the problem of shoulder surfing security issue. Users in this algorithm are required to choose the pass-images that were selected at the registration stage out of a group of objects that are displayed. Users utilizing this technique have to click the inner part of the convex hull that shapes the pass-object as shown in figure (2.15).



Figure 2.15 : Triangle Scheme (Sobrado, 2002)

In this technique, the author proposed that the objects which are displayed during the login phase ought to be raised to one thousand objects to enable the password space

to be big enough and harder to predict. The technique proposes that users should discover just 3 of the pass-objects out of all the objects that are displayed to formulate a triangle form in order for authentication to take place. When conducting it for real, the amount of objects should be scattered randomly on the computer screen and the objects may vary sufficiently so that users would be able to differentiate them. The main disadvantage of this algorithm is that if there are too many objects that are displayed, it would be harder for the users to pin point the pass-objects and if there are too few objects then the space used will be smaller and hence become simpler to predict or hack (Touraj, 2015).

#### 2.9.4 Story Scheme

In 2004, the story scheme proposed by categorizing the available picture to nine categories as shown in figure (2.16), which are cars, animals, children, men, women, food, objects, sport, and nature. According to the figure, the users have to select their passwords from the mixed pictures of 9 classes with the intention of making a story easily to remember. There were some users who used this method without defining a story for themselves (Farnaz, 2009).



Figure 2.16 : Story Scheme (Farnaz, 2009).

This research showed that the story scheme was harder to remember in compare for Passface

### 2.9.5 Comparison of Typical Recognition-Based Graphical Password Schemes

The following table (2.3) shows Comparison between Passfaces , Déjà Vu , Triangle Scheme and story Scheme:

Table 2.3 : Comparison of Typical Recognition-Based Graphical Password Methods

Password Schemes	Authentication method	Remarks
<b>Passfaces</b>	To login, user is needed to identify and click 1 of the 4 pre-registered human faces from among decoys in 4 rounds of 9 images being displayed in a panel.	System generated faces are used in commercial version of Passfaces to avoid predictable passwords because users tend to choose faces from their own their race or attractive faces.
<b>Déjà Vu</b>	The scheme generates images from mathematical formulae with the help of a seed which serves as user specific data. To authenticate successfully, user has to recognize 5 images out of a total of 25 randomly generated images in any order.	The seeds are stored in the server in clear text to facilitate image generation process.
<b>Triangle (Object passwords)</b>	Its uses icons instead of images. The login process requires users to click inside a visualized convex geometrical shape made by the icons in 5 different rounds.	users never have to click directly on their password images.
<b>Story</b>	User selects a sequence of 4 images for his/her portfolio and logins by identifying one image from among decoys in 4 sequential rounds.	Story scheme authentication process has a sequence of 4 rounds of 9 images per challenge panel.

## 2.10 Comparison of Typical Recognition-Based Schemes Resistance Against Possible Attacks

The recognized possible attacks are based on the Common Attack Pattern Enumeration and Classification (CAPEC) and 3 features of password security founded by Angeli et al. 2005: recordability, observability, and guessability as in figure (2.17)

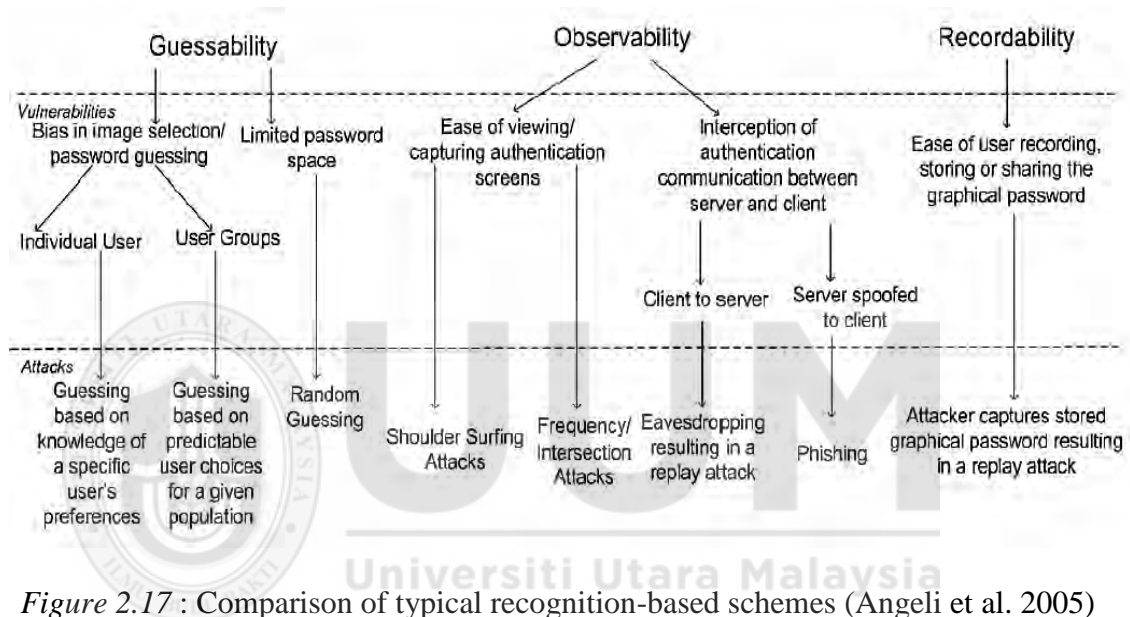


Figure 2.17 : Comparison of typical recognition-based schemes (Angeli et al. 2005)

Observability associates to the comfort in which the attackers may see the graphical password as it is being inserted into the system. Guessability associates to how simply the attackers may deduct the graphical password. Lastly, recordability associates to the comfort in which the users may verify the graphical password, preparing it simpler for the attackers to seize and repeat. Each of these features has been analyzed to underline the possible attacks which will manipulate defenselessness (Chowdhury, 2013). The workable attacks are mapped to the Recognition-based system on table (2.4)

Table 2.4 : Comparison of typical recognition-based schemes

Methods	Security issues	
	Authintication process	Possible attack methods
<b>Pass-face</b>	➤ User needs to select four pictures of human face from the nine pictures to be authinticated.	➤ Brute force, dictionary, guess and shoulder surfing
<b>Déjà vu</b>	➤ Authintication process is based on Hash Visualization techinque. User needs to pick various images out of many options. The user should recall all his\her selecting pictures and display only one panal.	➤ Brute force, guess and shoulder surfing
<b>Triangle</b>	➤ Users in this scheme are required to select the pass-images that were chosen at the registration stage out of a set of objects that are displayed and click the inner part of the convex hull that shape the pass-object.	➤ Brute force and guess
<b>Picture Password</b>	➤ Users choose a theme to identify the thumbnail pictures that would be utilized and after that register the arrangement of the thumbnail pictures to be utilized as the password from here on end.	➤ Brute force, guess and shoulder surfing
<b>WIW</b>	➤ Users in this scheme are required to select various images as pass-object. Each pass-object has numerous variations and each variant is given a particular code.	➤ Brute force and spyware
<b>Image Pass</b>	➤ Select a username, a 6X5 grid with a graphical password selection which reveals the images possible to be selected.	➤ Brute force and shoulder surfing
<b>WYSWYE</b>	➤ Users need to select N images of passwords within the M grid (where $N < M$ ).	➤ Brute force, guess and shoulder surfing

## 2.11 Culture

Culture is taken from Latin language which means to cultivate the soil (Hofstede, 1980). However, it has a much richer significance in anthropology. Culture can be describes as “that complex whole which includes knowledge, belief, art, morals, law, custom and any other capabilities and habits acquired by man as a member of society” (Kronenfeld et al., 2011). By 1952, Kroeber and Kluckhohn catalogued 164 definitions of culture (Liu, 2003). In 1951, Kluckhohn described it as:

*"Culture comprises of patterned ways of thinking, feeling, and reacting learned and conveyed largely by symbols, establishing the distinguishing successes of human parties, containing their personifications in objects; the critical center of culture contains traditional (i.e. historically sprung and chosen) ideas and particularly their associated values"* (Hofstede, 2001).

Working from Kluckhohn's definition of culture, Hofstede (2001) refined the definition of culture as the element of “mental programs” that are approved by masses from their childhood and established during their learning and working lives.

Hofstede (2001) divides the mental program of people into 3 broad categories, i.e., universal category, collective category, and individual category or level. The universal category of ‘mental program’ is distributed among people around the globe and it consists of normal behaviors, for example, expressing sorrows by crying and happiness by laugh. Most of the people inherit this category of their mental program from their parents. At the collective category of mental program, people from specific groups or societies share behaviors such as manners of drinking, discussion with parents, and the languages that they speak for expressing themselves. These behaviors vary from group to group, and can express diverse national cultures. Hofstede (2001) states that the collective category or national culture is totally

studied from childhood and not genetically inherited from parents. The individual category of mental program is a distinctive category containing individual traits, and is not shared among the people, though part of people's individual category is inherited from their parents.

## **2.12 Cultural Images**

The term 'cultural image' can refer to two different concepts. Firstly, they can be actual graphical images which can be associated with a particular culture. Secondly, the word 'image' can refer to a mental image rather than a graphical one. In this way, a cultural image can refer to the way in which people in a certain culture define or deal with a particular concept such as social mobility (Einwhoner et al, 2000). To complicate matters, a mental cultural image, such as of social mobility, may be explained by pictures illustrating different cultural aspects of social mobility. This thesis is mainly concerned with the first meaning, graphical images that can be associated with a particular culture.

## **2.13 Cultural Images in Graphical Passwords**

Cultural images are those pictures which can be associated with a particular culture. Example of using such pictures in computer science was shown in the work of Sun (2001). Sun showed the importance of using images that represent the users' national culture in the design of a web interface. This design would increase the user satisfaction of the web site.

In order to find cultural images, we need to find a clear definition of culture. According to Tylor (Jusdanis, 2011) culture is defined as "the list of all items of the

general life of people represents that whole which we call its culture”. From this definition, an image can be “cultural” if it is associated with the general life in a particular society.

Cultural images can give a feeling of familiarity within their contents for those people who belong to the associated culture. According to Pettersson (1982), “the things we human perceive in a visual field and the manner in which we interpret image content depend greatly on whether or not the image is familiar within our society and whether proper interpretation of the image has survival value within our particular culture”. It is a difficult task, however, to find cultural images that can be measured on an objective scale because of the subjective nature of the connotative meaning that individuals with different experience have with the shown image. Mathur (1978) identifies three factors that may affect the connotative interpretation of the visual image. The first is personality differences, which shows the unique characteristics for every human that may influence their view of the image. Those characteristics include their experience, communication abilities, expressiveness and other aspects. The second factor is the perceptual differences between people, as they would interpret only the part of the image they were interested in. The third factor is the difficulty of understanding of the connotative meaning of the image. It is easy to interpret the denotative meaning of an image, but it can be hard to get the connotative meaning. Due to this difficulty, some researchers suggested to focus only on the denotative messages in classifying images to avoid subjectivity problems (Yoon, 2008).

However, those differences in interpreting connotative meaning are not anarchic as it can be classified in terms of practical knowledge, national knowledge, cultural knowledge and aesthetic knowledge. It was shown that the connotative message of



an image could be interpreted in the same way for people from the same socio-cultural context (Yoon, 2008). In other words, while there are varieties of ways of reading the connotative message of an image based on the cultural knowledge of the people, there will be a common way of reading the connotative message within every socio-culture.

## **2.14 National Images**

National-specific images are those which denote objects such as foods, landscapes, famous people, famous buildings, and traditions that are located within a specific country. By revising the Tylor's definition of culture mentioned above, those national-specific images can be associated with the knowledge, belief, art, custom and habit of the country. Therefore, they can be considered as one type of cultural images that we believe they would establish sense of cultural familiarity with graphical password users who came from the same country. Moreover, national-specific images can be understood denotatively and connotatively in a common way by the people from the same socio-cultural context (Yoon, 2008). Therefore, they can be measured in an objective scale to decide whether they belong to the national cultural images or not.

Example of the national-specific images is shown in Figure (2.18). For example, this image of a famous Malaysian famous building "PETRONAS Twin Towers" can be seen as a cultural image for Malaysia as it cannot be related to any other countries such as Middle East countries , for example.



Figure 2.18 : A Malaysian famous building called “PETRONAS Twin Towers

Some images will be associated with a sub-culture of the national culture, and so it is important to specify the scope of the ‘national culture’. In this work the researcher has focused on Malaysia, which would be recognized by the Malaysian participants, and Malaysia culture.

## **2.15 Cultural Effects on Usability and Security of Recognition-Based Graphical**

### **Password Authentication**

Although there are several good RBGPs methods in technical terms, intensive study of their usability, reliability, and security remains incomplete (Suo et al., 2005). In particular, very few studies focus on how cultural effects might affect recognition-based GP schemes. For example, Jebriel and Poet (2014) carried out a cross-cultural study on Doodle scheme to find the relation between users’ cultures and their doodles. The results showed significant effect of culture on the drawings that might facilitate the guessing attack.

Most RBGP systems have been developed in western countries, and the suitability of such schemes would be suitable for users who live outside those countries has yet to be tested. In other words, it is unclear whether the developers considered cultural differences when they design their techniques. For instance, most of the images used for the existing RBGP schemes are from western cultures. Therefore, it could be discussed that deploying such RBGP methods in other nations would need more devotion to cultural impressions on their security and usability. By analyzing researches on the relationship between cultures and the usability features of human computer interaction, it is recommended below that cultures would have an effect on RBGPs in terms of both user acceptance and user performance.

## **2.16 Cultural Models**

Several anthropological researches have been done to study various cultures (Jiao, 2008). As a consequence, numerous cross cultural paradigms have been offered by researchers such as Hofstede (2001), and Trompenaars (1997); these paradigms serve as a valuable outline to learn highly-specific variations among different cultures. For instance, various of these cultural prototypes have been utilized in the field of information security, management , ecommerce , web engineering, and e-government.

Trompenaars designed his cultural paradigm based on the notion that “culture is the way in which a group of people solves problems and reconciles dilemmas” (Trompenaars and Turner, 1997). Similarly, Trompenaars believes that culture is defined by joint challenges and conflict resolution. These issues may be further divided into three classes: issues in interpersonal relationships; issues associated with time; and issues associated with the environment. Based on the outcomes of the

questionnaires finalized by 30,000 members from various nations, Trompenaars suggested 7-cultural dimensions for showing that how peoples of different nations can resolve these issues:

- i. particularism versus universalism.
- ii. communitarianism versus individualism.
- iii. emotional versus neutral.
- iv. diffuse versus specific.
- v. ascription versus achievement.
- vi. attitudes to time
- vii. attitudes to the environment

From 1968 to 1972, Hofstede (2001) managed a research to study how people from 40 different countries vary in thinking or acting with regard to social situations. Over 116,000 IBM employees in 40 nations took part in this research. Data was gathered and 4-dimensions were proposed to differentiate between national cultures. The 4-dimensions are low power distance versus high power distance, high insecurity prevention versus low insecurity prevention, collectivism versus individualism, and femininity versus masculinity. For every aspect, a score was allotted to 55-countries and 3-regions to expedite the process of their national cultures. A 5<sup>th</sup> aspect called short-term orientations versus long-term orientations was later added to the existing aspects. Hofstede (2001) exposed the idea for this aspect from a study managed by Michael Harris Bond in 1985 in Hong Kong. For this measurement, a score was allotted to 23 nations/countries to see if they are belonging to the long-term orientations or the short-term orientations.

## 2.17 Overview of Literature Review

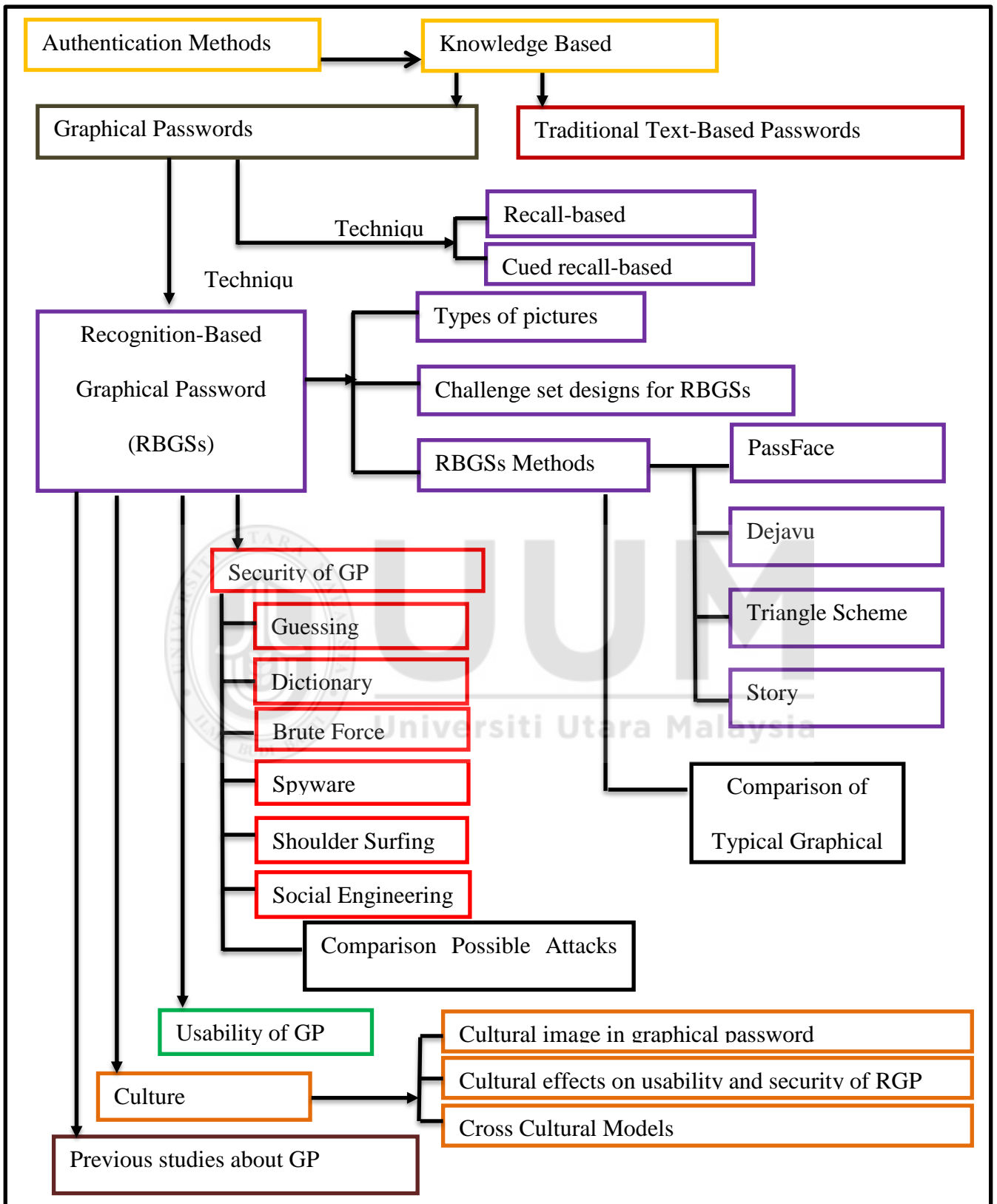
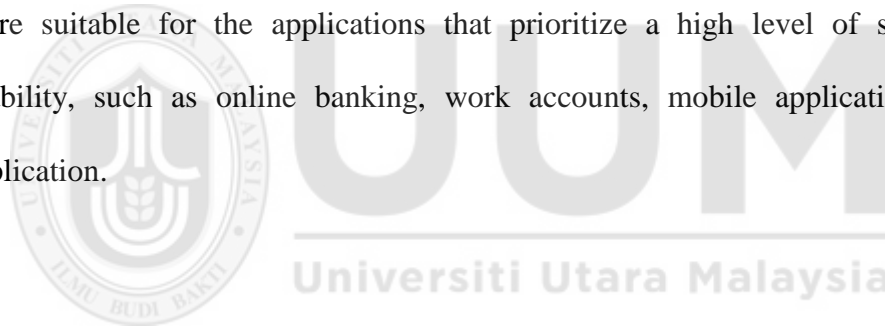


Figure 2.19 : Literature review Map

## 2.18 Summary

After all, the researcher in this study noticed an existing gap in the literature in which most studies mentioned above relied heavily on the characteristics of certain images without considering the end user background. Therefore, this study tries to tackle this by proposing a graphical password based on cultural tights among users in Malaysian region. The general findings of all studies in this section show that graphical password developers can choose any set to design user guideline with a familiar graphical password as long as they combine them with appropriate usability/security guidelines. This is because the guidelines will cover most of the disadvantages that may affect the usability or the security. Therefore the graphical password guideline is more suitable for the applications that prioritize a high level of security over usability, such as online banking, work accounts, mobile application and web application.



## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.1 Introduction**

This chapter presents and justifies the methodology and design of this research. This chapter also presents research method, research design, data collection, study sample, research instrument, data analysis, pilot test and validity and reliability of the instrument development (questionnaires).

The strategies for answering the research questions must be identified after planning the research design (Smith, 2012), which are considered to be very helpful to get a satisfactory outcome of this study. In the design of research, all those strategies will study the impact of cultural familiarity in Malaysia on the usability and security of Recognition Based Graphical Passwords RBGPs.

#### **3.2 Research Methodology**

The most appropriate methodology that can be used in this study is exploratory research, in which this study applies questionnaire technique combined with an experiment (Miller, 2006) . Exploratory research is most useful in situations where limited information is available and the researcher wishes to have the flexibility to future explore of research (Polonsky and Waller 2005; Cooper and Schindler 2006).

The primary goal of exploratory research is to gain better understanding of an issue or situation and it is appropriate way to provide ground work for later more rigorous studies at a later date (Davis 2000; Cooper and Schindler 2006).

Zikmund (2003) notes that the first step in exploratory research is to analysis and review the existing related studies in the subject area then transform potential issues into more defined problems to develop research objectives. Chapter Two has provided a review of previous studies into the area of graphical passwords and related issues.

This study seeks to identify the role of cultural familiarity with the user's choice when create a graphical password and how can the cultural familiarity can affect the usability and security of Recognition Based Graphical Passwords (RBGP's).

### **3.3 Research Design**

It is important to mention that this study will use the six phases below to achieve the objectives of this research: i.e., (1) Problem identify, (2) Construct database, (3) Prototype, (4) Experiment, (5) Analysis (Quantitative data Collection), and (6) Discussion as demonstrated in figure (3.1). Therefore, this strategy is considered the most appropriate methodology to obtain data to facilitate in-depth explanation of the participant with regard to their perceptions when using Recognition Based Graphical Passwords (RBGP).



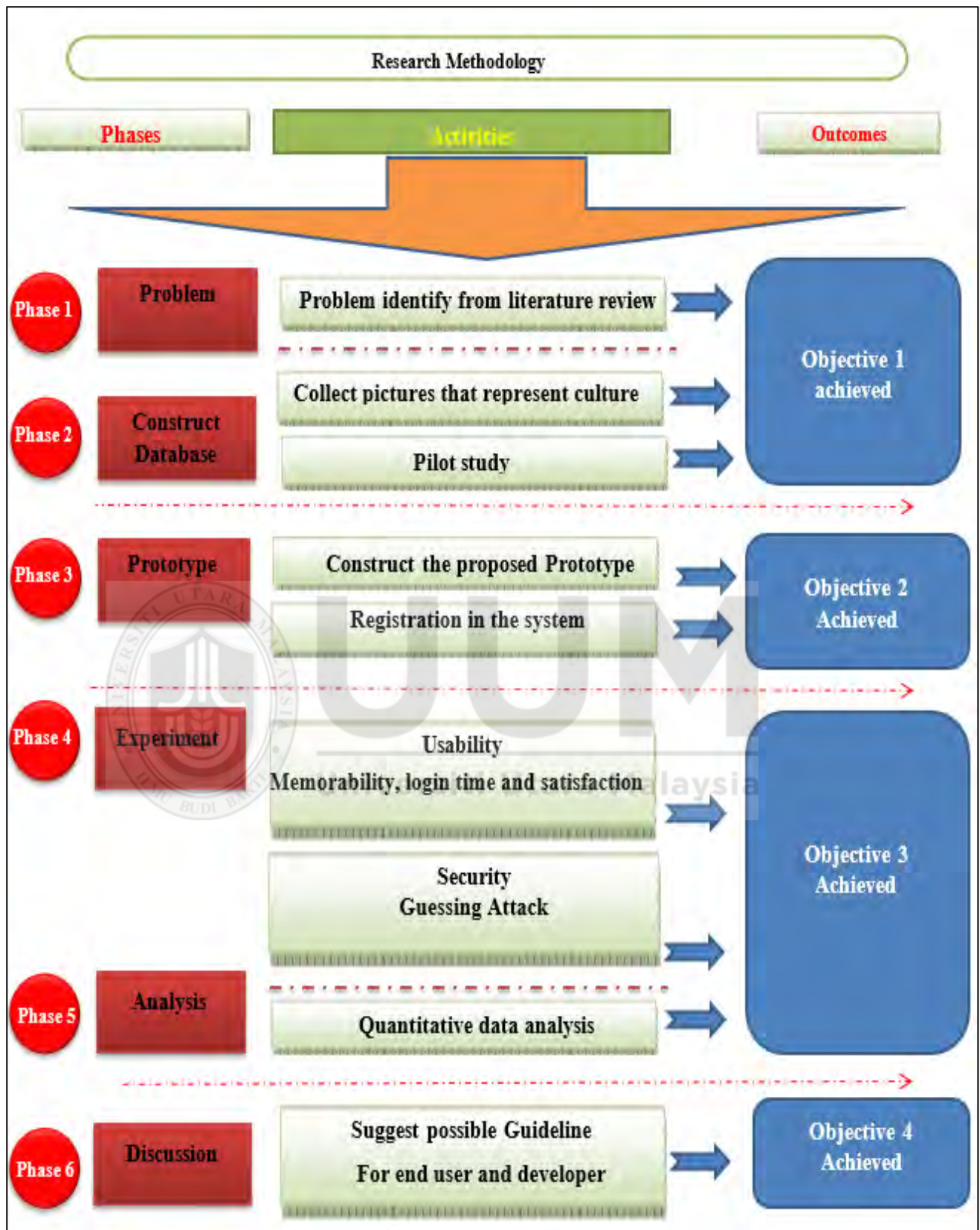


Figure 3.1 : Overall phases of research design

### **3.4 Phase One : Identification of the Problem**

The main problem of this study concerns about the current techniques of graphical password to which it revealed a number of weaknesses and drawbacks in terms of memorability and security related aspects. As such, researchers (e.g., (Sun, Chen, Fang, & Chang, 2012; Yadav & Mohod, 2013; Zangoeei, Mansoori, & Welch, 2012)) acknowledged the need for more efforts to simplify the memorization procedure by linking graphical elements into users' cultural or context.

On one hand, other problems in the Recognition Based Graphical Password method, such as instructions on how to correctly operate those systems, were not extensively discussed; on the other hand, a majority of the schemes that have been proposed in Western countries was the recognition-based graphical-password scheme (Aljahdali & Poet, 2014a, 2014b). Therefore, the types of pictures used for those graphical passwords were of western culture origin. Hence, the cultural influences on those graphical password systems should be taken into consideration before employing them in other countries, e.g., Asian countries.

### **3.5 Phase Two : Collecting Pictures**

It was decided that pictures representing different national cultures would be collected in order to be used in the proposed scheme and while researching the cultural factors in RBGPs. Initially, various ways of collecting pictures were analyzed and discussed. For example, the researcher discussed the possibility of showing participants of different cultures a set of pictures collected from the web and asking them to indicate whether or not those pictures reminded them of their own cultures; the possibility of biasness may occur if study authors themselves were to

choose the pictures. Therefore, it was decided that the participants should be allowed to choose the image that they think best represents their national culture. An online questionnaire was created to collect pictures along with demographic information in order to achieve this goal (refer to Appendix A). The questionnaire was designed to give the participants the option of submitting images by directly uploading them.

### **3.6 Phase Three : Construction Database and Prototype**

In order to conduct the experiment, a database should be constructed to collect the cultural pictures and start an experiment. Below the construction and registering in the system :

#### **3.6.1 Construct Database and Prototype**

To conduct the experiment, the researcher built a prototype and a database for these pictures which are collected by the participants (Roy, Barik, & Mazumdar, 2004), in order to prepare to present it during the experiment while the participants are going to choose their graphical passwords. The proposed prototype carried out in Java language , it's offering an elegant and easy-to-understand presentation of interface graphics, in addition java language it very strong language in the security applications ( Zhang,et al. 2007; Liang, et al. 2013) , and the database constructed via SQL server 2008. The figure (3.2) shows one of interfaces of the prototype.



Figure 3.2 : An interface to start registering a graphical password

### 3.6.2 Registration in the System

In this phase, the participants were asked to register in the system by giving a user name and make his/her graphical password. The purpose of this phase is to see how much the participant affected by his/her cultural environment and at the end the graphical password. It was measure through the database of the prototype and the reasons behind choosing were measured through a questionnaire adapted by (Aljahdali, 2015).

### 3.7 Phase Four : Experiment

Summarize the related aspect of the experiment according to (Renaud, 2009b; Aljahdali, 2014a) :

- i. **Secret pictures:** each participant chose 4 pictures and each picture was assigned to a separate challenge set. This number of pictures is used by most RBGP schemes and has at least the same security level as a 4 digit PIN depending on other design factors.

- ii. **Challenge set size:** each challenge set has 16 pictures in a grid of 4\*4 (1 secret picture and 15 distractors). This is the upper limit size of the challenge set as it can take long time to search for the target picture in a larger challenge set size.
- iii. **Picture size:** All pictures were in the largest possible size without the need to scroll left-right or up-down. This was in the case of displaying the challenge sets. However, it was impossible to show all the available pictures without the need to scroll up-down. For storage space, there was no problem with storing the pictures in this scheme due to the limited number of users.
- iv. **Progress indicators:** there should be clear indicators and instructions for users about the authentication process. This scheme uses the upper part of the screen to show the instructions for the users during the registration and login process.

### 3.7.1 Security Aspects

One of the most important factor in Graphical Passwords is the security issues, in order to study the feasibility of using the cultural familiar picture and its effects in the aspect of guessing attack, an experiment was conducted by inviting people who have relations with the participant (victims ) as attacker, they given three times to guess the graphical password and the result stored in the prototype while reasons behind security attack (guessing) were shown in a questionnaire adapted from (English, 2012).

### 3.7.2 Usability Aspect

To study the effect of cultural familiarity on the usability of RBGPs, usability is an essential parameter. Generally, for usability, three factors are involved which are

effectiveness (memorability), efficiency (login time), and user satisfaction. The measurement of those factors covered by the data base of the prototype and through a questionnaire adapted from System Usability Scale (SUS) Template.

### **3.8 Phase Five : Data Analysis**

In this section, the quantitative data analyzed with the help of SPSS (Statistical Package for Social Sciences) version (20) to assemble and schedule the data analysis according to number of different factors. These include consideration of the type of question to address, the type of items and scales that were included in questionnaire, the nature of the data that are available for each of variables and the assumptions that must be met for each of the different statistical techniques (Pallant, 2011).

This study has categorical variable which is (cultural familiarity with user's choice). The researcher used statistical tests such as the standard deviation (SD), mean (M), and paired two-tailed t-test in the analysis of the responses of the person concerned to compare the differences in means among participants. Independent-Samples T test, correlation and regression are conducted as the descriptive analysis. The descriptive analysis examines the gathered responses and the distribution of the data to draw a possible conclusion.

### **3.9 Phase Six : Discussion**

During this phase, a discussion about the findings from previous phases and through a quantitative study in order to suggest possible guideline for both end user was done. Moreover, at the same time, the problem of usability and security were discussed to tackle the possible problems that may occur during the experiment, and the finally for making recognition-based password more usable and secure.

### 3.10 Data Collection Procedures

The findings of most studies are generally supported by field data (Zikmund et al., 2010). In this research, data has been collected as following figure (3.3):

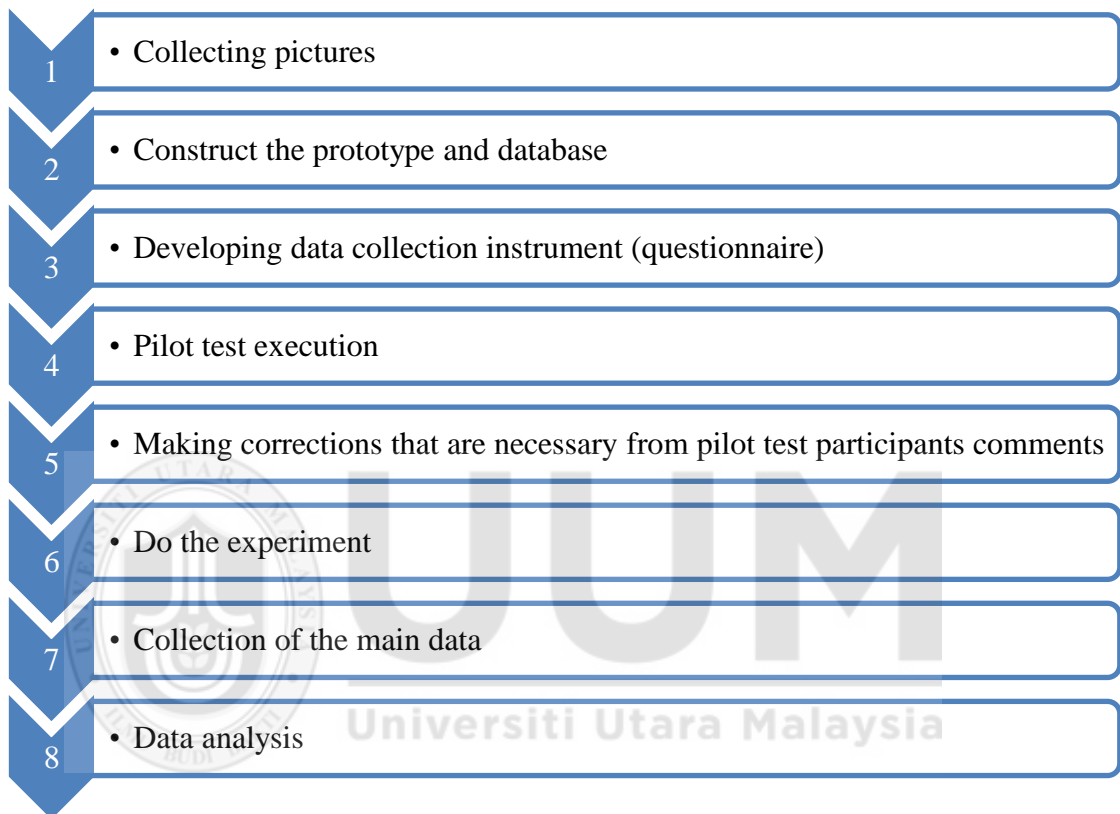


Figure 3.3 : Procedure of Data Collection

### 3.11 Sampling Technique and Study Sample

This study was focused on the undergraduate and postgraduate students of UUM. Several sampling methods are adopted to reveal the unidentified characteristics of the selected population.

This study adopts the simple random sampling technique in which all elements in the population are considered and such elements has an equal chance of being chosen as the subject in order for each aspect of the population to be represented in the sample

(Zikmund et al., 2010) and to provide accurate statistical descriptions of the population. In the same vein, Creswell (2012) stated, this type of sampling from all sampling techniques is consider the most rigorous technique for select the participant, where representative all the population and also can make generalization to the population.

According to Smith (2012) survey participants should be gathered in such a way that they are confined in one space. For example, a survey can be administered to students inside classrooms or to people in the middle of a seminar or a program. This method saves money for postage and ensures a high response rate given that the potential subjects will have no choice but to participate in the survey.

According to Hartas (2015) the importance of sample size in any experimental study cannot be ignored. A sample is a subgroup of a population that participates in a study and provides data for the study (Clark & Creswell, 2014). Cresswell (2005) stated that, in an experimental study the sample size for per group (or cell) approximately 15 participants. And this number from the participants also recommended by Ashouri *et al*, (2015), who said that the sample size in experimental study is recommended about 15 people. Thus, based on the objectives of this study, and also according to the process on the experiential study, this study will select 30 participants for extract their perception on each task. As mentioned by Notani (1998), studies on working behavior should focus on the general adult population than on the student population given that the former population are more experienced than the latter.



### 3.12 Research Instruments

A survey has been conducted to gather primary information on related factors. The use of questionnaire as the data gathering instrument is considered as efficient (Kumar, 2011). Furthermore, questionnaire that are self-administered having closed-ended questions.

The questionnaires for this study has adapted from SUS, English (2012), Aljahdali (2015) as shown in the table (3.1):

Table 3.1 : Questionnaires

No	Type of Questionnaires	Adopted from
1	Collecting picture (A)	Aljahdali (2015)
2	Guideline (B)	Aljahdali (2015)
3	Security (C)	English (2012)
4	Usability (D)	SUS

For the instrument design, the questionnaires is divided into four parts: A, B, C and D. The part A is used to collect picture for the prototype and asks questions related to the respondents demographic background which are gender and age group. Part B is about deriving a guideline to make RBGP more secure and usable. Part C contains items to reasons about the way of guessing the graphical password. While the part D asks questions related to satisfaction about the RBGP

### 3.13 Pilot Test

A pilot study must be conducted before collecting data to validate the survey instrument (Bryman, 2004; Saunders *et al.*, 2003). A pilot study is conducted to determine if the questionnaire can be amended further for the respondents to understand and answer all questions with ease. According to Simon (2011) a small

number of participants (10) who will not be involved in the main study will complete the draft questionnaire to investigate whether it required any design modifications and to see the validity of the images provided by contributors (see Appendix A,B,C,D)). The selected participants were undertaking different courses at the School of Arts and Science, Universiti Utara Malaysia. The selection of the participants was random in which the researcher invited the students to a series of experiments during their free time. A short demonstration was given to the participants to help them understand the aim of the study and to eliminate any misconception when answering or responding to the researcher's questions. A total of 10 questionnaires were distributed to the students to identify if these instruments are properly constructed and if the questions can be easily understood by the respondents. The students have been asked to answer these questionnaires and to provide some feedback with regard to the validity and clarity of the instrument.

### **3.13.1 The Importance of Pilot Study**

Blaxter, et al. (1996) found that "You may think that you know well enough what you are doing, but the value of pilot research cannot be overestimated. Things never work quite the way you envisage, even if you have done them many times before, and they have a nasty habit of turning out very differently than you expected". It is along these lines clear to the analyst, that the pilot concentrate on in the momentum research was fundamental to keep the exercise in futility, vitality and cash. The esteem is additionally stressed by the focuses recorded beneath.

As per Welman and Kruger (1999) numerous amateur scientists are frustrated when they find that the rules for study are just legitimate in an accurate situation, and not in the down to earth examine environment where they direct their examination

contemplate. It can be the principle motivation behind why a pilot study is required. Welman and Kruger (1999) likewise recorded the accompanying three estimations of a pilot study:

- i. It is expected to recognize conceivable blemishes in estimation systems (counting directions, time cutoff points, and so on) and in the operationalization of autonomous factors. This estimation of the pilot study was extremely appropriate in the ebb and flow study of investigation. The analyst utilized two distinctive estimation methods with the exploration gatherings to pick up data and to do a pre-and post-test.
- ii. A pilot study is additionally profitable to recognize vague or uncertain things in a survey. In spite of the fact that the present study did not make utilization of self-planned polls for the pre-and post-test, guiding of the utilization of the current survey was vital.
- iii. The non-verbal behavior of members in the pilot study may provide with basic data regarding any dishonor or inconvenience faced about the stuff or expression of items in a questionnaire.

### **3.13.2 The Goal of a Pilot Study**

The specialist sees the objective of a pilot study by and large as identified with the point of the examination venture of which it shapes part. The general objective of a pilot study is to give data that may add to the achievement of the exploration extend all in all. The last is bolstered by the accompanying quotes related to the esteem and objective of pilot studies: "to check whether the brute will fly" (De Vos, 2002), "reassessment without tears" (Blaxter, Hughes and Tight, 1996), and "Don't go out on a limb. Pilot test first." (Van Teijlingen and Hundley, 2001). The primary objective along these lines appears to save some time, effort and cash that could be

vanished if a noteworthy study concentrate on falls flat in light of unexpected traits. The objective is in this way to test the study on little scale first to deal with all the conceivable issues that may prompt to disappointment of the exploration technique. It may minimize the danger of disappointment.

In the present study the objective of the pilot study on comprises of two sections. The first was to discover however many as would be prudent handy game plans that may affect the accomplishment of the exploration technique. The other included dealing with all reasonable items identified with estimation instruments and also the materialness of these tools to the prospective results of the work.

### **3.13.3 Validity and Reliability**

The validity and reliability of the developed measures must be ensured. The former refers to the capability of the instrument to assess the target items, whereas the latter refers to its consistency (Sekaran, 2003). According to Smith (2012, p. 5), *“the quality of a measurement procedure that provides repeatability and accuracy.”* The validity and reliability of the instrument has been analyzed after the pilot test. Smith (1991, p. 106) added the following: *“validity is defined as the degree to which the researcher has measured what he has set out to measure.”* Smith (2012) argued that validity only pertained to a particular instrument. However, a reliable measure may not be able to assess a specific item despite showing consistency. The reliability coefficient is expressed in terms of Cronbach’s alpha.

An  $\alpha$  of 0.70 to 0.80 is generally acceptable (Kaplan & Sacuzzo, 2008). The correlation between the dependent and independent variables must be estimated after ensuring the reliability of the measurements. However, ensuring the reliability of the measurements does not necessarily ensure their validity. The questionnaires can be

validated by a group of expert judges (Kidder & Judd, 1986). Validity can be used to improve and evaluate the reliability of existing scales. For the validity, there may be no need to carry out the validity of questionnaire items that were originally adapted from another studies (Yıldız, 2016; Golafshani, 2003). Different procedures, such as factor analysis, can be used to establish construct validity (Zikmund et al., 2010; Smith, 2012). Therefore, a pilot study was conducted to enhance the reliability and validity of the measures.

#### **3.13.4 Face Validity**

Face validity which is likewise known as "Content validity" needs to do with the testing respondents' cognizance of the things in the instrument. It alludes to the straightforwardness or significance of a test as they seem to test members, Holden and Ronald (2010). This is extremely crucial in this sort of research settings; it has been done before continuing to the fundamental information gathering phase, with the end goal of watching the slip-ups in the instrument and to be rectified before going for the principle information accumulation. For this reason, every question of the instrument things was reframed and copied to look at if there could be any variety or misconception to the reaction of any of the inquiries, this to guarantee the examination on how objective and bona fide the assembled information are. As Pallant (2011) and Zikmund et al. (2010) proposed, scientists are likewise among the reasonable people to be utilized for face validity amid the process of survey designing.

#### **3.13.5 Population Distribution of the Pilot Study**

This pilot study involves 6 males representing 60%, and 4 females represented by 40%. The result is shown in Table (3.2) below:

Table 3.2 : Gender Distribution of the Pilot Study

<b>Valid</b>	<b>Frequency</b>	<b>Percent %</b>
<b>Male</b>	6	60
<b>Female</b>	4	40
<b>Total</b>	10	100

Seven (7) out of the respondents are postgraduate students and three (3) are undergraduate students in the School of Arts and Science (IT/ICT), making 70% and 30% respectively. Table (3.3) shows the course level distribution.

Table 3.3 : Course Level Distribution of the Pilot Study

<b>Valid</b>	<b>Frequency</b>	<b>Percent %</b>
<b>undergraduate</b>	3	30
<b>Postgraduate</b>	7	70
<b>Total</b>	10	100

From the respondents administered during the pilot testing phase, more than 90% which have a good experience in the using of computer, however; less than 10% have limited experience in the using of computer.

### **3.13.6 Pilot Test Results (Appendix A)**

In this study, a small number of participants (10) completed the draft questionnaire to investigate whether it required any design modifications and to check the validity of the pictures provided by participants (see Appendix A). In particular, the aspects that were examined in the pilot study are the following:

#### **1. Time required to finish the questionnaire**

The results showed that time needed to finish the questionnaire was not long;

Table 3.4 shows the time spent by each participant. Two participants (20%) believed that the questionnaire took much time and should be shortened while

eight participants (80%) reported that the questionnaire did not take too much time to complete. Therefore, it was decided that there was no need to revise the questionnaire because the completion time was too lengthy.

Table 3.4 : Time to finish the questionnaire of the Pilot Study

<b>Time required to complete the questionnaire</b>	<b>Up to 5 min</b>	<b>6-10 min</b>	<b>11-15 min</b>	<b>16-20 min</b>
<b>Number of Participants</b>	3	5	0	2

## **2. Layout of the questionnaire**

The results showed that all the participants were satisfied with the layout of the questionnaire. The only suggestion by 4 of participants was about rearrangement for some items to be more clear, this modification should be helpful. Therefore, it has been decided to modify the layout of Questions.

## **3. The appropriate number of pictures requested from the participants**

Initially, the questionnaire was designed to ask for five pictures representing a participant's national culture. The results showed that nine participants (80%) agreed with five pictures as an appropriate number, because they found it easy to imagine and then find five pictures from their national cultures. Only two participants (20%) found it hard to think about five pictures representing their national cultures and felt it should be a lower number (either three or four) in order to make it easier for the participants to complete the questionnaire. Based on these results, there was no need to change the number of pictures to be asked of the participants.

The pilot study was helpful, because the questionnaire was updated based on feedback from the participants and other key elements of the study process proved to be reliable. The updated questionnaire will be used in the main study of the research.

### **3.13.7 Pilot Test Results (Appendix B,C and D)**

The components of the pilot testing are the reliability testing of the items contained in the questionnaire and population distribution of the pilot study. The first of the pilot testing is the reliability testing of the items contained in the questionnaire. The results shown in the following tables .

Table 3.5 : Reliability Testing Result

<b>Variable</b>	<b>Cronbach's Alpha</b>	<b>No of Items</b>
<b>Usability</b>	0.722	10
<b>Security</b>	0.781	8
<b>Guideline</b>	0.823	15

### **3.14 Summary**

The methodology of the research is presented in this chapter. Several procedures and justifications are incorporated in the methodology to fulfill the objectives and to answer the questions of the research. The research framework is also presented in this chapter.

This study uses a questionnaire and the prototype as the primary data collection instrument. The questionnaire also has been piloted before conducting the main survey to test the validity and reliability of the measures (Chapter four). The survey data then be used to fulfill the research objectives.



# **CHAPTER FOUR**

## **CULTURAL FAMILIARITY’S IMPACT ON CHOOSING PICTURES FOR RECOGNITION-BASED GRAPHICAL PASSWORDS**

### **4.1 Introduction**

Since the main aim of this study is to determine the feasibility of cultural graphical password, understanding the patterns in which users preferences may contribute to the way they secure and recall information. Therefore, this chapter consist of two parts the first one (Experiment 1) attempts to identify the type of pictures to be considered for a certain population in accordance to their culture. To do so, the researcher conducted web study (Appendix A) among students from different countries in order to categorize the common and uncommon selections with regards to their country of origin. This part also described the validity of the selection process. The characteristics of the students and the procedure are also discussed at this chapter. This is to provide more insights about the participants’ background used for selecting the collection of pictures. It also highlights the main elements associated with the selection of culture images for securing personal information. This part also presents the pictures that have been collected in order to construct the database for the experiment which leads to achieve objective one .

The second part (Experiment 2) explains the respondent profile, main procedure and results from examining the cultural familiarity’s impact on choosing pictures for recognition-based graphical passwords. The rational for carrying out this experiment

was due to the literature which addressed how people with different cognitive abilities can process information in accordance to their mental capacity.

Before testing the usability and the security of a culture familiar graphical passwords, it is necessary to examine the methods of choosing the pictures for the graphical password GP in order to see how much the participant affect by their culture which at the end of this chapter an objective two would be achieved.

#### **4.2 The Aims of the Experiment 1**

The researcher relied on the obtained images in order to build the culturally-familiar picture database for this study. This is because images that feature a certain cultural values are easier to remember than pictures with less cultural values. It is evident from the literature that images are commonly used to convey a perceptual and cultural message based on the anticipation of its elements in shaping that message (Mitchell, 2002). In addition, Bal (2003) added that user build his or her perceptual understanding of the display based on the objects used to construct a certain meaning or message. On the other hand, the connotative meaning of the image relies on the cultural and historical context of the image. Based on this understanding, one can assume that picture with cultural object mixed can be easily used to convinced the message better than picture with unfamiliar cultural objects. In order to achieve objective one of this thesis, a database established which it contains pictures that represent Malaysian and other cultures.

### **4.3 The Design and Method of Experiment 1**

This experiment was based on between-subjects design. Although this type of design requires more participants, but in order to would not be a compounding factor, biasing the results. The main survey began by sending invitation emails randomly to the students of the University Utara Malaysia (UUM). In addition, social networks like Facebook were used to invite people to participate. The invitations began with a brief introduction of the experiment and its aims, followed by a link to the survey. The required data were provided by each participant: gender, age, education, country, and set of pictures belonging to the particular national culture.

### **4.4 The Procedure of Experiment 1**

The participants who agreed to take part in this survey began by answering a few demographic questions about gender, age, education, and the country they believe represented their national culture. After completing the demographic questions, the participants were asked to provide five pictures that came from their countries. They provided those pictures by uploading it directly to the web questionnaire . All instruction for filling the questionnaire were explained to the participants in order to illustrate the purpose of questions.

However, it was necessary to clarify the meaning of national cultural pictures. At the end of the survey, all the information was stored in an online database for later analysis.

## 4.5 Results of the Experiment 1

The following sub-sections will present the results of experiment

### 4.5.1 Respondent Profile Appendix (A)

The population distribution of the respondents is based on gender, academic degree, and age. This is holistically presented in appendix (A). For the gender distribution, out of the 40, 25 making 62.5% are females while 15 of 37.5% are the males. Figure 4.1 presents the gender distribution of the respondents.

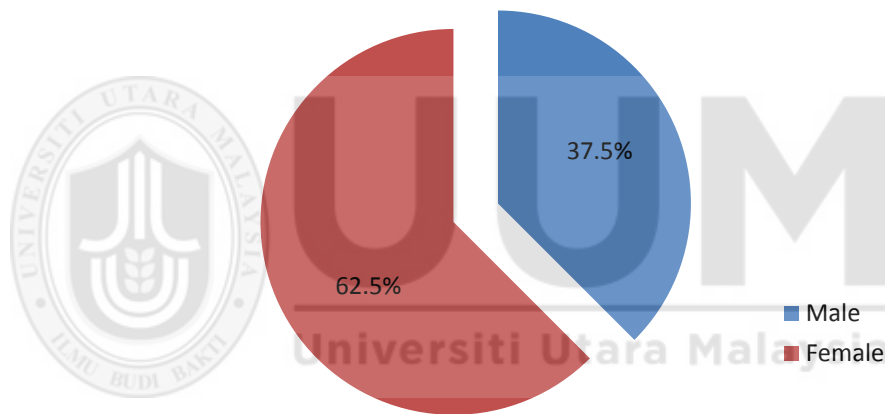


Figure 4.1 : the gender distribution of the respondents

To depict the academic degree of the respondents, the questionnaire administered inquires about the academic degree of the respondents. The respondents' degrees were exclusively drawn from BSc, MSc and PhD degrees, and the distribution shows that 25 making 62% were BSc students, 7 of 22% were MSc students while only 5 of 13% were PhD students. Figure 4.2 shows the academic degree distribution of the respondents.

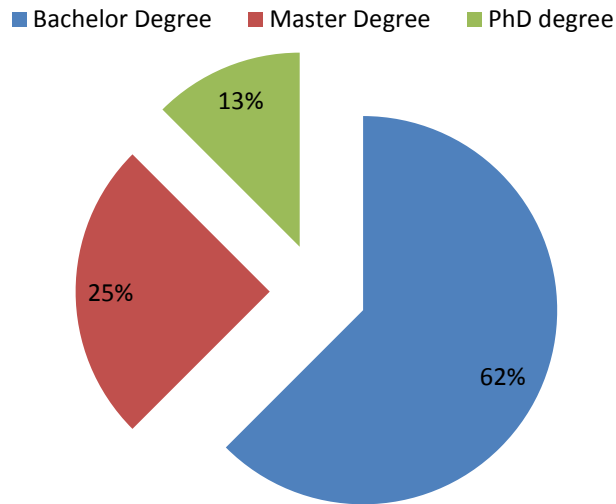


Figure 4.2 : the academic degree distribution of the respondents

The age distribution of the respondents is also reported. Out of the 40 respondents, 29 which is 72% are between 18-25 years old, 9 respondents which represent 23% are between 26-35 years old, while only 2 respondents which 5% were between 36-45 years old and no one was in 45 years old and above. Figure 4.3 shows the age distribution of the respondents.

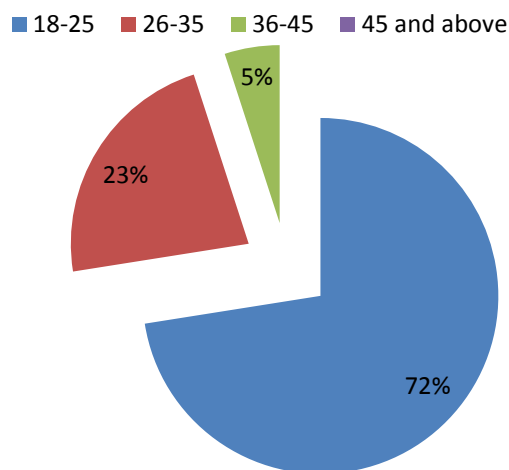


Figure 4.3 : The age distribution of the respondents.

The questionnaire administered asked to enquire about nationality of the respondents. It is important to note that nationality is one of the factors that affect the relationships to reflect the participants culture in creating graphical passwords. The profile shows that 30 which is 75% were represent Malaysian culture while 25% were represented the other cultures. Figure 4.4 shows the nationality distribution.

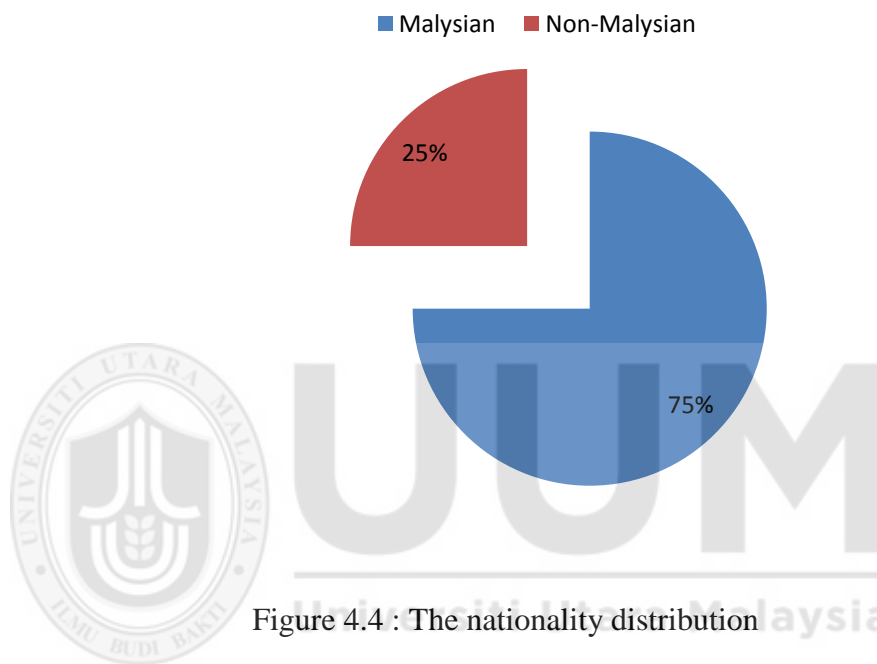


Figure 4.4 : The nationality distribution

#### 4.5.2 Pictures Database

The main aim of this survey was to have a database of representative pictures that came from different countries; the total number of picture links was 200. This number presented the opportunity to exclude pictures that came from participants who did spend most of their lives in their designated national-culture countries, so as to increase the validity of the representative nature of the final pool of pictures. There were only 4 such participants, which meant eliminating 20 pictures. Before finalizing the database of national culture pictures, all pictures were refined on the basis of quality, simplicity, and validity.

#### **4.5.2.1 Quality**

An image must have acceptable resolution to make it functional for any GP scheme, so all pictures with a resolution lower than 72dpi were removed from the database. It was also determined to remove all black-and-white pictures because they can be distinguished so easily from color pictures and thus do not work well together in a single GP scheme.

#### **4.5.2.2 Simplicity**

Pictures with complex layouts were removed from the database. For example, some pictures had multiple pictures combined into one frame, while others had written comments that diminished their clarity.

#### **4.5.2.3 Validity**

As with any online survey, some participants may misbehave and send pictures that offend people. Therefore, all pictures were reviewed carefully to identify and remove unsuitable pictures.

#### **4.5.2.4 The culturally-familiar picture database**

After application of the above conditions on all the pictures received from the participants, the final database was 188 pictures from Malaysia and other countries. Examples pictures are shown in Appendix E. In order to make the database ready for this research, it was divided into two categories: pictures from Malaysia selected by Malaysian students and pictures selected by non-Malaysian students. Out of the 200, 150 making 75% were pictures sent by Malaysian student while 50 of 25% were

picture sent by Non-Malaysian student. Figure 4.3 shows the number of pictures for each category.

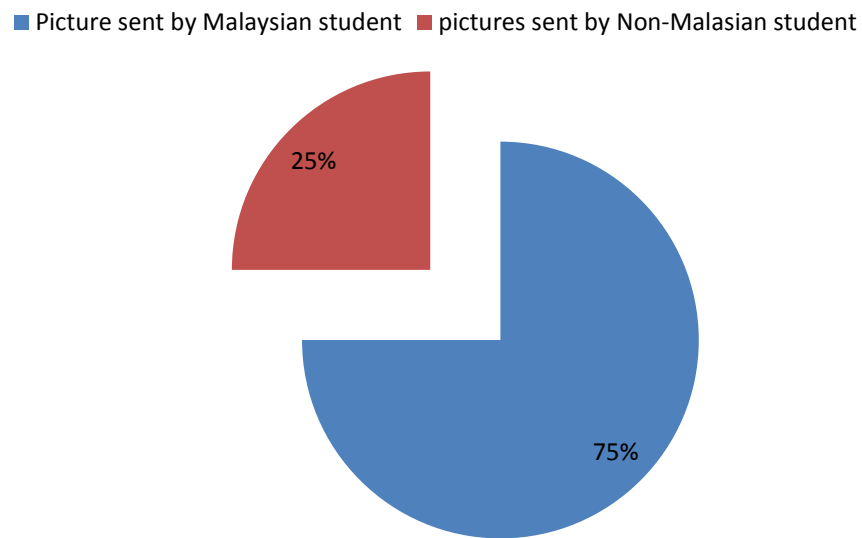


Figure 4.5 : The number of pictures for each category

#### 4.6 The Aim of Experiment 2

In order to have more insights about the cultural images and its selection process, researchers like Fischman (2001) stated that for one to consider the use of visual cultures, it is essential to conduct some research about the cultural characteristics of the selected population in order to embed the necessary features into the visual images. This include incorporating the main concept of inquiry and the reflection of what individual may consider familiar to his or her own environment.

#### 4.7 The Design of Experiment 2

In order to investigate the objective two, a culturally-familiar graphical password scheme has been developed (see Figure 5.1). This scheme was proposed to test participants from Malaysia. The design of the culturally familiar graphical password



scheme was based on the guidelines proposed by (Aljahdali 2015; Renaud, 2009b) who designed it based on previous studies in order to provide in an-depth understanding about students' views about the selected pictures. During the design of the interface for this method, the researcher considered the following aspects in the design to insure high level of efficiency :







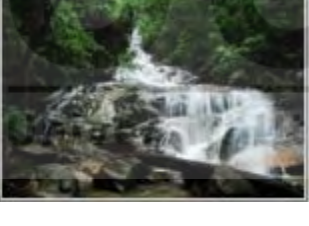





- i. **Selecting the secret pictures:** the selected participants were asked to choose only relevant 4 pictures in accordance to the challenge set they decide for each selection. This number of pictures is used by most RBGP schemes and has at least the same security level as a 4 digit PIN depending on other design factors (Renaud, 2009b). The selected pictures were supplied from the 40 participants identified from the early chapter which were categorized into Malaysian and non-Malaysian students.
- ii. **Challenge set size:** A matrix of 4 x 4 (1 secret picture and 15 distractors) was designed in order to allow students to choose effectively. The design of this grid was determined when the researcher asked students to determine the appropriate number of attempts and pictures in a system.
- iii. **Picture size:** The size of the pictures was all set to the average size with the same height and width for all pictures. Next and previous buttons were used in order to allow the students to navigate between the attempts and to simplify the viewing process of pictures when registering for their GPs. (see Figure (5.1))



Figure 4.6 : : User interface for the first attempt

- iv. **Picture type:** The type of pictures for each attempt was categorized based on the previous recommendations addressed by some scholars in the literature. Therefore, the researcher used a grid of 4x4 16 pictures for each attempt (4 attempts). The challenge in this experiment was to find sets of pictures that represent different national cultures in order to use them for a more inclusive and flexible GP scheme, and the proposed solution involves using the culturally-familiar picture database for the scheme. For the participants, a grid of 16 pictures (4\*4) was presented in random sequential order to the participants, who were then asked to select four pictures that combined would serve as their GP. Table 5.1 shows how the chosen pictures of the scheme were related to their national context.

Table 4.1 : Familiar pictures based on the participants' preferences

Category	Malaysian	Other cultures
Foods and Drinks		
Animal and Plants		
Famous People		
Landscapes		
Buildings		
Traditions and History		

Religious Places		
Others		

#### 4.8 The Method of Experiment 2

In order to assess students' selection of the pictures from the designed system, the researcher divided participants into five groups (according to familiarity for their choice to the graphical passwords). The researcher requested from the students in each group to create a graphical password (GP) by choosing four pictures from a set of 64 pictures. The instructions for doing so along with a brief demonstration about their role in this study was explain to all the participants before starting to create their graphical passwords.

After finishing the experiment, the system stored all the selected pictures and related information from the participants' account which later used by the researcher in this study (see figure 5.2) in order to determine how much the familiarity culture affects the participant when it comes to choose familiar and unfamiliar pictures for creating their graphical passwords (GPs).





1	User ID	zaim
	Name	muhammadzaimtajuddinbindzulkepli
	Gender	male
	Age	18-25
	Email	zaimtajuddin_08@yahoo.com
	Academic degree	Bachelor
	No. of familiar question	4
	No. of un familiar question	0
2	User ID	zulkarnain
	Name	muhdzulkarnain
	Gender	male
	Age	18-25
	Email	dzul_94_10@yahoo.com
	Academic degree	Bachelor
	No. of familiar question	2
	No. of un familiar question	2

Figure 4.7 : Show the stored related information about the participants

#### 4.9 The Procedure of Experiment 2

On the first page of the web experiment, participants were given a brief introduction in English about the experiment and its aims. Then, they were asked to they were willing to participate or not. Participants who did not want to take part in the experiment we excluded from the experiment; the others who agree were directed to invite them to start the experiment. The participants were asked to register in the system and give a brief information about name, age academic degree and emails, then after filling the required information they asked to create username, in next page participants asked to press a “Create my graphical password” button to take them to the next page, which was the core of the experiment. That page displayed a grid of 16 pictures sequential allowing participants to select four pictures for their GP from it. Each time the participants selected a picture, it appeared at the bottom of the page

in order to confirm their choice. In the event that the participant did not like the choice, they had the ability to delete the selected picture and start again by pressing the “Delete” button on the page.

After four pictures were selected, a page display which contains a specific question “How do you categories the four pictures that have been chosen?” and down the question the participant had to give the specific number of familiar and unfamiliar pictures in order to know how much the culture affect the participant choice (see figure 5.3). After finished the required number and all related information the participant became active; participants pressed finished to send their information to the database and complete the experiment by taking them to the exit page.



Using Strong Passwords

How do you categorize the four pictures that you have chosen ?

				
No. of familiar images				3 ▼
No. of unfamiliar images				1 ▼

Submit Reset

Figure 4.8 : Show familiarity question

## 4.10 Results of the Experiment 2

The following sub-sections will present the results of experiment

### 4.10.1 Respondent Profile Appendix (B,C and D)

The population distribution of the respondents for the experiment was based on gender, academic degree, and age. This is holistically presented in appendix (D). For the gender distribution, out of the 30, 17 making 57% are females while 13 of 43% are the males. Figure 5.4 presents the gender distribution of the respondents.

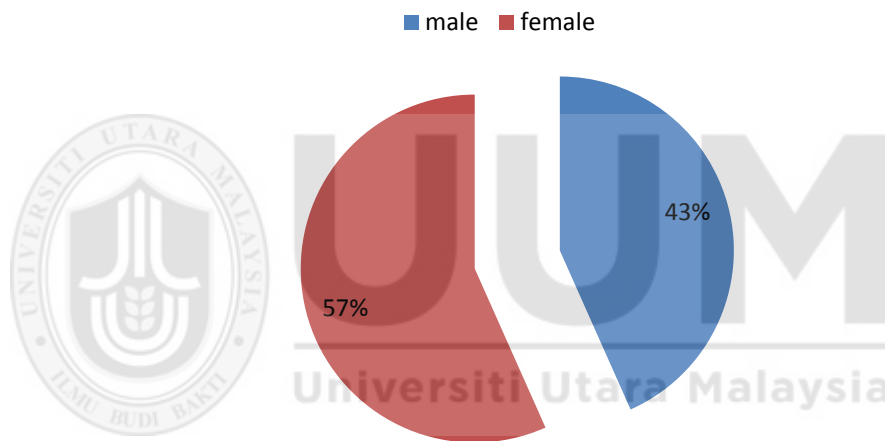


Figure 4.9 : The gender distribution of the respondents

To depict the academic degree of the respondents, the questionnaire administered inquires about the academic degree of the respondents. The respondents' degrees were exclusively drawn between undergraduate and postgraduate, the distribution shows that 24 making 80% were undergraduate students, while only 6 of 20% were postgraduate students. Figure 5.5 shows the academic degree distribution of the respondents.

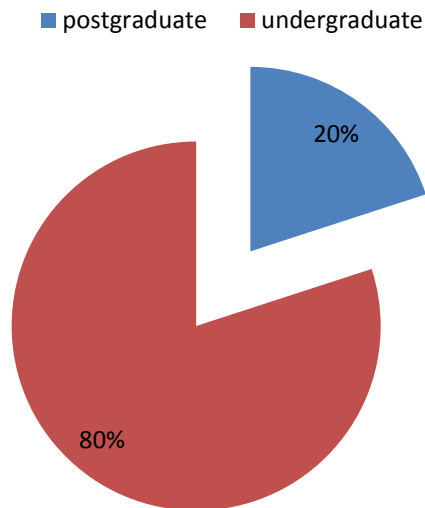


Figure 4.10 : The academic degree distribution of the respondents

The age distribution of the respondents is also reported. Out of the 30 respondents, 21 which is 70% were between 18-25 years old, 9 respondents which represent 30% were between 26-35 years old, no one was in between 36-45 years old or 45 years old and above. Figure 5.6 shows the age distribution of the respondents.

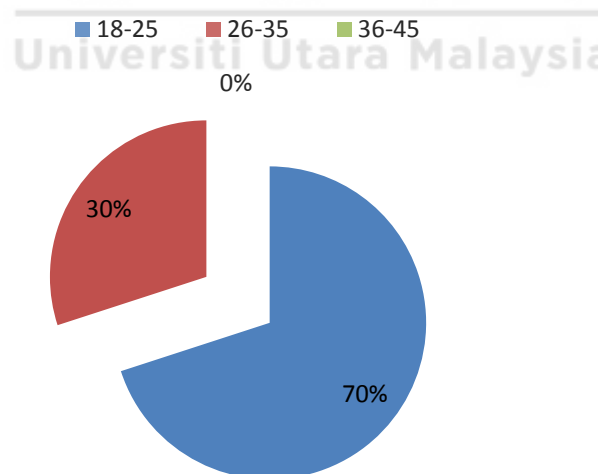


Figure 4.11 : The age distribution of the respondents

The questionnaire administered asked to enquire about the colleges and schools of the respondents. The profile different schools that the participant come from. Figure 5.7 shows the schools that the participants have belong to it.



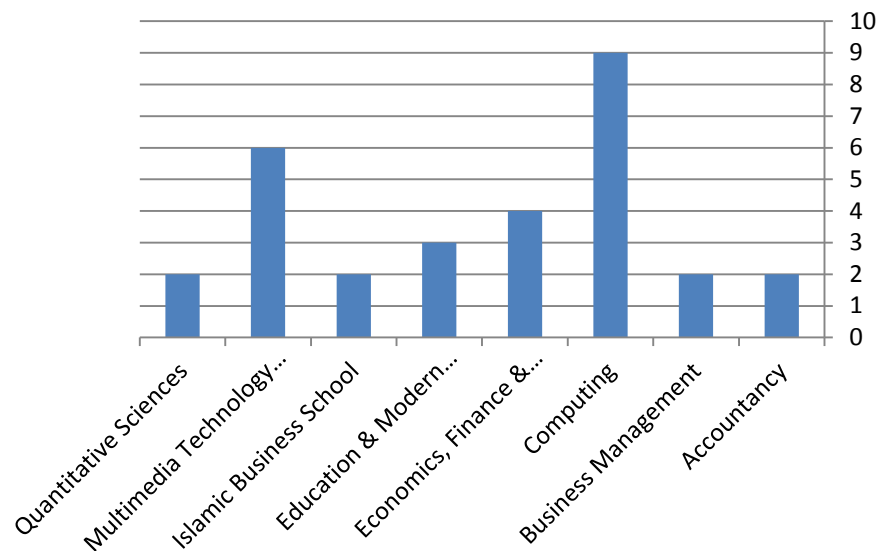


Figure 4.12 : Schools of the participant

#### 4.10.2 Number of Familiar Pictures Selected

Each participant chose four pictures as a GP. For the participant, the mean number of culture pictures selected for their GP was 2.7, (SD) = 1.24. Figure 5.8 shows the frequency of Malaysia pictures selected by participants for their GPs.

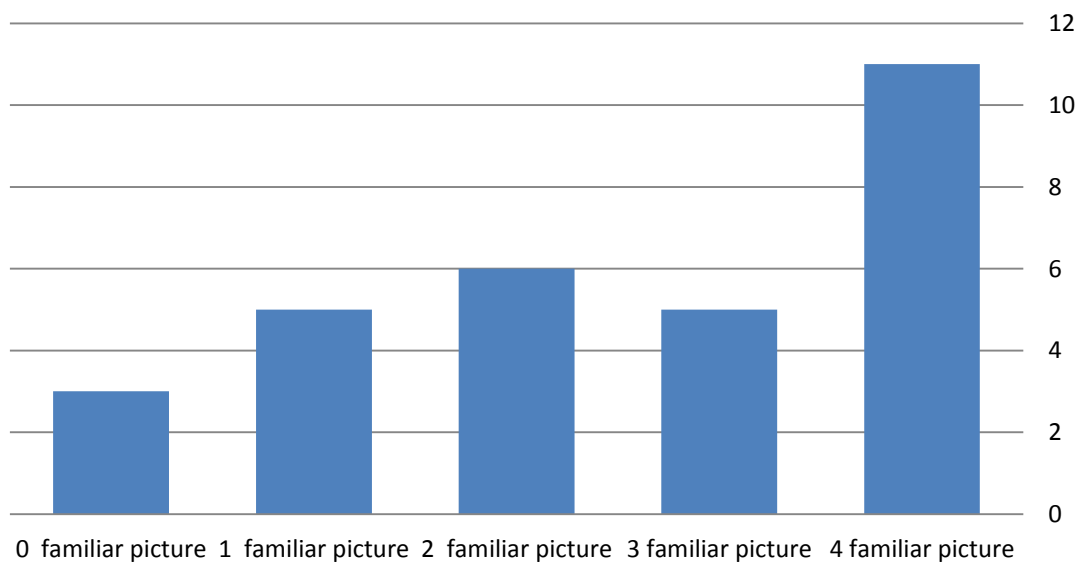


Figure 4.13 : Number of pictures selected from Malaysia culture for creating graphical passwords

The results show that culture affects the method of choosing GPs for participants, who had spent most of their lives in their designated country of culture. Figures 5.4 show that 60% of participants created their GP by choosing at least three pictures from their respective cultures. By contrast, only 10% of participants did not rely at all on culturally-familiar pictures, as they chose their GPs entirely from pictures that came from other countries.

#### **4.11 Discussion**

The principle consequence of this research is such as members were very influenced by their experience culture when they picked pictures for GPs. This impact was watched for members, matured 18-35. There is a relationship between a lifted selection of pictures provided by people from the national culture for GPs and countries that are higher in the vulnerability shirking measurement. Since the GP validation system was produced to secure individuals' data, individuals might be worried that they pick pictures for their passwords that they won't overlook, even with long stretches between utilization.

So as to accomplish a decent rate of memorability for those GPs, individuals vary in their sorts of GP picture decisions in view of their way of life. Individuals who originate from high vulnerability evasion societies have a tendency to maintain a strategic distance from pictures that don't have a place with their way of life, as they may feel that picking those photos would build the instability without bounds in the event that they couldn't recall their passwords.

These outcomes may recommend that both security and ease of use of the RBGP would be influenced. Security may be traded off by making a speculating assault hardly simpler by disregarding pictures that did not have a place with the user's way

of life and concentrating just on those that are outstanding in the user's nation. More research is expected to explore this probability.

For the convenience of RBGPs, it may be hard for individuals from high instability evasion nations to feel great with pictures that they see as remote to their societies. Thusly, picking an excessive number of such pictures for GP choice may influence the time and momentousness required to complete the verification procedure. This claim requires more research for conclusions to be proposed. Next part explores this question in more points of interest. One option that may fortify both the convenience and security of RBGPs is to constrain the photos from which a user picks her secret key pictures, so that users from high vulnerability shirking societies would pick just commonplace pictures that they connected with their own way of life. All things considered, knowing the person's nationality would not help any attacker to encourage their speculating assault. Moreover, both the time and momentousness required to experience the verification procedure would be enhanced as the GPs would be made from pictures that users discovered well known.

The fundamental motivation behind this study was to discover the guessability of socially well-known instead of socially new pictures regarding taught speculating assaults. The fundamental wellsprings of data were utilized depended on individual involvement with the casualties. Moreover, the guessability of socially recognizable pictures that were regularly picked by the users of the model was researched.

#### **4.12 Summary**

The first part of this chapter (Experiment 1) has shown the respondents' profile, population distribution and the procedure of creating the culturally-familiar picture database. This database was used to create a culturally-familiar graphical password

scheme that strives for high performance in terms of usability and security for users from Malaysia.

The central finding of second part (Experiment 2) was that participants were highly affected by their background culture when they chose pictures for GPs. the type of pictures used for GPs should be selected with careful consideration of the end users' background in order to improve the system's usability. Studying the specific cultural effects on different types of RBGP schemes is recommended in order to find out how to optimize the current GP schemes to make them more usable and secure. In general, people tend to choose pictures that represent their own cultures. The next step is to study the effect of cultural familiarity on the usability of GPs.



# **CHAPTER FIVE**

## **USER GUIDELINES BASED ON CULTURAL FAMILIARITY'S IMPACT ON THE SECURITY AND USABILITY OF RECOGNITION- BASED GRAPHICAL PASSWORDS**

### **5.1 Introduction**

This chapter is divided into three main parts the first one (Experiment 3) was focusing on security attack, in this chapter introduces a study that aims to find the security level of culturally-familiar and unfamiliar graphical passwords against one security attack in particular, the educated guessing attack. While the second part (Experiment 4) was about the role of culture familiarity in creating graphical password and its effects on the usability in terms of memorability, login time and satisfaction. Therefore, it is predicted that choosing GPs from pictures belonging to the users' culture will improve both memorability and login time. These pictures should look familiar and thus easier for the participants.

The third part (Experiment 5) addresses the users' guidelines in order to provide a secured and usable graphical password. The researcher in this study used a questionnaire in order to determine the participants' perception about certain security aspects related to graphical password. This is believed to provide the necessary information for providing a design recommendations to be used by system designers and developers of the graphical password.

## 5.2 Participants of Experiment

The overall number of participant in the experiment (Usability and Security) were (30), and the participant's profile according to their age, gender and academic degree were explain in the (5.6.1). The researcher employed a within-subject design in order to determine the overall success login, memorability and the success rate of guessing among attackers in the familiar culturally and unfamiliar culturally pictures.

The participant in the usability and security stages were divided according to the number of pictures familiarity in their graphical password which was done in the previous chapter. Table 6.1 shows the dividing of groups according to their choice for graphical password.

Table 5.1 : Number of participants for each group in the study

No.	Groups	Number of familiar picture in their graphical password	Number of participant in each group (percent)
1	Group (1)	4/4	12 (40%)
2	Group (2)	3/4	6 (20%)
3	Group (3)	2/4	5 (16.6%)
4	Group (4)	1/4	4 (13.3%)
5	Group (5)	0/4 (means all picture are not familiar)	3 (10%)

## 5.3 Reliability Test for Appendix (B,C and D)

After the main data is gathered, a construct reliability test is done. The main data reliability test is to confirm the consistency of the construct scale and compare with the results gathered from the pilot testing. This is essential to establish the reliability

of the study's instrument. Table 6.2 presents the verification –comparing the main with the pilot test results.

Table 5.2 : Comparing the main with the pilot test results

No	Variable	No. of Item	Pilot Test Cronbach's Alpha	Main Test Cronbach's Alpha
1	Usability	10	0.722	0.7
2	Security	6	0.781	0.792
3	Guideline	14	0.823	0.788

Assessing the table presented in 6.2 above with a comparative consideration to the values of Cronbach's Alpha generated for the pilot and main tests for each of the variables, it is observed that usability and guideline recorded a lower value to what is obtained during the pilot test. However, values obtained at both ends are still greater than 0.7 which suggest the consistency of the items and the construct.

#### 5.4 Security Evaluation ( Experiment 3 )

The previous study in the registration phase (Chapter 5) showed that users prefer to choose culturally-familiar pictures for their GPs. As was shown in the usability part, cultural familiarity with pictures can certainly improve RBGP usability, but its security could be adversely affected by cultural familiarity. This part consists on experimenting the security aspects from using cultural familiarity's pictures and its impact on RBGP.

##### 5.4.1 The Aim of Experiment 3

The main idea behind testing the security feature of the GP was to determine the threats of an outsiders to guess the GP created by the user. To do so, the researcher invited the participants to participate in a guess attack experiment in which a set of

questions were asked to indicate the security prospects from having one GP guessed by others such as relatives or friends.

The attack method used in this study named individualized educated guessing attack as recommended in the literature. This type of attack is typically carried out by people who know sensitive information about the user which may include relatives, friends, etc. This attack involves guessing one's GP by simply selecting pictures relevant to his/her preferences. Therefore, attackers who are knowledgeable about user may guess the combination of pictures used to construct the GP. The process can be explained using the following example, in the event the attacker know some information about user's favorite brand, he or she may simply select the picture combination that consists of any item related to that brand. Thus, it is important to test the proposed system for guessing attacks by individual with knowledge about the victims.

#### **5.4.2 Educated guessing attack**

This type of attack goes against knowledge-based authentication where the hacker attempts to guess a user's GP based on previously acquired personal information. According to Hayashi et al. (2011), the educated guessing attack may be divided into collective educated guess attacks and individualized educated guess attacks.

The collective educated guess attack utilizes information about a group of users to guess their GPs. For example, if the attacker knows that most of the users are keen on cars, then they will select any picture of a car in the challenge set. This form of attack was previously discussed in terms of the RBGP (Davis et al., 2004).

The latter type of guessing attack according to Hayashi focuses mainly on using particular information about an individual user to guess the GP. The attacker tries to identify GP images that match the victim's personal information and interests. For



example, when an attacker knows that the victim supports the Manchester United football team, they will look for any image related to football in general or particularly Manchester United that are in the challenge set. . The effect of individualized educated guessing attacks on RBGPs was discussed in English (2012).

### **5.4.3 The Method of Experiment 3**

In order to examine the objective of this chapter, the same system was used as it consisted of culturally-familiar and unfamiliar pictures based on the users' backgrounds. The participants from the usability phase(victims) were asked to invite a few friends to play the attacker and try to guess their GPs. The attackers were of similar cultural heritage as the victims. This ensured that the attackers would have a rough idea about the main features of the victims culture and have a better chance at guessing which image would be more preferred and popular.

Each attacker also had a different type of relationship with the user, ranging from family members to close friends. This factor was key in identifying the group of attackers that were best at guessing GPs. The attackers also used different sources of information to guess their targets GP. One can identify the ideal source of information for an individualized guessing attack by analyzing the number of correct guesses.

The attackers were given three attempts to find their targets' GP within four challenge sets, each one including a real target picture amongst fifteen decoys in a 4 by 4 grid. These images were randomly collected from various cultural pictures as well as from the victims' own culture. The same decoys were used for each of the attackers in order to maintain uniformity. Upon completion of the experiment, the

system stored the attackers selection which was later used by the researcher as explained in the section below (refer to Figure 6.1).

nurul fatahiyah / Attempt2			Match
			Match
			Not Match
			Not Match
Time	32.30/seconds		

Figure 5.1 : Shows the security attack similarity with GP

#### 5.4.4 The Design of Experiment 3

A within-subject design was used in this study. This design could give more accurate results as every participant tried to guess both GPs' conditions: culturally-familiar and culturally-unfamiliar. Based on the GPs created in the previous study in Chapter 5, every attacker faced one of the following GPs:

1. A GP consisting of four culturally-familiar picture only.
2. A GP consisting of three culturally-familiar pictures and one unfamiliar picture.
3. A GP consisting of two culturally-familiar pictures and two unfamiliar pictures.

4. A GP consisting of one culturally-familiar picture and three unfamiliar pictures.
5. A GP consisting of four unfamiliar pictures.

By the end of the study, A scores was calculated for each group. The guessing success rate (GSR) for culturally-familiar pictures, this score represents the average correct guesses of culturally-familiar pictures for the groups. It indicates the security level of culturally-familiar pictures against an educated guessing attack. The mechanism used for estimating the guessing success rate (GSF) :

$$\text{GSR} = \frac{\text{number of correct guess pictures in GP}}{\text{total numbers of picture of each group}} \times 100$$

Participants filled in a post-study questionnaire designed to obtain descriptive data about the methods that attackers used to guess their target GPs correctly. Information about the main source used for guessing each GP along with the reasons for selecting the pictures was obtained from each participant. A complete version of this questionnaire is presented in Appendix D.

#### **5.4.5 The Procedure of Experiment 3**

The same participants who created a GP with the system discussed in Chapter 5 were asked to join. They were then asked to extend the invitation to their friends and relatives as well.

On the first page of the system, the attackers were given general information regarding the system along with instructions and what was expected of them. In order to achieve optimum performance, the participants were given motivation by being promised a gift if they could correctly guess their targets GP on the first,

second, or third attempt only. Moreover, it was felt that this would encourage the attackers to be more focused during the experiment.

The attackers who consented in partaking in the study would press the “Start” button to proceed to the second page. Then, they were asked to enter the provided victim’s username. The attackers were required to go through four challenge sets, each consisting of one GP picture and 15 decoys. They were given three attempts to correctly guess their target’s GP by identifying the target picture in each set. Upon completing the challenge set, they were asked to fill up a post-task questionnaire regarding the source of information used in guessing the targets GP and why they selected those particular images.

#### **5.4.6 The Result of Experiment 3**

Although the main aim of this study was to compare the guessability between culturally familiar and unfamiliar pictures among groups, this particular section shows the guessability of the proposed system. This was to give a general idea about its security before moving on to the details of culturally-familiar and unfamiliar pictures.

The results showed that no one out of 30 attackers succeeded in finding their target GPs. This was to the limit number of attacker, but they can guessed a part of the GP in different ratio among groups.

The selected attackers were asked to guess the GP that consisted of both culturally familiar and unfamiliar pictures. The obtained result shown in Table 5.4 presents the GSR for attackers of culturally-familiar and unfamiliar pictures. The GSR result for familiar pictures as group 1, the overall GSR was 43.18% as compared to the GSR for unfamiliar pictures like group 5 was 8.1%. Based on this, it can be noted that

attackers were able to increase the guess rate when using familiar pictures than unfamiliar one. This indicate that there is a significant differences in the GSR or culturally familiar and culturally unfamiliar pictures among attackers.

Table 5.3 : GSR for culturally familiar and unfamiliar pictures

<b>Groups</b>	<b>Number of guessed pictures among group</b>	<b>GSR (%)</b>
Group 1	19 from 44 pictures	43.18%
Group 2	8 from 20 pictures	40%
Group 3	5 from 24 pictures	20.83%
Group 4	4 from 20 pictures	20%
Group 5	1 from 12 pictures	8.3%

#### 5.4.7 Post-questionnaire (Appendix C) Results for Experiment 3

The total number of attackers in this study was 30, 13 male and 17 female. They were either close friends / relative (60%) or friends (40%) of the victims (Figure 6.2). The total number of target GPs was 30, and most of them were partially guessed by attackers. The reason for using close friends / relative and friends as attackers is that they have some information about the victims' preferences that might help them in guessing the correct GPs. For education level, most of the attackers hold an undergraduate degree (80 %) as shown in Figure (6.3).

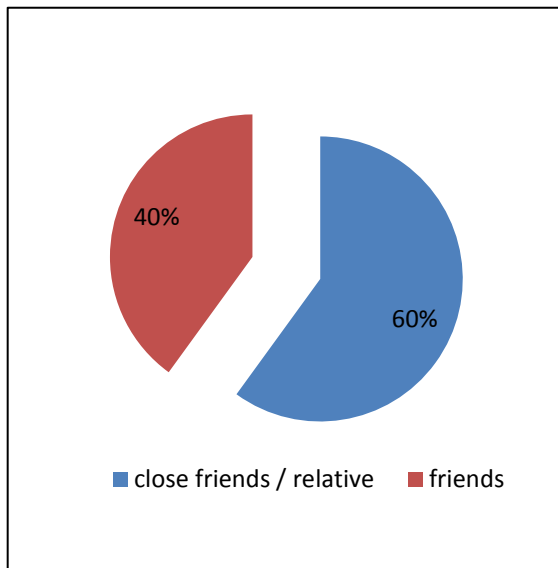


Figure 5.2 : Relationship with victims

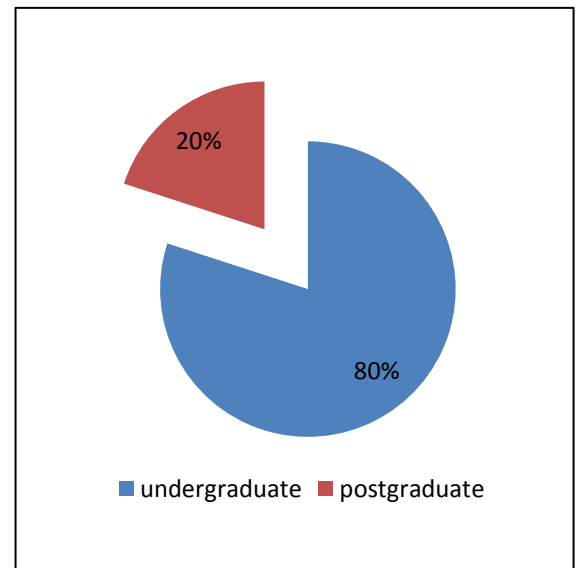


Figure 5.3 : Educational Background

While reasons behind guessing, The results showed that most of the attackers chose were based on guessing the pictures through knowledge of the users likes/dislikes (64%). Figure 6.8 shows that only a few attackers guessed their target's GPs based on guessing the images based on assumptions of what people in general might select (22%) or randomly guessing / repeated attempts (14%). By combining this result with the educated guessing attack findings, it appears that culturally familiar pictures that mainly represent users' likes/dislikes are vulnerable to educated guessing attacks.

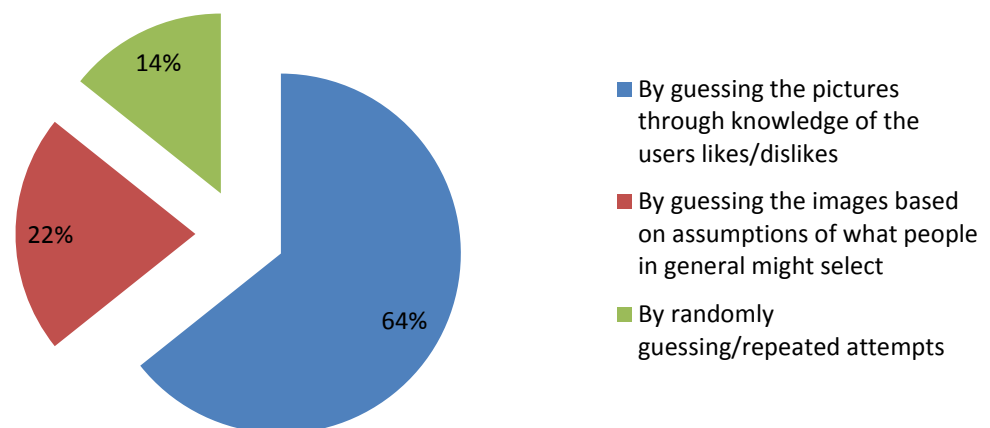


Figure 5.4 : Reasons behind guessing

#### **5.4.8 Discussion of Experiment 3**

The fundamental result was that attackers speculated their objective's natural pictures more than their new pictures. Well known pictures were those that originated from casualties' societies while new pictures were those that originated from different societies. The assailants who utilized victims' data additionally speculated their objectives' commonplace pictures more than new pictures. For the most chosen pictures in the framework, the outcomes indicated less demanding guessability over less-picked pictures.

The primary purpose for the security of new pictures is that they are not anticipated that would be decided for GPs. In actuality, users will probably make their GPs from commonplace pictures as was appeared in the past study sketched out in Chapter 5. The assailants would do a similar thing by utilizing the data they have about their victims and concentrating on the photos that will probably be well known to the victims. Despite the fact that it has preference regarding convenience as appeared in this part, well known pictures seem more powerless against instructed speculating assaults.

Frequently, socially well known pictures incorporate those photos that speak to the victims' advantages, propensities, or side interests. Data about those components can be known by relatives and companions. This is by all accounts the fundamental consider speculating well known pictures instead of new pictures for the assailants who had an association with the casualties or who utilized interpersonal organizations data. It appears that individuals can't practically control the measure of data they distribute over those applications, and at times informal communities turn into the fundamental wellspring of cooperation with other individuals. Additionally,

individuals may give more data about themselves on those applications than in up close and personal discussions (Tidwell and Walther, 2002).

It is imperative to discover proficient approaches to expand the security level of commonplace GPs in order to diminish the advantages of utilizing informal organizations for an informed speculating assault. One of the arrangements the recognition with the baits in the test set may enhance the security of well known pictures and make them as secure as new pictures. As such, having just natural imitations with the objective well known picture would make it harder to decide for a speculating aggressor since all photos will have a similar level of recognition to the casualties. This plan of the test set should be analyzed as far as both convenience and security all together enhance its proficiency.

For the most evident pictures, those picked by a large portion of the clients in the plan, it gives the idea that the model is not secure against an aggregate taught speculating assault. The high guessability rate for those photos instead of different pictures shows that attackers would require just study the general parts of the victim's way of life and focus on those photos that are frequently favored by individuals from that foundation.

This shortcoming is a genuine hazard for the model. One conceivable answer for it is to use more exertion into expelling evident pictures. The users ought to likewise be cautioned about the dangers of picking such evident pictures for their GPs, maybe at the enlistment organize through rules that plainly demonstrate the users which sorts of pictures must be stayed away from.



## **5.5 Usability Evaluation ( Experiment 4 )**

It is an evident from the literature that users who regularly use different passwords tend to forget about it after a period of time. This is because the characteristics of the password may not facilitate one's memorability. Therefore, it is assumed that creating GPs will help users to effectively memorize and reduce the number of failed attempts to access their accounts. The researcher's review of the literature also showed that when a user is familiar with the context of pictures such as culture, then it is believed that such familiarity would help them to memorize and lessen the login attempts required to access their accounts.

This part consists on examining the Cultural Familiarity's Impact on the usability of Recognition using the usability test and satisfaction questionnaire. The usability test consists of determining the number of successful attempts participants made to login to their account and the time consumed. Using the logs, the researcher was able to determine both attempts and the time required. Participants who were unable to correctly select the GP from the first attempt were asked to try again. During the experiment, participants were asked to start login to their accounts and after 24 hours as it was acknowledge in literature. This was essential to determine their ability to remember their GPs created during the registration stage.

### **5.5.1 The Method of Experiment 4**

In order to investigate research objective (3), the same RBGP scheme from the registration stage (Chapter 5) was used. The participants in the previous study were invited to participate. Those participants were divided into five groups based on the GPs they created in the previous study:

- i. Group 1: participants who have GPs consisting of four familiar pictures from their own culture;
- ii. Group 2: participants who have GPs consisting of three familiar pictures from their own culture and one unfamiliar picture from other cultures;
- iii. Group 3: participants who have GPs consisting of two familiar pictures each from their own and from other cultures;
- iv. Group 4: participants who have GPs consisting of one familiar picture from their own culture and three unfamiliar pictures from other cultures;
- v. Group 5: participants who have GPs consisting of four unfamiliar pictures from other cultures.

Each participant was asked to log in to the RBGP scheme. The login process consisted of four challenge sets. The aim of this procedure was to analysis the successful and failed logins and the time required to complete the authentication process for all five groups.

#### **5.5.2 The Procedure of Experiment 4**

All participants from the previous chapter were requested to further be a part of the second experiment in order to indicate the memorability, login time, and their satisfaction of using GPs based on the login success rate. Before starting, the participants were given a brief glance into the experiment and their respective roles were explained. Afterwards, the participants were asked to log in to the system in order to enter their account.

Those who consented to taking part in the study were directed to the first page, which served as the first step of the authentication process. They were then asked to enter the email that they had used in the registration stage of the first

study (Chapter 5) and were directed to the first challenge set in the login process. The database registered the time at which the login process was initiated. The participants were required to identify their four target pictures from four challenge sets; each containing only one target picture. After completing the fourth challenge set, they were asked to press the “Done” button to signify the end of their authentication process. The four selected pictures were compared with the pre-stored GPs in the database. The time at which this stage was reached was recorded. If the login was successful, the participants were then directed to the exit page and all of their information was stored in the database. However, a failed login resulted in the participants returning to the first page in order to make another attempt. If they failed to login three times, the participants would finally be directed to the exit page and all their attempts would be stored in the database.

The time allotted between creating the password and re-logging was 24 hours. This period was agreed to be sufficient enough in previous studies like Komanduri and Hutchings (2008) and Stubblefield and Simon (2004) who acknowledged the potential of examining one’s memorability in different periods including 24 hours. From the cognitive part, Conway and Dewhurst (1995) stated that human ability in memorizing certain aspects related to past experiences can be gradually altered. They found that within 24 hours of carrying on certain experience, a human’s ability to remember starts to decrease. Based on these previous findings, the researcher deemed 24 hours to be sufficient enough in determining the suitability of the proposed GP.

### 5.5.3 Results of Experiment 4

#### 5.5.3.1 Login Success rates (Effectiveness)

As stated earlier, all the participants had to login using their email and GPs created from the previous chapter. The system was designed to allow only 3 login attempts. The experiment result in Table 6.4 showed that majority of the participants in different groups had a high success rate from the first attempt.

Table 5.4 : Login attempts among groups

Group No.	Success %	Fail %
Group 1	10 (90.90%)	1 (9.09%)
Group 2	5 (83.3%)	1 (16.6%)
Group 3	4 (80%)	1 (20%)
Group 4	3 (60%)	2 (40%)
Group 5	2 (66.66%)	1 (33.33%)

The result of the overall success login rate was 79.51%. A total of 60% were found to make it from the first attempt, 11% were needed twice attempt to login, and 8.51% were need three attempt to login to system. However, the overall rate for failed login for all the participants was 20.48%. Based on these results, it can be concluded that GPs based cultural picture increased students' familiarity with the pictures in which it also revealed a potential impact of on their memorability of GPs. Figure 6.2 shows the number of attempts for each group.

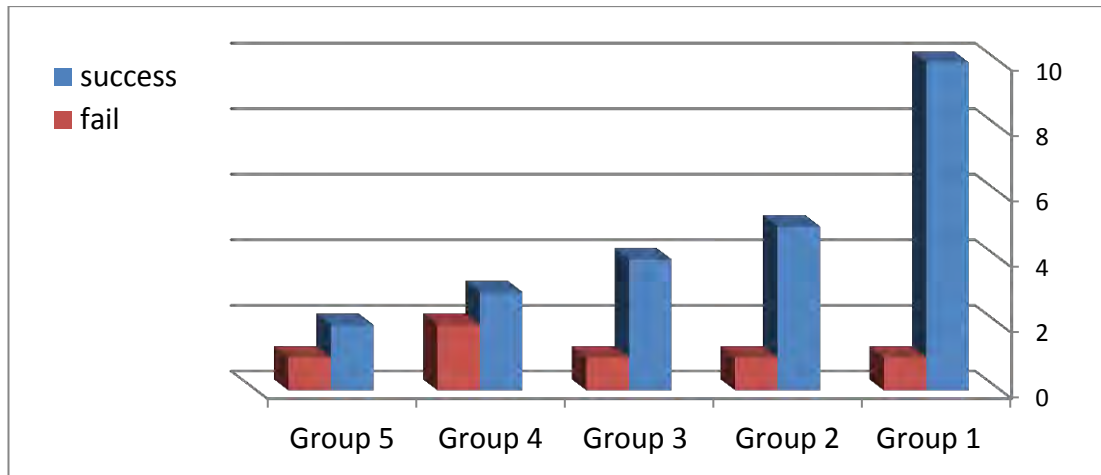


Figure 5.5 : Successful and failed login rate for each group

The login success rate (effectiveness): this score records the average successful login rate (*SR*) in every group, indicating memorability performance:

$$SR = \frac{\text{login success rates at training session} + \text{login success after 24 hour}}{2} \times 100$$

#### 5.5.3.2 Time required to log in (Efficiency)

The results showed that culture did not affect the time required to log in by using recognition based graphical password (RBGP). Figure 6.2 shows the mean number of the time required to log in by using the RBGP for every group in the study. The overall time required to log in for all groups was approximately 25 seconds.

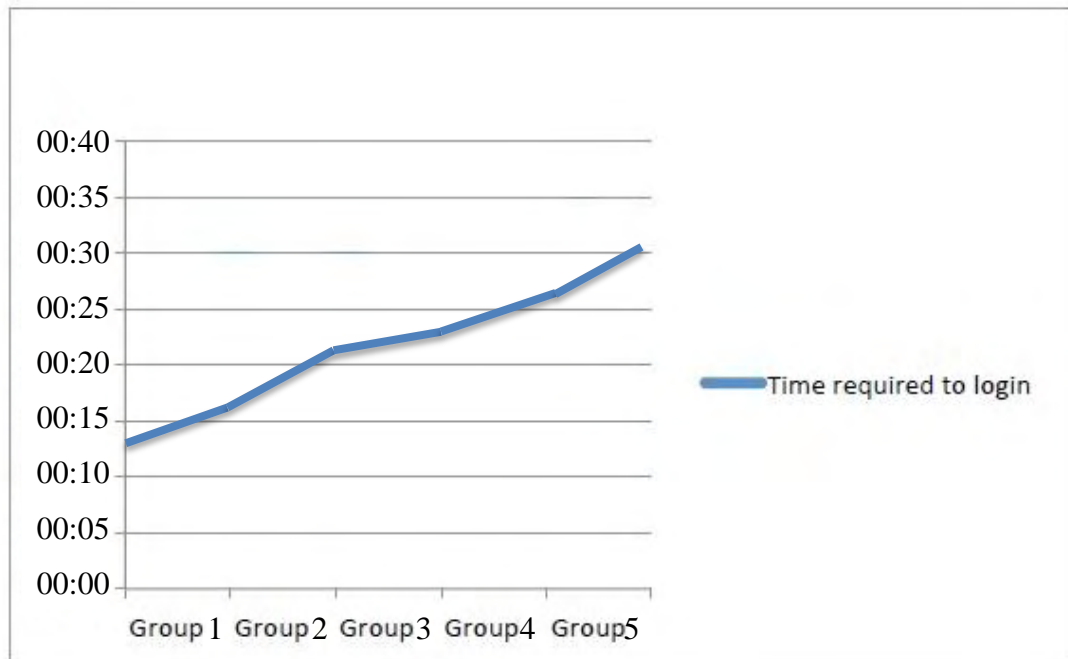


Figure 5.6 : Time to login in

The time required to log in (efficiency): this score records the average time required to finish the authentication process (TL), starting from the first challenge set until the end of the fourth challenge set

$$TL = \sum \text{login time} / n ; \text{ where } (n) \text{ represent the number of login in the groups}$$

### 5.5.3.3 Satisfaction

Satisfaction was one of the factor that the study focus on, Table 6.4 shows the results obtained from asking the participants to rate the system using the usability questionnaire provided to them after completing the login attempts. All the participants who redirected to the main page were asked to further undergo the usability evaluation of the system by distribute the questionnaire among them. A

total of 10 questions were provided scaled from 1 which indicate strongly disagree to 5 which indicate strongly agree.

From the result, it can be noticed that majority of the participants found the system to be flexible and they were motivated to use it frequently (Mean=4.10 and SD=0.60), functions in this system were well integrated (Mean=4.30 and SD=0.59), and learn to use this system very quickly (Mean=4.23 and SD=0.72). In addition, the participants felt that using the GPs in the proposed system made them feel confident (Mean=4.40 and SD=0.67).

Based on this, the overall reaction to the system was positive among the participants who had successful and failed login attempts. In addition, it is believed that the cultural picture was the main factor that improved students' perception about the system simplicity, ease of use and reliability.

Table 5.5 : Descriptive results for the usability test

Questions	N	Mean	Std. Deviation
Q1	30	4.1000	.60743
Q2	30	1.7333	.73968
Q3	30	3.9333	.63968
Q4	30	2.2667	.82768
Q5	30	4.3000	.59596
Q6	30	1.5333	.62881
Q7	30	4.2333	.72793
Q8	30	1.3667	.49013
Q9	30	4.4000	.67466
Q10	30	2.5667	.81720

#### 5.5.4 Discussion of Experiment 4

In terms of logging in, the main result was that the participants whose GPs consisted only of pictures belonging to their cultures had the highest successful login rate. This finding is likely due to the fact that these participants were more familiar with the

scenes in their GP images than any of the other groups, all of whom had chosen at least one culturally unfamiliar image. Therefore, people might recognize familiar pictures that come from their backgrounds more effectively than unfamiliar pictures that come from other cultures.

Regarding the time required to log in, the results showed some differences in the time required to complete the login process among all five groups. It is possible to say that the participants who create their GP based on familiar picture did not pay a lot of time to detect the GP. While the participants who depend on unfamiliar pictures in their GP need a little bit more time, it could be understood that the participant need more time to recognize their GP.

For the participant's satisfaction, it was clear to notice that the majority of participants were satisfy with the recognition based graphical password. Also for their motivation for using the system recorded high degree. It was believed that the cultural picture was the main factor that improved students' perception about the system simplicity, ease of use and reliability.

The study's results suggest that the type of pictures used for RBGPs could affect its usability, so pictures that meet the familiarity condition are likely to increase the memorability of GPs. Pictures belonging to a user's background would be suitable to form part of her GPs.



## 5.6 The Aim of Experiment 5

This part addresses the users' guidelines in order to provide a secured and usable graphical password. The researcher in this study used a questionnaire in order to determine the participants' perception about certain security aspects related to GP. This is believed to provide the necessary information for providing a design recommendations to be used by system designers and developers of the GP. The literature showed that a number of recommendations were proposed by various researchers to secure one's information by suggesting steps for users to follow when creating their passwords.

However, GP developers tend to follow certain schemes in order to determine the strengths and weakness of the proposed mechanism. De Angeli, Coventry, Johnson, and Renaud (2005) explained the needs for examining the feasibility of GPs when it comes to use or adapt it for the evaluation purposes. This include examining the main aspects related to the system usability and security. The literature showed that such recommendations can be used to construct a proper understanding of the user requirements in order to facilitate secure and better user experience. The researcher in this study considered the suggestions and recommendations from previous studies. This study followed the authentication steps suggested by De Angeli et al. (2005) to formulate the study's guidelines for secured GP. These are the same recommendations used by Aljahdali (2015) who also designed a GP and investigated its suitability based on the following recommendations:

- i. The method used for password authentication must be designed in accordance to the users' needs, background and the nature of the system.

- ii. Provide a different variety of colours, context, and clear pictures that can help user to recall the information embedded into the image easily.
- iii. Provide a customizable challenge for user to choose from, this include ensuring the following aspects:
  - Increase usability by providing the sort of display based on the semantic categories from those in the challenge set.
  - Increase the usability by providing the sort of display that visually-dissimilar distractors from those in the challenge set.
  - Increase the security by applying several categories in order to distract attackers from guessing the user GP.
- iv. It is believed that codes generated by the system may positively effect on the usability of the system.
- v. Keys displayed in fixed locations at each authentication attempt increase usability but decrease security.
- vi. It is recommended to provide a portfolio-based solutions by increasing guessability and decreasing observability.

## **5.7 The Method of Experiment 5**

In order to investigate research objective (4), A quantitative study was conducted after the experiment 3 and 4 were finished . The participants in the previous study were invited to participate. Each participant was asked to fill the questionnaire and to complete it. The questionnaire consisted of 14 questions. The aim of this method was to suggest guideline that can make the recognition based graphical passwords more secure and usable.

## **5.8 The Procedure of Experiment 5**

A questionnaire for determining users' preferences when they registered their GP was administered to all the participants (Appendix B). The same participants from the previous chapter were used (30 students) in order to fill up a set of 15 questions related to the construction of users' guidelines for usable GP. These questions were adapted from Aljahdali (2015). All the participants had been asked to indicate their agreement about these questions. All the participants responded to the questions accordingly and their responses were stored.

## **5.9 The Results of Experiment 5**

The obtained result shown in Table 7.1 was obtained from the 30 participants. It can be noticed that 76.66% of the participants have chosen familiar pictures for creating their graphical passwords (23 participants) while only 16.66% of them have chosen unfamiliar pictures which is somehow relevant to the claims made in the second part of chapter 5 when creating the categorization of the pictures. On the other hand, 70% of the users (21) have chosen pictures that are believed to improve their memorability. In addition, 66.66% of users stated that the selected pictures have direct relationship to them. Which indicate that users are more tending to select GP that consider it related to their background. This may include aspects related to food, clothes, etc. However, only 25% of those who answered no found the unfamiliar picture to improve their memorability.

The result also showed that 70% of the participants believed that the chosen pictures were famous and preferred by the general public in Malaysia. On the other hand, only 16.66% answered no in which 80% of them believed that such pictures will

improve their memory. The researcher also indicated that 58.55% of the users were focusing on the small details when creating the GP whereas only 26.66% were not paying much attention to the details. 15 out of 17 of those who focused on the details found this method to be useful in recognizing the GP. The result also showed that 56.66% of the participants were hesitating between two or more pictures in which 64.70% of them reasoned it to the difficulty in recognizing the image features. It was also found that 36.66% of the users were choosing the pictures based on sequential pattern while 56.66% were not doing so. Only 90.90% of those who followed a sequenced patterns found this method to be useful in recognizing GP.

As for comparing the pictures selected, the result showed that 50% of the users compared the GP with the decoys in the challenge sets in which 80% of them believed that such comparison is useful in the recognition stage. Finally, 30% of the users were found to have taken screen-sheet for their GP or save it by anyway. This may indicate that some users may still perceive GP to be difficult to remember after sometimes.

Table 5.6 : Agreement rate among participants when registered for GP

Questions		yes	no	not sure
1	Did you choose familiar pictures for your graphical password?	23	5	2
2	In you answered (yes), did the familiarity with those pictures improve your memory today?	21	1	1
3	During the registration, did you choose pictures that have direct relationship with you?	20	6	4
4	If you answered (no), do you think this type of pictures will improve your memory?	4	1	1
5	During the registration, did you choose pictures that are very famous and preferred by the general public in Malaysia?	21	5	4
6	If you answered (no), do you think this type of pictures will improve your memory?	4		1
7	During the registration, did you focus on the small details of the pictures of your graphical password?	17	8	5

8	If you answered (yes), was this way useful in recognizing your graphical password today?	15		2
9	During the registration, did you hesitate between two or more pictures?	17	8	5
10	If you answered (yes), did this hesitation cause you difficulty at the recognition stage?	11	3	3
11	During the registration, did you select your pictures based on sequential pattern? For example, did you make a short story of your graphical passwords?	11	17	2
12	If you answered (yes), was this way useful in recognizing your graphical password today?	10	1	
13	Did you compare your graphical passwords with the decoys in the challenge sets? Did you find that your pictures are better than the decoys?	15	8	7
14	If you answered (yes) was this comparison useful as the recognition stage today?	12	1	2

Based on the result stated earlier, it can be concluded that creating GP depends on many aspects that corresponds to the user preferences for choosing and processing pictures in the challenge set.

The guidelines originated from these answers are formulated into the following points:

1. Try to select the pictures that are relevant to your context.
2. Choose pictures with less association to popular aspects in your culture.
3. Do not use pictures that are well-known due to its popularity.
4. Do not let the characteristics of a picture drive your choice.
5. Do not rush when choosing a picture so that you do not need to spend high cognitive load when trying to memorize it.
6. Consider following a sequences pattern that can help you decide and recall any GP.
7. Use set of pictures that are different from one challenge set to another.
8. Do not use pictures that are not within the mental model of yours.

## 5.10 Summary

The main result of this chapter for the part one was that the memorability rate for GPs consisting only of pictures belonging to participants' backgrounds was higher than the memorability rate that do not meet that criterion. This difference was expected due to the fact that people can recognize culturally-familiar pictures more easily than unfamiliar pictures. Additionally, there was no evidence that the participants who had GPs consisting only of pictures from their own backgrounds will spend less time logging in than those with only some such images or no culturally-familiar images.

The second part was about the effects of choosing familiar pictures for the GP against the educated guessing attack, the GSR for the groups were highly guessed for the group who they depend on familiar picture, in contrast the group who depend on unfamiliar picture was the lowest GSR which mean have more secure against an educated guessing attack.

While the last part was about deriving guidelines based on the results of the last both experiment and also based on questionnaire in order to determine the participants perception about certain security aspects related to GP. The suggested guidelines can be used to construct a proper understanding of the user requirements in order to facilitate secure and better user experience.

## CHAPTER SIX

### CONCLUSION AND FUTURE WORKS

#### 6.1 Introduction

This chapter introduced the conclusion and future works based on the results obtained from this study. The researcher found that GP based on the cultural properties of the users can offer a flexible way for securing the personal information and provide an easy to remember method. The researcher was able to obtain a set of pictures that were used to design the proposed system from 200 pictures. Then, these pictures were categorized into familiar and unfamiliar categories. These two categories were investigated further by the researcher in which the result led us to a set of pictures. The researcher also examined the users' memorability and usability from using these pictures to login to their accounts. After all, an examination of the users' preferences to the challenge sets used in the system to create the GP was carried out. The researcher found a set of guidelines to be used by GP developers when designing and developing system that consists on GP schemes. The feasibility of using these guidelines are yet to be investigated which can be extended to include other non-cultural aspects in accordance to the context of use.

The researcher believed that familiarly cultural GP can be used effectively in system that demand less cognitive load for user to easily memorize their selections. In addition, providing a set of challenges to guess the password combination adds an extra advantages to the current schemes by allowing users to choose from multiple items to construct certain patterns. These patterns can be used later for other purposes.

## 6.2 Discussion

This study provided a set of recommendations that can be used in order to design a proper GP based on the culturally pictures extracted from users in Malaysia. The result found that pictures for any culture can be divided into familiar and non-familiar culturally pictures in which the featuring of these pictures can be relevant to users' background. Previous studies like Davis, Monroe, and Reiter (2004) supported this by finding by asserting that GP schemes require a different posture toward password selection than text passwords. In addition, Wiedenbeck, Waters, Sobrado, and Birget (2006) also added that novice users are able to enter their GPs accurately and to remember it over time, which led to one conclusion that GP enriched by the context in which the user lives in can serve as an easier way for creating a password. These thoughts are relevant to the outcomes of this study which found that users who used culturally familiar pictures tends to remember the password with less time. This can be explained by the assentation made by Dunphy and Yan (2007) who stated that GP provide a better way for creating password for those who prefer visual aspects on textual one.

On the other hand, the main guidelines found in this study consists of providing an in-depth understanding of the method for designing password authentication with regards to the users' needs, background and the nature of the system. This is somehow relevant to Jali, Furnell and Dowland (2011) who addressed the needs for linking password authentication to users' preferences. This study also found that allowing users to create a GP that contain different variety of colours, context, and clear pictures would improve their recalling of the graphical elements as recommended by Renaud (2009). On the other hand, the researcher found that when



users used the proposed cultural GP, they were more intended to be involved in a security challenge that include sort of display based on the semantic categories that contain visually-dissimilar distractors. This finding provide some new insights to previous studies on GP development like Vu et al. (2007) who highlighted the needs for proper settings for users to engage in a security challenge. Moreover, the researcher found that when the GP display the keys in fixed locations at each authentication, then users will be able to easily recall and recognize the graphical elements. Users can also benefit from the use of portfolio-based by increasing guessability and decreasing observability as highlighted by Eljetlawi (2010).

This study also provide a clear indication about the choice of a user when it comes to use culturally familiar pictures from culturally unfamiliar pictures by examining the guessing success rate among different users. It was found that attackers tend to guess the familiar pictures better than the unfamiliar one, which can be reasoned to the probability of having the victim preferring pictures with easy, popular, and clear indications. This was explained by Nali and Thorpe (2004) as the possibility a user may have when determining the predictable characteristics for creating the GP. Such mechanism may results in a couple of recall-based properties which require “exact repetition” of pictures that shares similar or relevant patterns. As such, users who use such schemes may find themselves unable to establish the pattern for selecting the type of pictures that are favoured by their cultural properties.

### **6.3 Research Contributions**

The main contrition of this study is providing an effective cultural-based mechanism for graphical password in Malaysian context. The second thing is that analysis of the effect of cultural familiarity on users’ choice for GPs. This research is giving an

analysis of the effect of cultural familiarity on both the security and usability of RBGPs, and proposed guidelines can improve the memorability of a graphical password system as well as decrease the risk of educated guess ability attacks against a graphical password system.

#### **6.4 Limitations of the Study**

Few limitations can be addressed so far in this study. For example, this study was limited to only 30 students who were chosen from one university. The study was also limited to a certain culture with no consideration of participants from other cultures. In addition, the study did not perform cognitive ability test from using GP due to the time limit and complexity in doing so. Moreover, the researcher was limited to a set of questions to determine the users' guidelines for usable GP.

#### **6.5 Future work**

Based on the mentioned limitations, the researcher propose the following to be carried by the future studies:

1. Consider larger sample size for evaluating the culturally familiar picture vs culturally unfamiliar one.
2. Provide a wider selection of pictures that can represent more than one culture in order to decrease the guessing rate of attackers when trying to guess the victims passwords.
3. Conduct a focused group interview in order to determine an in-depth understanding of the guidelines needed to construct a usable GP.

## REFERENCES

- Adebola, Obasan, Owohunwa, Patrick, & Sikiru, Abdulazeez. GRAPHICAL PASSWORD AUTHENTICATION METHODS IN INFORMATION SECURITY. *Journal of Physical Science and Innovation*, 6(2), 2014.
- Aljahdali, Hani Moaiteq, & Poet, Ron. (2014a). Challenge Set Designs and User Guidelines for Usable and Secured Recognition-Based Graphical Passwords. Paper presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on.
- Aljahdali, Hani Moaiteq, & Poet, Ron. (2014b). Educated Guessing Attacks on Culturally Familiar Graphical Passwords Using Personal Information on Social Networks. Paper presented at the Proceedings of the 7th International Conference on Security of Information and Networks.
- Aljahdali, Hani Moaiteq, & Poet, Ron. (2014c). Users' Perceptions of Recognition-Based Graphical Passwords: A Qualitative Study on Culturally Familiar Graphical Passwords. Paper presented at the Proceedings of the 7th International Conference on Security of Information and Networks.
- Almuairfi, Sadiq, Veeraraghavan, Prakash, & Chilamkurti, Naveen. (2013). A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. *Mathematical and Computer Modelling*, 58(1), 108-116.
- Ávila, Ismael, Menezes, Ewerton, & Braga, Alexandre Melo. (2013). Strategy to Support the Memorization of Iconic Passwords. *Emerging Research and Trends in Interactivity and the Human-Computer Interface*, 239.
- Baddeley, Alan D. (1997). *Human memory: Theory and practice*: Psychology Press.
- Bellare, Mihir, Ristenpart, Thomas, & Tessaro, Stefano. (2012). Multi-instance security and its application to password-based cryptography *Advances in Cryptology—CRYPTO 2012* (pp. 312-329): Springer.
- Biddle, R, Chiasson, S, & Oorschot, PCv. *Graphical Passwords: Learning from the First Generation*. 2009: Ottawa: Canada.
- Biddle, R, Chiasson, S, & van Oorschot, P. (2010). Graphical passwords: Learning from the first twelve years, in *ACM Computing Surveys*. Carleton Univ.
- Biddle, Robert, Chiasson, Sonia, & Van Oorschot, Paul C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4), 19.
- Brooke, J. 1996. SUS—A quick and dirty usability scale. *Usability Evaluation in Industry*.

- Brostoff, Sacha, & Sasse, M Angela. (2000). Are Passfaces more usable than passwords? A field trial investigation *People and Computers XIV—Usability or Else!* (pp. 405-424): Springer.
- Catuogno, Luigi, & Galdi, Clemente. (2014). Analysis of a two-factor graphical password scheme. *International Journal of Information Security*, 13(5), 421-437.
- Cavalcante, Rodolfo Carneiro, Bittencourt, Ig Ibert, da Silva, Alan Pedro, Silva, Marlos, Costa, Evandro, & Santos, Robério. (2012). A survey of security in multi-agent systems. *Expert Systems with Applications*, 39(5), 4835-4846.
- Chang, Ting-Yi, Tsai, Cheng-Jung, & Lin, Jyun-Hao. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software*, 85(5), 1157-1165.
- Chaturvedi, Smita, & Sharma, Rekha. (2015). Securing Text & Image Password Using the Combinations of Persuasive Cued Click Points with Improved Advanced Encryption Standard. *Procedia Computer Science*, 45, 418-427.
- Checkoway, Harvey, Pearce, Neil, & Kriebel, David. (2004). *Research methods in occupational epidemiology* (Vol. 34): Oxford University Press.
- Chin, John P, Diehl, Virginia A, & Norman, Kent L. (1988). Development of an instrument measuring user satisfaction of the human-computer interface. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.
- Chowdhury, Soumyadeb. (2015). Exploring the memorability of multiple recognition-based graphical passwords and their resistance to guessability attacks. University of Glasgow.
- Chowdhury, Soumyadeb, Poet, Ron, & Mackenzie, Lewis. (2013). A comprehensive study of the usability of multiple graphical passwords *Human-Computer Interaction—INTERACT 2013* (pp. 424-441): Springer.
- Colella, Antonio, & Colombini, Clara. (2012). Security paradigm in ubiquitous computing. Paper presented at the Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on.
- Conway, Martin A, & Dewhurst, Stephen A. (1995). The self and recollective experience. *Applied Cognitive Psychology*, 9(1), 1-19.
- Cranor, Lorrie Faith, & Garfinkel, Simson. (2005). *Security and usability: designing secure systems that people can use*: " O'Reilly Media, Inc."
- Davis, Darren, Monroe, Fabian, & Reiter, Michael K. (2004). On User Choice in Graphical Password Schemes. Paper presented at the USENIX Security Symposium.

- De Angeli, A. et al. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*. 63(1-2).
- Dhanake, Mr Sagar A, Korade, Mr Umesh M, Shitole, Mr Chetan P, Kedar, Mr Sagar B, & Lomte, VM. (2014). Authentication Scheme for Session Password using matrix Colour and Text: IOSR-JCE/ISSN.
- Duggan, Geoffrey B, Johnson, Hilary, & Grawemeyer, Beate. (2012). Rational security: Modelling everyday password use. *International journal of human-computer studies*, 70(6), 415-431.
- Dunphy, Paul, Nicholson, James, & Olivier, Patrick. (2008). Securing passfaces for description. Paper presented at the Proceedings of the 4th symposium on Usable privacy and security.
- Eckhardt, Giana. (2002). Culture's consequences: Comparing values, behaviors, institutions and organisations across nations. *Australian journal of management*, 27(1), 89-94.
- Einwohner, R. L., Hollander, J. A., & Olson, T. 2000. ENGENDERING SOCIAL MOVEMENTS Cultural Images and Movement Dynamics. *Gender & Society*, 14(5)
- Eljetlawi, Ali Mohamed. (2008). Study and develop a new graphical password system. Universiti Teknologi Malaysia, Faculty of Computer Science and Information System.
- English, Rosanne. (2012). Modelling the security of recognition-based graphical password schemes. University of Glasgow.
- Ford, Gabrielle, Kotzè, Paula, & Marcus, Aaron. (2005). Cultural dimensions: Who is stereotyping whom. *Internationalization, Online Communities and Social Computing: Design and Evaluation*, 10, 1-10.
- Forsberg, Kevin, & Mooz, Harold. (1991). The relationship of system engineering to the project cycle. Paper presented at the INCOSE International Symposium.
- Frøkjær, E. et al. 2000. Measuring usability: are effectiveness, efficiency, and satisfaction really correlated? In *Proceedings of the SIGCHI conference on human factors in computing systems*.
- Fulkar, Ashwini, Sawla, Suchita, Khan, Zubin, & Solanki, Sarang. (2012). A study of graphical passwords and various graphical password authentication schemes. *World*, 1(1), 04-08.
- Gao, Haichang, Ren, Zhongjie, Chang, Xiuling, Liu, Xiyang, & Aickelin, Uwe. (2010). A new graphical password scheme resistant to shoulder-surfing. Paper presented at the Cyberworlds (CW), 2010 International Conference on.

- Gasti, Paolo, & Rasmussen, Kasper B. (2012). On the security of password manager database formats Computer Security–ESORICS 2012 (pp. 770-787): Springer.
- Gurav, Shraddha M, Gawade, Leena S, Rane, Prathamey K, & Khochare, Nilesh R. (2014). Graphical password authentication: Cloud securing scheme. Paper presented at the Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on.
- Hart, S. G. and Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. *Advances in Psychology*.
- Herley, Cormac, Oorschot, PC, & Patrick, Andrew S. (2009). Passwords: If We're So Smart, Why Are We Still Using Them?, *Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers: Springer-Verlag, Berlin, Heidelberg*.
- Hlywa, Max, Biddle, Robert, & Patrick, Andrew S. (2011). Facing the facts about image type in recognition-based graphical passwords. Paper presented at the Proceedings of the 27th Annual Computer Security Applications Conference.
- Hong, Dawei, Man, Shushuang, Hawes, Barbra, & Matthews, Manton M. (2004). A Graphical Password Scheme Strongly Resistant to Spyware. Paper presented at the Security and Management.
- Hofstede, G. 2001. *Culture's consequences: Comparing values, behaviours, institutions, and organizations across nations*. 2nd ed. Thousand Oaks, CA: Sage.
- Hui, Liew Tze, Bashier, Housam Khalifa, Hoe, Lau Siong, Michael, Goh Kah Ong, & Kwee, Wee Kouk. (2014). Conceptual framework for high-end graphical password. Paper presented at the Information and Communication Technology (ICoICT), 2014 2nd International Conference on.
- Jain, Anil, Bolle, Ruud, & Pankanti, Sharath. (2006). *Biometrics: personal identification in networked society* (Vol. 479): Springer Science & Business Media.
- Jiao, K. 2008. The influence of the cultural differences between the UK and Taiwan on Kellogg's international marketing strategies. MA thesis, Bournemouth University
- Jali, Mohd, Furnell, Steven, & Dowland, Paul. (2011). Quantifying the effect of graphical password guidelines for better security Future Challenges in Security and Privacy for Academia and Industry (pp. 80-91): Springer.
- Janakiraman, Siva, Thenmozhi, K, Rayappan, John Bosco Balaguru, & Amirtharajan, Rengarajan. (2014). Graphical Password Authentication

- Scheme for Embedded Platform. *Journal of Artificial Intelligence*, 7(4), 161-171.
- Jansen, Wayne. (2004). Authenticating mobile device users through image selection. *The Internet Society: Advances in Learning, Commerce and Security*, 1, 183-194.
- Jebriel, Salem, & Poet, Ron. (2014). Automatic registration of user drawn graphical passwords. Paper presented at the Computer Science and Information Technology (CSIT), 2014 6th International Conference on.
- Jermyn, Ian, Mayer, Alain J, Monrose, Fabian, Reiter, Michael K, & Rubin, Aviel D. (1999). The Design and Analysis of Graphical Passwords. Paper presented at the Usenix Security.
- Johnson, Margaret L. (2004). Biometrics and the threat to civil liberties. *Computer*, 37(4), 90-92.
- Jusdanis, G. 2011. The necessary nation. Princeton University press.
- Kawagoe, Kyoji, Sakaguchi, Shinichi, Sakon, Yuki, & Huang, Hung-Hsuan. (2012). Tag association based graphical password using image feature matching. Paper presented at the Database Systems for Advanced Applications.
- Kawale, Nilesh, & Patil, Shubhangi. (2014). A Recognition Based Graphical Password System. *International Journal of Current Engineering and Technology*, 4(2).
- Khanh Dang, Tran, & Tri Dang, Tran. (2013). A survey on security visualization techniques for web information systems. *International Journal of Web Information Systems*, 9(1), 6-31.
- Khodadadi, Touraj, Alizadeh, Mojtaba, Gholizadeh, Somayyeh, Zamani, Mazdak, & Darvishi, Mahdi. (2015). Security Analysis Method of Recognition-Based Graphical Password. *Jurnal Teknologi*, 72(5).
- Khot, Rohit Ashok, Kumaraguru, Ponnurangam, & Srinathan, Kannan. (2012). WYSWYE: shoulder surfing defense for recognition based graphical passwords. Paper presented at the Proceedings of the 24th Australian Computer-Human Interaction Conference.
- Kitayama, Shinobu, Duffy, Sean, Kawamura, Tadashi, & Larsen, Jeff T. (2003). Perceiving an object and its context in different cultures A cultural look at new look. *Psychological Science*, 14(3), 201-206.
- Komanduri, Saranga, & Hutchings, Dugald R. (2008). Order and entropy in picture passwords. Paper presented at the Proceedings of graphics interface 2008.
- Kronenfeld, David B, Bennardo, Giovanni, de Munck, Victor C, & Fischer, Michael D. (2011). A companion to cognitive anthropology: John Wiley & Sons.

- Ku, Yunlim, Choi, Okkyung, Kim, Kangseok, Shon, Taeshik, Hong, Manpyo, Yeh, Hongjin, & Kim, Jai-Hoon. (2012). Extended OTP mechanism based on graphical password method Future Information Technology, Application, and Service (pp. 203-212): Springer.
- Kumari, Swati, & Oberoi, Ruhi Kaur. Defense against Shoulder Surfing Attack for Recognition Based Graphical Password.
- Lashkari, Arash Habibi, Manaf, Azizah Abdul, & Masrom, Maslin. (2011). A Secure Recognition Based Graphical Password by Watermarking. Paper presented at the Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on.
- Lashkari, Arash Habibi, Manaf, Azizah Abdul, Masrom, Maslin, & Daud, Salwani Mohd. (2011). Security evaluation for graphical password Digital Information and Communication Technology and Its Applications (pp. 431-444): Springer.
- Lonner, Walter J, Berry, John W, & Hofstede, Geert H. (1980). Culture's Consequences: International Differences in Work-Related Values. University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship.
- Luvaas, Brent. (2013). DIY style: fashion, music and global digital cultures: A&C Black.
- Mathur, P. N. 1978. Barriers to effective visual communication. Media Asia, 3
- Mayer, Richard E, & Moreno, Roxana. (2003). Nine ways to reduce cognitive load in multimedia learning. Educational psychologist, 38(1), 43-52.
- McCoy, Scott, Galletta, Dennis F, & King, William R. (2007). Applying TAM across cultures: the need for caution. European Journal of Information Systems, 16(1), 81-90.
- Mihajlov, Martin, & Jerman-Blažič, Borka. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. Interacting with Computers, 23(6), 582-593.
- Mihajlov, Martin, Jerman-Blažič, Borka, & Ilievski, Marko. (2011). Recognition-Based Graphical Authentication with Single-Object Images. Paper presented at the Developments in E-systems Engineering (DeSE), 2011.
- Miller, S. (2006). Experimental Design & Statistics: New Essential Psychology : Routledge, 2 vol. 1.
- Monrose, Fabian, & Reiter, Michael K. (2005). Graphical passwords. Security and Usability, 147-164.



- Nicholson, James, Dunphy, Paul, Coventry, Lynne, Briggs, Pamela, & Olivier, Patrick. (2012). A security assessment of tiles: a new portfolio-based graphical authentication system. Paper presented at the CHI'12 Extended Abstracts on Human Factors in Computing Systems.
- Nisbett, Richard E, & Miyamoto, Yuri. (2005). The influence of culture: holistic versus analytic perception. *Trends in cognitive sciences*, 9(10), 467-473.
- Nisbett, Richard E, Peng, Kaiping, Choi, Incheol, & Norenzayan, Ara. (2001). Culture and systems of thought: holistic versus analytic cognition. *Psychological review*, 108(2), 291.
- Noiwan, Jantawan, & Norcio, Anthony F. (2006). Cultural differences on attention and perceived usability: Investigating color combinations of animated graphics. *International journal of Human-computer studies*, 64(2), 103-122
- O'Sullivan, E, Rassel, GR, & Berner, M. (2003). *Research Methods for Public Administrators*. Addison Westely Longman: Inc.
- Olukayode, Obasan Adebola, Ithnin, Norafida, & Ogunnusi, Olumide Siemeon (2014). Memorability Rates of Graphical Password schemes. *Journal of Theoretical & Applied Information Technology*, 66(1).
- Parkin, Alan J. (1993). *Memory: Phenomena, experiment and theory*: Psychology Press.
- Perrig, Adrian. (2000). Shortcomings of password-based authentication: September.
- Pettersson, R. 1982. Cultural differences in the perception of image and color in pictures. *Educational technology research and development*, 30(1),
- Ploehn, Cathryn A, & Greene, Kristen K. (2015). *The Authentication Equation: A Tool to Visualize the Convergence of Security and Usability of Text-Based Passwords Human Aspects of Information Security, Privacy, and Trust* (pp. 95-106): Springer.
- Poet, Ron, & Renaud, Karen. (2009). An algorithm for automatically choosing distractors for recognition based authentication using minimal image types. *Ergonomics Open Journal*, 2, 178-184.
- Prasad, PESN Krishna, Prasad, BDCN, Chakravarthy, ASN, & Avadhani, PS. (2012). Password Authentication using Context-Sensitive Associative Memory Neural Networks: A Novel Approach *Advances in Computer Science and Information Technology*. Computer Science and Engineering (pp. 454-468): Springer.
- Prasanth, N Narayanan, Azarudeen, K, Kabeer, M Gulam Ahamed, & Mohamed, J Gulam Peer. (2014). Enhanced Graphical Password Based Authentication Using Persuasive Cued Click-Points. *i-Manager's Journal on Software Engineering*, 8(3), 26.

- Qingxue, Liu. (2003). Understanding Different Cultural Patterns or Orientations Between East and West. *Investigationes Linguisticae*, 9.
- Raja, Kiran B, Raghavendra, R, Stokkenes, Martin, & Busch, Christoph. (2015). Multi-modal authentication system for smartphones using face, iris and periocular. Paper presented at the Biometrics (ICB), 2015 International Conference on.
- Raza, Mudassar, Iqbal, Muhammad, Sharif, Muhammad, & Haider, Waqas. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, 19(4), 439-444.
- Renaud, Karen. (2009a). On user involvement in production of images used in visual authentication. *Journal of Visual Languages & Computing*, 20(1), 1-15.
- Renaud, Karen. (2009b). Web authentication using Mikon images. Paper presented at the Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09. World Congress on.
- Renaud, K. 2009c. On user involvement in production of images used in visual authentication, *Journal of Visual Languages & Computing*, vol. 20
- Renaud, Karen, Mayer, Philip, Volkamer, Melanie, & Maguire, Joel. (2013). Are graphical authentication mechanisms as strong as passwords? Paper presented at the Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on.
- Roy, Jhulan, Barik, Mridul Sankar, & Mazumdar, Chandan. (2004). ESRML: a markup language for enterprise security requirement specification. Paper presented at the India Annual Conference, 2004. Proceedings of the IEEE INDICON 2004. First.
- Salim, Farzad, Reid, Jason, & Dawson, Ed. (2015). Authorization models for secure information sharing: A survey and research agenda. *The ISC International Journal of Information Security*, 2(2).
- Sarohi, Harsh Kumar, & Khan, Farhat Ullah. (2013). Graphical password authentication schemes: current status and key issues. *Int. J. Eng. Innovative Technol.(IJEIT)*, 10(2).
- Simon, M, K. (2011) . Dissertation and scholarly research : Recipes for success (2011 ed). Seattle, WA: Dissertation Success, LLC.
- Sobrado, Leonardo, & Birget, JC. (2004). Graphical Passwords. *The Rutgers Scholar: An Electronic Bulletin of Undergraduate Research*, Volume 4, 2002.
- Straub, Detmar, Keil, Mark, & Brenner, Walter. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & management*, 33(1), 1-11.

- Stubblefield, Adam, & Simon, Dan. (2004). Inkblot authentication. Microsoft Research.
- Sun, Hung-Min, Chen, Yao-Hsin, Fang, Chiung-Cheng, & Chang, Shih-Ying. (2012). PassMap: a map based graphical-password authentication system. Paper presented at the Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security.
- Suo, Xiaoyuan, Zhu, Ying, & Owen, G Scott. (2005). Graphical passwords: A survey. Paper presented at the Computer security applications conference, 21st annual.
- Suo, Xiaoyuan, Zhu, Ying, & Owen, G Scott. (2006). Analysis and design of graphical password techniques *Advances in Visual Computing* (pp. 741-749): Springer.
- Suresh, S, & Prakash, G. (2015). On reviewing the limitations of graphical password scheme.
- Tao, Hai. (2006). Pass-Go, a new graphical password scheme. University of Ottawa.
- Thorpe, Julie, & Van Oorschot, Paul C. (2004). Towards secure design choices for implementing graphical passwords. Paper presented at the Computer Security Applications Conference, 2004. 20th Annual.
- Towhidi, Farnaz, & Masrom, Maslin. (2009). A Survey on Recognition Based Graphical User Authentication Algorithms. arXiv preprint arXiv:0912.0942.
- Towhidi, Farnaz, Masrom, Maslin, & Abdul Manaf, Azizah. (2013). An enhancement on passface graphical password authentication. *Journal of Basic and Applied Scientific Research*, 3(2), 135-141.
- Trompenaars, F. and Turner, C. H. 1997. *Riding the waves of culture: Understanding cultural diversity in business*. London: Nicholas Brealey.
- Tullis, Thomas S, & Tedesco, Donna P. (2005). Using personal photos as pictorial passwords. Paper presented at the CHI'05 extended abstracts on Human factors in computing systems.
- Umar, Mohammad Sarosh, Rafiq, Mohammad Qasim, & Ansari, Juned Ahmad. (2012). Graphical user authentication: A time interval based approach. Paper presented at the Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on.
- Vacca, John R. (2013). *Managing information security*: Elsevier.
- Vachaspati, PSV, Chakravarthy, ASN, & Avadhani, PS. (2013). A Novel Soft Computing Authentication Scheme for Textual and Graphical Passwords. *International Journal of Computer Applications*, 71(10).

- van Eekelen, Wouter AJ, van den Elst, John, & Khan, Vassilis-Javed. (2013). Picassopass: a password scheme using a dynamically layered combination of graphical elements. Paper presented at the CHI'13 Extended Abstracts on Human Factors in Computing Systems.
- Van Teijlingen, Edwin R, Rennie, Anne-Marie, Hundley, Vanora, & Graham, Wendy. (2001). The importance of conducting and reporting pilot studies: the example of the Scottish Births Survey. *Journal of advanced nursing*, 34(3), 289-295.
- Venkatesh, Viswanath, & Davis, Fred D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, 46(2), 186-204.
- Venkatesh, Viswanath, Morris, Michael G, Davis, Gordon B, & Davis, Fred D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.
- Vockell, EL. (2001). *Educational Psychology: A Practical Approach* (Online Ed.), Retrieved Feb 5, 2009.
- Vu, Kim-Phuong L, Proctor, Robert W, Bhargav-Spantzel, Abhilasha, Tai, Bik-Lam Belin, Cook, Joshua, & Schultz, E Eugene. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65(8), 744-757.
- Weidenbeck, Susan, Waters, Jim, Birget, Jean-Camille, Brodskiy, Alex, & Memon, Nasir. (2005). Authentication using graphical passwords: Basic results. Paper presented at the Proc. of the 11th Int'l Conf. on Human-Computer Interaction.
- Werner, Steffen, & Hoover, Connor. (2012). Cognitive approaches to password memorability—the possible role of story-based passwords. Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.
- Wiedenbeck, Susan, Waters, Jim, Birget, Jean-Camille, Brodskiy, Alex, & Memon, Nasir. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1), 102-127.
- Wright, Nicholas, Patrick, Andrew S, & Biddle, Robert. (2012). Do you see your password?: applying recognition to textual passwords. Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security.
- Yadav, Uma D, & Mohod, Prakash S. (2013). Adding Persuasive features in Graphical Password to increase the capacity of KBAM. Paper presented at the Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on.

- Yoon, J. 2008. Searching for an image conveying connotative meanings: An exploratory cross-cultural study. *Library & Information Science Research*, 30(4),
- Zakour, Amel Ben. (2004). Cultural differences and information technology acceptance. Paper presented at the Proceedings of the 7th annual conference of the Southern association for information systems.
- Zangooui, Toomaj, Mansoori, Masood, & Welch, Ian. (2012). A hybrid recognition and recall based approach in graphical passwords. Paper presented at the Proceedings of the 24th Australian Computer-Human Interaction Conference.



## APPENDIX A

### Collecting Cultural Familiar Picture to construct the Database

#### A.1 Introduction

Dear Sir/Madam

The aim of this survey is to find a set of pictures that represent the national cultures in the Malaysia. By clicking on the link below, you agree to participate in this research. Your answers and personal information in this research will be confidential and anonymous. You may withdraw from the questionnaire by closing the web browser at any time without giving any reason to do so. To achieve the questionnaire please click on the link :

[http://student-enppf.formstack.com/forms/untitled\\_form](http://student-enppf.formstack.com/forms/untitled_form)

For more information about this questionnaire or the project, please contact me on:

-Abdullah Ibrahim

-School of Computing

-College of Arts & Science

-University Utara Malaysia

-E-mail : [abdo.ibra55@gmail.com](mailto:abdo.ibra55@gmail.com)

-Tel : 01127441076

-

#### A.2 The questions

<b>Question 1</b>
Enter your email: <i>Textbox</i>
<b>Question 2</b>
Select your gender: Multiple Choices (Only One Answer)
<b>Question 3</b>
Enter your age: Multiple Choices (Only One Answer)
<b>Question 4</b>
Enter your academic degree? Multiple Choices (Only One Answer)
<b>Question 5</b>
Please THINK of any (5) pictures that belong to your national culture

## APPENDIX B

### Guideline Questionnaire

Please tick (✓) at the appropriate box

	Questions	yes	no	not sure
1	Did you choose familiar pictures for your graphical password?			
2	In you answered (yes), did the familiarity with those pictures improve your memory today?			
3	During the registration, did you choose pictures that have direct relationship with you?			
4	If you answered (no), do you think this type of pictures will improve your memory?			
5	During the registration, did you choose pictures that are very famous and preferred by the general public in Malaysia?			
6	If you answered (no), do you think this type of pictures will improve your memory?			
7	During the registration, did you focus on the small details of the pictures of your graphical password?			
8	If you answered (yes), was this way useful in recognizing your graphical password today?			
9	During the registration, did you hesitate between two or more pictures?			
10	If you answered (yes), did this hesitation cause you difficulty at the recognition stage?			
11	During the registration, did you select your pictures based on sequential pattern? For example, did you make a short story of your graphical passwords?			
12	If you answered (yes), was this way useful in recognizing your graphical password today?			
13	Did you compare your graphical passwords with the decoys in the challenge sets? Did you find that your pictures are better than the decoys?			
14	If you answered (yes) was this comparison useful as the recognition stage today?			
15	At the registration process, did you take screen-sheet for your graphical password or save it by anyway?			

## APPENDIX C

### Security Questionnaire

**Please tick (✓) at the appropriate box**

What is your age ?	
<input type="checkbox"/>	18-25
<input type="checkbox"/>	26-35
<input type="checkbox"/>	36-45
<input type="checkbox"/>	45 and above
What is your gender ?	
<input type="checkbox"/>	Male
<input type="checkbox"/>	Female
What is your current academic degree ?	
<input type="checkbox"/>	Bachelor degree
<input type="checkbox"/>	Master degree
<input type="checkbox"/>	PhD degree
<input type="checkbox"/>	Others degree
How well do you know the person you have just attacked?	
<input type="checkbox"/>	Close friend/relative
<input type="checkbox"/>	Friend
<input type="checkbox"/>	Acquaintance
<input type="checkbox"/>	Stranger
How did you collect the passimages?	
<input type="checkbox"/>	By observing multiple logins and noting the images selected
<input type="checkbox"/>	By observing multiple logins and noting the images common between sessions
<input type="checkbox"/>	By capturing their record of the images selected
<input type="checkbox"/>	By guessing the pictures through knowledge of the users likes/dislikes
<input type="checkbox"/>	By guessing the images based on assumptions of what people in general might select
<input type="checkbox"/>	By randomly guessing/repeated attempts
<input type="checkbox"/>	Other - please provide details
Any other comments?	



## APPENDIX D

### Usability Questionnaire

**Please tick (✓) at the appropriate box**

I think that I would like to use this system frequently						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I found the system unnecessarily complex						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I thought the system was easy to use						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I think that I would need the support of a technical person to be able to use this system						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I found the various functions in this system were well integrated						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I thought there was too much inconsistency in this system						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I would imagine that most people would learn to use this system very quickly						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I found the system very cumbersome to use						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I felt very confident using the system						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree
I needed to learn a lot of things before I could get going with this system						
strongly disagree	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	strongly agree

## APPENDIX E

### Examples from the Culturally-familiar Picture Database





