AN ANALYTICAL STUDY OF 4-WAY RECOGNITION BASED SEQUENCE REPRODUCTION SCHEME IN GRAPHICAL PASSWORD

SAMANEH FARMAND

DISsertation submitted in fulfilment of the requirements for the master of information technology

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALALUMPUR

June 2010
Abstract

Computer and Network security is a very crucial issue of growing concern impacting user authorisation where textual passwords are widely used when accessing computers, networks, accounts and websites.

A big drawback of the textual password is its inability to resist against several forms of password attacks such as guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering. Other than being able to be secure against these attacks, passwords should be easy to memorise and recall. Therefore, usability and security are two important issues of concern when working with passwords.

Graphical Password seems to be the solution for the conventional type of authentication, text-based passwords, which will be briefly described throughout this document.

Graphical authentication schemes originally contain pictures that either the user has to click on parts of it or choose different shapes and images. Researchers have also made possible for users to draw their own image on grids. Despite the high standards of Graphical Passwords, they are still vulnerable to some kinds of attacks.

Our goal is to propose a new Graphical Password scheme that takes advantage of graphical input display capabilities to achieve higher security and better usability levels than can be achieved through text-based passwords. The proposed research is an approach to enhance existing Graphical Password techniques and make it resistant against attacks like Shoulder Surfing. This system has been improved to provide a wider password space in such a way that more server variables are involved such as the inclusion of a date and its combinations when choosing the password.

A waterfall model is used to perform the software development life cycle phases because is the most adequate model for implementing small to mid size projects. On top of that other techniques for gathering data such as questionnaires and surveys are used to assess the security and usability features of the system [See Chapter Six, Tables 6.5 and 6.6]. Overall, based on the results of the evaluation of the system it is concluded
that users were satisfied using the system; therefore it can be concluded that most of the usability features have been achieved, as well as the mentioned security parameters that is being resistant to shoulder surfing and guessing attacks. The study on the robustness of the system against Sniffing and the provision of a facility for users to upload their own pictures as another alternative for a password is also suggested for further study.
Acknowledgement

Finally, with the submission of my thesis I find the opportunity to thank those who made the completion of this thesis possible. It is a pleasure to convey my appreciation to them all in my humble acknowledgement.

I would like to express my greatest gratitude firstly to my supervisor, Dr. Omar Zakaria, who has been guiding me for over a year through the completion of my dissertation. The fruition of thesis would not have been possible without his encouragement, guidance and support from the initial stages right through to the eventual completion of the thesis.

My utmost gratitude and admiration goes to my family especially my beloved parents for they both have been the wind beneath my wings. I am forever grateful to them for their endless support and unconditional love.

I would like to extend my appreciation to Mr. Reza Azizi, an Information Technology specialist, who gave me the confidence and support to begin my masters program and provided me the inspiration to follow through right to the finishing line.

In addition, I wish to express my sincere thanks to Assoc. Prof. Dr. Diljit Singh, the Deputy Dean of our faculty whose enthusiasm for the underlying structures of doing a research has a lasting effect on me. It certainly was a pleasure and a great learning experience to be his student.

Last but not least, it is an honour for me to thank my friends, Mr. Arash Habibi Lashkari for his invaluable advice, comments and suggestions. He has made available his support in a number of ways. As our research area was close in significance, we have been writing journal and conference papers together after our literature reviews were done. I would like to thank my dearest friend Mrs. Tinah Annuar for her generous assistance in editing this document.
Publications


SAMANEH FARMAND and OMAR BIN ZAKARIA, “Improving Graphical Password Resistant to Shoulder-Surfing Using RBSR™”, *The 2nd IEEE International Conference on Information Management and Engineering (ICIME)*, 2010, Chengdu, China.

# Table of Contents

Abstract .......................................................................................................................... i  
Acknowledgement .......................................................................................................... iii  
Publications .................................................................................................................... iv  
List of Figures .................................................................................................................. viii  
List of Tables ................................................................................................................... x  

CHAPTER 1  Introduction ................................................................................................. 1  
1.1  Background ............................................................................................................. 1  
1.2  Research Overview ............................................................................................... 3  
1.3  Research Motivation .............................................................................................. 3  
1.4  Problem Statement ................................................................................................. 4  
1.5  Research Objectives .............................................................................................. 5  
1.6  Research Requirements ......................................................................................... 6  
1.7  Expected Outcome ................................................................................................. 6  
1.8  Research Schedule ................................................................................................ 6  
1.9  Thesis Structure ..................................................................................................... 7  

CHAPTER 2  Literature Review ...................................................................................... 9  
2.1  Introduction ............................................................................................................ 9  
2.2  Authentication Methods ......................................................................................... 9  
2.3  Graphical Passwords .............................................................................................. 11  
2.4  Reviews on Several Graphical Password Techniques ............................................. 12  
2.4.1  Problems ........................................................................................................... 12  
2.4.2  Solutions ............................................................................................................ 15  
2.5  Conclusion ............................................................................................................. 24  

CHAPTER 3  Methodology ............................................................................................ 28  
3.1  Software Methodology .......................................................................................... 28  
3.2  Software Methodology Approach ......................................................................... 28  
3.2.1  Waterfall ........................................................................................................... 29  
3.2.2  Prototyping ......................................................................................................... 29  
3.2.3  Spiral .................................................................................................................. 30  
3.3  Waterfall Model as the Software Methodology Approach ................................... 31  
3.3.1  Phase 1 – Requirements Analysis .................................................................... 33
3.3.2 Phase 2 – Design ................................................................. 34
3.3.3 Phase 3 – System Implementation .............................. 34
3.3.4 Phase 4 – System Testing ............................................. 34
3.4 Conclusion ........................................................................... 34

CHAPTER 4 Requirement Analysis and System Design .................. 35
4.1 Requirements ........................................................................ 35
  4.1.1 Functional Requirements ............................................... 35
  4.1.2 Non-Functional requirement analysis .............................. 37
4.2 Architecture Design ............................................................. 38
4.3 Program Design .................................................................... 39
  4.3.1 Programming Language: ............................................... 39
  4.3.2 Database Design: ........................................................... 40
4.4 System Design ...................................................................... 41
  4.4.1 Flowchart as our Modelling Language ............................ 41
  4.4.2 RBSR\textsuperscript{4} Data Flow Diagrams .......................... 42
4.5 Conclusion ........................................................................... 44

CHAPTER 5 Implementation .......................................................... 45
5.1 Introduction ......................................................................... 45
5.2 Registration Module ............................................................ 46
5.3 Login Module ....................................................................... 60
5.4 Conclusion ........................................................................... 65

CHAPTER 6 Testing and Evaluation .................................................. 66
6.1 Introduction ......................................................................... 66
6.2 Testing the Design of the System .......................................... 66
6.3 Usability and Security Study ................................................ 70
6.4 Shoulder Surfing Attack Test ............................................... 73
6.5 Conclusion ........................................................................... 74

CHAPTER 7 Conclusion ............................................................... 76
7.1 Summary of Research .......................................................... 76
7.2 Summary of Findings ............................................................ 77
  i. Objective 1 ....................................................................... 77
  ii. Objective 2 ...................................................................... 78
7.3 Research Contributions ........................................................ 78
List of Figures

Figure 1.1: Project overview ................................................................. 4
Figure 3.1: Basic Waterfall Model (Smith & Sarfaty 1993) and (Dennis et al. 2006) ... 29
Figure 3.2: Prototyping Model (Parida 2006; Shelly et al. 2008) ......................... 30
Figure 3.3: Spiral Model (Boehm 1985) ................................................... 31
Figure 3.4: Advanced Waterfall Model (Smith & Sarfaty 1993; Dennis et al. 2006) .... 32
Figure 3.5: Waterfall Methodology for SDLC containing divided subprojects (Dennis et al. 2006) ................................................................. 33
Figure 4.1: Data flow in the Login module ................................................. 36
Figure 4.2: Data flow in the Registration module ........................................ 36
Figure 4.3: An overview of the software development process (Gosling & McGilton 1996) ................................................................. 40
Figure 4.4: RBSR4 Simple Flowchart ......................................................... 42
Figure 4.5: Register Sequence Flowchart .................................................. 43
Figure 4.6: Login Sequence Flowchart ..................................................... 44
Figure 5.1: Login Screen ........................................................................ 46
Figure 5.2: Registration module, Phase one .............................................. 47
Figure 5.3: Compulsory fields in Registration module .................................. 48
Figure 5.4: Filling up the Form ................................................................. 49
Figure 5.5: Choosing the Sequence of the Password .................................. 50
Figure 5.6: Choosing the Password ......................................................... 51
Figure 5.7: Error according to choose a duplicate username ....................... 52
Figure 5.8: Changing the Username ........................................................ 53
Figure 5.9: Registration module, Phase 2 .................................................. 54
Figure 5.10: Reselecting the Password ..................................................... 55
Figure 5.11: Reselecting the Sequence of the Password ............................ 56
Figure 5.12: Error due to choosing an incorrect password ......................... 57
Figure 5.13: Error by choosing less than 4 items for password .................... 58
Figure 5.14: Error by choosing incorrect sequence for the password .......... 59
Figure 5.15: User is successfully added to the database ............................. 60
Figure 5.16: Login module, Phase 1 Entering the Username ...................... 61
Figure 5.17: Incorrect Username ........................................................... 61
Figure 5.18: Correct Username .............................................................. 62
Figure 5.19: Login module, Phase 2 Entering the password......................... 63
Figure 5.20: Error occurred by entering wrong numbers of password............... 64
Figure 5.21: Successful Login.................................................................... 65
List of Tables

Table 1.1: Gantt chart of the research ................................................................. 7
Table 2.1: Authentication Methods ................................................................. 10
Table 2.2: Password Attacks ........................................................................... 10
Table 2.3: Graphical Password Security and Usability Features ...................... 15
Table 2.4: Picture Based Password Methods ................................................... 24
Table 2.5: Summary of Graphical Password schemes ..................................... 26
Table 6.1: Registration module design test ..................................................... 67
Table 6.2: Password tested parameters ........................................................... 68
Table 6.3: User ID test case ............................................................................ 69
Table 6.4: Login module test parameters ......................................................... 69
Table 6.5: Security and Usability Questionnaire ............................................. 71
Table 6.6: Users Comments ......................................................................... 72
Table 6.7: Shoulder Surfing Test ..................................................................... 73
Table 6.8: Guessing Result for shoulder surfing attack ................................... 74
CHAPTER 1  Introduction

1.1 Background

Security is the hottest topic in network and computer systems. Authentication systems are largely used nowadays in which passwords are the main part of them. When the system verifies if the user has input a legitimate username and password, the user is under the authentication process. Users have to register first to be authorised for using the system and each time they want to logon they have to remember their password and username of which they acknowledged during the registration phase. This is the knowledge of password that ensures the user is not an intruder.

Back in the old days there were Sentries who put passwords in place simply by letting those who knew the secret word enter a city, while today passwords are ubiquitously used in any electronic computer systems that require the login process to be controlled such as automated teller machines, computer operating systems and mobile phones, as well as in the Internet when accessing websites and databases.

Current authentication methods can be divided into three main areas:

a. Text-based: A conventional password method which comprises alphanumeric characters.

b. Biometrics-based: A kind of authentication which utilises other methods of demonstrating identity like the retina scans and voice recognition.

c. Token-based: When employing physical devices such as the key fob and USB token.

Based on the review of various literatures we have found that researchers elaborated two main points that a good authentication system should have a password (1) being easy to remember and (2) secure in overall (Wiedenbeck et al. 2005; Qibin et al. 2008; Phen-Lan et al. 2008; Eljetlawi & Ithnin 2008).

Studies on evaluating users of authentication systems have disclosed that users choose and keep textual passwords very negligently (Wiedenbeck et al. 2005).
Moreover, physical devices used in token-based authentication methods can be stolen. In addition, biometric-based authentication tends to be more expensive than other techniques plus requires users to participate willingly in this kind of authentication. As a consequence, to prevent all the weaknesses mentioned above, strengthening the authentication process is compulsory and inevitable.

Guessing attacks, dictionary attacks, key-loggers, shoulder-surfing, and social engineering are counted as expected general attacks to authentication systems (Klein 1990). To resolve the above weaknesses of traditional password schemes, scientists have introduced Graphical Passwords which have been put into place since the last decade of the 19th century. Moreover, after touch-screen devices and stylus ones have spread in the technology market, applications using such devices became increasingly popular and made the use of graphical user authentication techniques necessary. In addition, studies have proven that recalling graphical images for human beings is easier than memorising texts (Wei-Chi & Tsaur 2005).

A Graphical Password authentication system is demonstrated in a graphical user interface (GUI). Users have to choose images or draw shapes as their password. The orders of their clicking and the angles of the shapes will be saved as their password sequence. One of the first researchers who gave the idea of Graphical Passwords is Greg Blonder. His system works by getting a user to click on images in a complex picture.

Graphical Password techniques can be classified into two categories: Recognition-based and Recall-based. Recognition-based is where users are represented with images for authentication purpose. On the other hand Recall-based is a way of authenticating the user based on what the user has provided to the system on the earlier stage of registration phase for authentication (Eljetlawi & Ithnin 2008). In this research a new recognition-based Graphical Password is presented.

In chapter two, solutions to all the shortcomings of textual password will be illustrated. While having a convincing usability, researchers are still having a hard time to find better solutions to problems encountered by password entropy and shoulder-surfing.
1.2 Research Overview

Until now the proposed shoulder surfing resistant schemes limit the usage of Graphical Password to hand-held or workstations where only one person is able to view the screen at the time of login. By completion of the proposed research, an efficient algorithm is expected to be produced and implemented that is robust against the known attack of shoulder surfing by employing either small or wide login screen in public places. The outcome design is named RBSR\(^4\) (Recognition-Based Sequence Reproduction 4-way) and will be referred to with the above abbreviation throughout this document. Our attempt in this research is to provide the balance between security and usability. While ensuring that the password is resistant to any direct and indirect observations, a concerted effort has been made in order to design the whole system to be as user friendly as possible to gain usability restrictions which will be presented and discussed more throughout this document.

1.3 Research Motivation

Due to the fact that Information Security is one of the most important issues in the world, the need for a strong authentication has increased dramatically. There are different types of passwords. Text passwords are the very first type and are known as traditional passwords. There are Token-based and Biometric passwords as well as knowledge-based ones which are text-based and picture-based ones. High security and good usability are two requirements needed to be achieved during an acceptable authentication evaluation. The problems with these passwords are the apparent weakness against different kind of attacks, which have been discussed in section [1.1]. Additionally, when using token-based passwords, people should remember to take the token with them, and also for Biometrics users, they have to be willing to use it. The latter password is costly which poses a bigger problem. To date, Graphical Passwords seem to be the preferred solution (Alsulaiman 2006) which is in line with the findings of psychological researchers which demonstrated that humans are better able to memorise and remember picture passwords than text-based ones. From a security standpoint this makes them less vulnerable to attacks in comparison to textual schemes.
Much like any other country Information Security is a hot topic in our nation. Intruders can still attack and find peoples’ account passwords, despite the existence of numerous strong systems not known to be vulnerable to any attacks. In our studies in UM we were greatly encouraged to explore the field of Information Security and thus lead to the effort to come up with a new algorithm that can provide sufficient secure password. After having researched and scoured through, the extensive literature of passwords, the Graphical Password stood out as one of the more interesting applications in the field. Upon further exploration, it was discovered that the study of Graphical Password is comparatively new, and that few significant results have been achieved as suitable solutions to the problem of not being resistant to shoulder surfing. This was another strong motivation to select RBSR$^4$ as a research topic to undertake. The chart below shows a clearer view of the nature of the research. A few important problems are mentioned in the chart will later be highlighted in section [1.4].

![Figure 0.1: Project overview](image)

### 1.4 Problem Statement

Through the review of related studies and literature on authentication systems, two major areas have been identified for consideration for the purpose of the research, namely security and usability issues.
From security point of view, despite the fact that Graphical Password techniques have proven to be more secure than textual passwords, they are still vulnerable to attacks through shoulder surfing (Alsulaiman 2006; Shushuang, et al. 2003; Wei-Chi and Maw-Jinn 2005; Qibin, et al. 2008; Di, et al. 2007; Phen-Lan, et al. 2008; Ziran, et al. 2009; Zhi, et al. 2005; Sabzevar & Stavrou 2008). It is a very popular choice of attack that occurs while accessing resources in public places which takes place when an authorised user’s password is being marked by a person directly watching over the user’s shoulders or monitored via a closed circuit camera, as well as when the password is captured by Trojan login screens and an electromagnetic pulse scanner that are used to keep track of the keyboard or the mouse (Sobrado et al. 2002; Wiedenbeck 2006; Kumar 2007).

From the usability standpoint, many researchers have approached this problem in attempts to produce an efficient algorithm that can be resistant to shoulder surfing but to date all those systems limit the usage of Graphical Passwords to small screen devices such as hand-held or workstations where only one person is able to view the screen at the time of login like in Pass-Faces (Eljetlawi & Ithnin 2008; Alsulaiman & El-Saddik 2008). The other case would be that it still has not reached the level of user satisfaction in that the system is still relatively complex to use and learn and lack faster process of inputting the password compared to textual schemes such as the ones demonstrated by the Cognitive Trapdoor Games (Volker et al. 2004) and Convex-Hull Scheme (Sobrado & Birget 2005) whilst in some others where the users have problems with regard to recalling their password such as in the Challenge-Response Identification Scheme (Man et al. 2003). The most important factor is to have a system with high security and at the same time possesses good usability design.

1.5 Research Objectives

The objectives of this research are as follows:

a. to study and understand modern Graphical Password techniques.

b. to design an efficient Graphical Password Algorithm resistant to shoulder-surfing.

c. to implement the proposed system.

d. to test it in an environment prone to shoulder surfing attacks.
1.6 Research Requirements

The System and Development Tools requirements are:

- **a.** Java development environment (NetBeans, MySQL),
- **b.** Screen Capturing Tools,
- **c.** Computer Network Lab,
- **d.** Java SE Development Kit 6 (JDK 6) to run Java,
- **e.** Windows XP Professional SP3.
- **f.** Pentium 4 processor or higher with minimum of 512 RAM and minimum of 2.0 GB of hard disc,
- **g.** VGA colour monitor and a standard keyboard.

1.7 Expected Outcome

The expected outcome of the system should be specified before developing it, but it requires good programming and an on time system development. It also depends on the proper evaluation of the system.

- **a.** The system is expected to be unsusceptible to the effects of shoulder surfing attack (See Chapter Six).

- **b.** The system should satisfy the user, and the password has to be hard to guess and robust against social engineering attack (See Chapter Six).

- **c.** A user manual will be provided for the end users (See Chapter Five).

1.8 Research Schedule

The table below shows the research timeline in a simple Gantt chart. A description of the software lifecycle approach and its timing can be seen in the table below of which will be elaborated further in Chapter 3. It must be noted that some of these phases actually overlap.
Table 0.1: Gantt chart of the research

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing and studying the research literature to acquire a deep understanding of the concept</td>
<td>May 2009</td>
<td>Aug 2009</td>
</tr>
<tr>
<td>Developing the algorithm</td>
<td>August 2009</td>
<td></td>
</tr>
<tr>
<td>Implementing the proposed system</td>
<td>Sept 2009</td>
<td>Oct 2009</td>
</tr>
<tr>
<td>Documenting the report</td>
<td>Nov 2009</td>
<td>Feb 2009</td>
</tr>
</tbody>
</table>

1.9 Thesis Structure

This research concentrates on the RBSR\textsuperscript{4} which is a Graphical Password resistant to shoulder surfing. Chapter 1 introduces the research. It sketches a summary of the plan for this research and contains the research overview, motivation, problem statement, research objectives, research requirements, expected outcome, research schedule, and finally the thesis structure.

The second chapter will be the review of related literature. It will investigate the problems associated with various authentication methods and will review important propose Graphical Password schemes as solutions to the mentioned problems. At the beginning, the readers will be provided with an overview of the different kinds of authentication systems, possible attacks and following that will further elucidate how the Graphical Password can overcome those shortcomings. Before designing,
developing and analysing our proposed method, justification for proposing a new model will be furnished in this chapter.

Chapter three will be on the methodology of the proposed system which shall entail structuring, planning and controlling it. A description of the chosen software methodology and the development phases will also be clarified. This chapter will present readers with the gist of the approach of the proposed algorithm for the purpose of this research.

The requirements analysis and system design will also be discussed in chapter 4. The analysis on requirements includes functional and non-functional requirements. It will be a brief introduction on the employed programming language and clarifying components to be incorporated in the system. Finally through the aid of flowcharts the overall structure of our system will be illustrated.

The fifth chapter will comprehensively illustrate the entire mechanism of the system and followed by the sixth chapter within which the outcome of the program testing will be explained in detail. We will clarify the evaluation of design and implementation of our system. Moreover, the security and usability will be tested separately.

Chapter seven will finally conclude the research which will comprise a summary of the investigated problem and the main findings of the proposed research. Apart from that, emphasised research contributions, implications of the research for professionals working in this field and future directions for further research will also be brought forth.
CHAPTER 2  

Literature Review

2.1 Introduction

Authentication system reinforces security for information and computer networks with the aid of passwords which are the main part of it. Confirming if someone is the one who they contend is the process of authentication. Authentication is usually performed by employing the logon passwords in private and public networks as well as the internet. Passwords hold many useful assets and as a result, we can see their use for the foreseeable future. Passwords are basically used to assure that the user is authentic. Every time the user wants to use the system to login, the user must use their previous confirmed password upon registration.

The background of applying passwords goes back to Sentries who would ask people for a watchword to let them get close or enter a region. At the present time passwords are often used to access protected computer operating systems, mobile phones and automated teller machines throughout login phase. Password is necessarily needed to enter websites, networks, databases, and computer accounts. A conventional password method is a text based which consist of alphanumeric characters. This method is applied for authentication in order to verify the user’s identity and permit them to access the computer system. Nevertheless it can include any other method of demonstrating identity such as a smart card, retina scan, voice recognition, or fingerprints and physical devices for instance a key fob and a USB token.

2.2 Authentication Methods

Until recently, the three major divisions of authentication methods are: token-based authentication, biometric-based authentication and knowledge based authentication. Text-based, PINs and Picture Passwords are categorised under knowledge based authentication (Xiaoyuan et al. 2005). The most common between them are alphanumeric username and password. For token-based and biometric-based authentication, the various methods are shown in Table 2.1.
Table 0.1: Authentication Methods

<table>
<thead>
<tr>
<th>Knowledge Based</th>
<th>Token Based</th>
<th>Biometric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text-Based</td>
<td>Tokens</td>
<td>Fingerprints</td>
</tr>
<tr>
<td>Pass-Codes (PINs)</td>
<td>Smart Cards</td>
<td>Palm-prints</td>
</tr>
<tr>
<td>Graphical Passwords</td>
<td>Keys</td>
<td>Hand Geometry</td>
</tr>
<tr>
<td></td>
<td>Chip Implants</td>
<td>Face Recognition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voice Recognition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Iris Recognition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retina Recognition</td>
</tr>
</tbody>
</table>

The main drawback of passwords is called the password problem; it means passwords are considered likely to have the following characteristics. “(1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and without difficulty by humans. (2) Passwords should be secure, i.e., they should look random, hard to guess, changed frequently, unlike on different accounts of the same user, not to be written down or stored in plain text. Classical studies have shown that human users tend to choose and handle alphanumeric passwords very insecurely.” (Wiedenbeck et al. 2005)

Table 0.2: Password Attacks

<table>
<thead>
<tr>
<th>Password</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text-Based</td>
<td>Guessing, Dictionary, Key-Loggers, Shoulder-Surfing, Social Engineering, Hard to Remember, Hidden camera &amp; Spyware attacks</td>
</tr>
<tr>
<td>Pass-Phrases</td>
<td>Advantages</td>
</tr>
<tr>
<td></td>
<td>Easier to remember and virtually impossible to crack due to their length.</td>
</tr>
<tr>
<td></td>
<td>Attacks</td>
</tr>
<tr>
<td></td>
<td>Key-Logger or sniffed if transferred over plain text communication channel.</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Advantages</td>
</tr>
<tr>
<td></td>
<td>Highly Accurate, cannot be stolen, forgotten, or given to another person.</td>
</tr>
<tr>
<td></td>
<td>Attacks</td>
</tr>
<tr>
<td></td>
<td>Can be expensive, Slow identification process, sometimes the number of false results, user’s tendency to subject their eyes in front of eye trackers for example, not feasible for those who are in far distance like internet users, unable to be revoked</td>
</tr>
</tbody>
</table>

10
Current authentication systems experience many shortcomings. The sensitivity of the textual username and password has been renowned. Registered users have a tendency to choose short passwords or easy to remember, which makes the passwords unprotected for attackers to break. Furthermore, alphanumeric password is vulnerable to guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering. Other problems are as indicated in Table 2.2.

To conquer the limitation of text-based password, techniques such as two-factor authentication and Graphical Password have been used. Two-factor authentication is when the users have to use more than one method of authentication together to access a secure system.

This is while with the appearance of stylus, touch screen and other input devices into the world of technology the usage of graphical authentication has become more vital than ever. Besides, they propounded the likelihood of providing a form of authentication that is severely stronger than text passwords. According to the fact that scientists have proved it more effortless and simpler for users to memorise and recall pictures than words, users will be also capable to remember stronger graphical sort of passwords (Wei-Chi & Tsaur 2005).

2.3 Graphical Passwords

Graphical Password as defined by Yokota and Yonekura (2005:367) is: “an authentication system that works by selecting or drawing images, by users in a specific order, presented in a graphical user interface (GUI). Thus, it is sometimes called graphical user authentication (GUA).” The GUI term is used when windows, icons, and menus are employed in a computer interface by a human who also can adopt and change them. Graphical Password was first researched by (Blonder 1996). As for Blonder states “Graphical Passwords have a predetermined image that the sequence and the tap regions selected are interpreted”. Many other Graphical Password proposed schemes can be found (Klein 1990).

Graphical Password techniques can be classified into two categories: Recognition based and Recall-based. Recognition-based in which various pictures will be displayed
on the registration and login screen. To successfully gain access to the system the user has to click on the exact images chosen in the registration section and in the same order. On the other hand Recall-based is a way of authenticating the user based on what the user has provided to the system on the earlier stage of registration phase for authentication (Eljetlawi & Ithnin 2008). Recognition-based authentication supposed to be more memorable and user friendly than recall-based as PIN (Personal Identification Number) (Zhi et al. 2005).

2.4 Reviews on Several Graphical Password Techniques

Based on a comparative study, we conclude our results in problems and solutions we found in the previous proposed methods that was studied during this research. As a conclusion, a complete comparison table on security, usability and drawbacks of the studied methods is presented. Finally we will introduce our system and its features.

2.4.1 Problems

There are weak and strong passwords for authentication process. The former is vulnerable to dictionary attack whilst the latter is difficult to memorise (Zhi et al. 2005; Wei-Chi & Maw-Jinn 2005; Phen-Lan et al. 2008; Sabzevar & Stavrou 2008). The most important issue in traditional password is that it is difficult for users to remember a secured password. In this case, the user neglects to pay attention about the password security just to have the process of authentication faster performed (Eljetlawi & Ithnin 2008).

Password space plays an important role in achieving high security. Large number of pictures will cause bigger password space in Graphical Password models than in text based ones. Therefore, it makes the system virtually more immune to attack like dictionary attacks but yet there is not known pre-existing dictionaries to search for graphical information. Two mainstreams of modern Graphical Passwords are click-based approach and image selection-based approach. These approaches suffer the problem of small password entropy (Zhi et al. 2005). Therefore, system passwords will face problems where their password entropy is small in size, eventually causing the
whole system to be weak against the guessing attacks (Zhi et al. 2005; Ziran et al. 2009; Alsulaiman & El-Saddik 2008; Sobrado et al. 2002).

It is not easy to plan automated attacks in Graphical Password; to elaborate this issue one can take an example where human beings are able to identify a person’s face faster than a computer. It will not take more than a second for humans whereas for computers it takes respectable amount of time to process millions of bytes of information without taking into account to find out if the image is a face, a landscape, or a meaningless shape (Sobrado et al. 2002). Studies have shown that because human can recall picture passwords easier and faster than text ones, therefore graphical authentication system is more usable than textual. These are studies according to psychology to proof that it is easier for people to remember picture passwords than text based “(1) An experimental study of memory (Kirkpatrick 1894) (2) Short studies in memory and association (Calkins 1898) and (3) Factors affecting item recovery and hypermnesia in free recall (Madigan & Lawrence 1980)” (Wei-Chi & Maw-Jinn 2005).

A good usability for Graphical Password should contain features such as to be easily used, created, memorised, and learned plus a good design and layout which brings along with it an adequate memorability (Eljetlawi & Ithnin 2008). Generally the benefits of image-based passwords over textual passwords should be about its recallability and memorability (Eljetlawi & Ithnin 2008; Zhi et al. 2005; Alsulaiman & El-Saddik 2008). The fact about memorability is to make the system more convenient for users in such that they can remember the password faster and easier (Qibin et al. 2008). According to (Ziran et al. 2009; Sobrado et al. 2002), users view of point, time consuming is an important issue. Memorability depends on several features such as how the user selects, encrypts the password and memorises it (Eljetlawi & Ithnin 2008). Noticeable, not too complicated objects and locations can improve memorability (Zhi et al. 2005).

From prior studies it can be seen that there are hotspots in many Graphical Password models such as Pass-Point which are categorised under recall-based schemes. Pass-Points can be predicted by assailants and guessed easily because people tend to choose those points more than other parts of the picture as their password mostly
because they can be recalled faster. In this case, different kinds of attacks can be used such as Brute-Force attacks.

Main drawback of image recognition passwords is the limited number of images shown on the screen each time, for instance in Pass-Faces in which only 9 images is displayed (Eljetlawi & Ithnin 2008; Al-Sulaiman & El-Saddik 2008).

As Al-Sulaiman and El Saddik (2008: 1935) mentioned that “Any authentication scheme is affected by the knowledge distribution of the user’s secrets”, therefore being able to write down or intrude by social engineering attacks is counted as another drawback of textual passwords. Another problem ought to be thought over carefully is that it is not difficult to change or cancel the password.

According to (Phen-Lan et al. 2008) phishing is another attack that any kind of passwords has to be tested against while analysing the system security.

Till 2005 Graphical Password has proven to overcome both dictionary attacks and memorability problems but at the same time have some possible drawbacks against shoulder surfing attack. It is more unprotected than traditional alphanumeric passwords against this attack (Blonder 1996; Sobrado et al. 2002; Al-Sulaiman 2006; Shushuang et al. 2003; Wei-Chi & Maw-Jinn 2005; Qibin et al. 2008; Di, et al. 2007; Phen-Lan et al. 2008; Ziran et al. 2009; Zhi et al. 2005; Sabzevar & Stavrou 2008).

Shoulder-surfing attack is another famous attack that occurs while accessing resources in public places:

1) when an authorised user is being monitored by a person (via camera or recording) and remarks the legitimate user's password,
2) when observing the login page directly over users shoulder while entering his password,
3) when an electromagnetic pulse scanner keep track of the keyboard or the mouse,
4) when a Trojan login screens capture the passwords (Sobrado et al. 2002),
5) when the individual’s authentication session is being logged (Wiedenbeck 2006).
This is a problem that has been difficult to overcome. Up to recently, the number of proposed solutions to shoulder surfing attack is very limited (Blonder 1996; Sobrado et al. 2002) and other implementations were only limited to small screen handheld device. A survey carried out by (Xiaoyuan et al. 2005) stated that there were no recall-based techniques designed to resist shoulder-surfing attack till that time.

### 2.4.2 Solutions

To have a good system, high security and good usability are both needed. They cannot be considered separately (Zhi et al. 2005; Ziran et al. 2009; Qibin et al. 2008). (Eljetlawi & Ithnin 2008) introduced a set of usability features in Graphical Password techniques which are ease of use, memorise, creation, learning and satisfaction. Table 2.3 shows a selective set of usability and security features for Graphical Password schemes in order to avoid their drawbacks.

<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>Usability Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Randomly Assigned</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>Unique to the Application</td>
<td>Intuitive to Use</td>
</tr>
<tr>
<td>Robust against known attacks</td>
<td>No User Rules</td>
</tr>
<tr>
<td>Simple</td>
<td>Independent of user’s aptitude, training, or attentiveness</td>
</tr>
<tr>
<td>Reliable – no fallback needed</td>
<td>No on-going training</td>
</tr>
<tr>
<td>Not Sharable casually or easily</td>
<td>Easy to Use</td>
</tr>
<tr>
<td>Lacks social vulnerabilities</td>
<td>Portable</td>
</tr>
<tr>
<td>Usable anywhere</td>
<td></td>
</tr>
<tr>
<td>Two-way Authentication</td>
<td>Fun</td>
</tr>
</tbody>
</table>

Many shoulder-surfing resistant Graphical Passwords schemes have been proposed. Following is a brief review of some major articles and papers in this field. The proposed methods overcome some of the problems that we had reviewed in previous section.
I. Universal Multi-Factor
(Sabzevar & Stavrou 2008) proposed a system called Universal Multi-Factor in which the system gives hints to the users so that he can just click on those areas accordingly to choose his password. User’s choice is not involved in choosing clickable areas, therefore all areas have the same chance to be clicked and guessing becomes completely irrelevant.

Additionally, it is obvious that the Graphical Passwords are unaffected by traditional key-loggers due to keystrokes (the pressing of a key on a specific computer keyboard) have been replaced with clicks. Nevertheless, more complex spywares are able to capture the screen and can seise the user password recognition (Sabzevar & Stavrou 2008).

II. A Remote User Authentication Scheme Draw-A-Secret (DAS)
“A Remote User Authentication Scheme” is a strong Graphical Password based on DAS scheme introduced by (Wei-Chi & Maw-Jinn 2005). In Draw-A-Secret there is a 2-dimensional grid, where the users draw their password on it, and the password is recorded from the coordinates of their drawing. The sequence of their drawing is also important in the code plus a “pen-up” event. Equal to number of coordinate pairs is the length of the stroke. They show their scheme is resistant against dictionary attack, replay attack, password-file compromise attack, the denial-of-service attack, the predictable n attack, and the insider attack. Moreover, it is reparable. They introduced two protocols, one for registration and another for login. They proved that in any of these frauds the adversary should know main components of these protocols for a successful attack which are not possible to gain.

III. Random Geometric Graphical Password (RGGPW)
The easy-to-recall and hard to guess “Random Geometric Graphical Password (RGGPW)” was proposed by Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang in 2008. Their goal was to overcome drawbacks of picture-based passwords, easily guessed, passwords being alike if similar pictures were used, shoulder-surfing and phishing. They claimed that their system is secured because of these reasons: (1) Sufficient password space to be resistant against brute-force search attack; (2) Complicated geometric shapes makes it very difficult to be fraud by shoulder surfing or...
There are different geometric shapes in the image. The users can choose their own pass-objects. The final password is a chain containing the characteristic points of all the pass-objects like angles of critical points and position of centroid. Systems like RGGPW are based on click points which remind users of the exact places they clicked during the registration phase. For security, they analysed their scheme against different types of attacks. In brute force search they prove that the password space is much greater than in text-based password. It is resistant against guessing and forgery attacks because the tracks and colours are generated from a random seed based on the information of both the user and the server. They do not use click points straight, though the special characters of the position will be the final password. This is why a spyware cannot capture mouse clicks. The objects are layered on top of each other so it won’t be easy for an attacker to surf over users shoulder. The password will be very complicated so the user cannot pass on the information to another person. This model also does not need any database, like random-art-based scheme and Grid-positions-based DAS scheme. It is also resilient against key logger as the password screen is dynamically placed (Phen-Lan et al. 2008).

IV. An Interactive and Secure User Authentication Scheme for Mobile Devices

Another authentication scheme is “An Interactive and Secure User Authentication Scheme for Mobile Devices”. High security and good usability is accomplished by using an authentication protocol between server and the device. Today almost all mobile phones have camera, and the picture taken from the user will be unique, these two facts helped them to make the scheme robust against shoulder surfing attack. This is done by the aid of biometrics. The latest studies have shown that a strong bit-string can be produced from user face (Qibin et al. 2008).

On top of that (Qibin et al. 2008) classified a state-of-the-art IBA approach which stands for Image Based Authentication into two categories: “click-based approach (Blonder 1996, Perra & Giusto 2005) and image selection-based approach (Pass-faces,
Déjà Vu, Pass-Pic, Takada & Koike 2003). The former is based on sequential clicks of some points on an image, in which the location and order of the clicks are used as the password. In the latter approach, the user selects some “recognisable” secret images from a given image list. The whole authentication process consists of several rounds of such selections.” (Qibin et al. 2008)

Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto introduced a new design named association-based Graphical Password in their previous paper ‘An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack’. The main rule is based on human perceptive ability of this model. They used this fact that splitting password elements assists the memory and help users to memorise better, which is called Method of Loci. They also used zero-knowledge proof protocol to make their design resistant to shoulder surfing attack, but at the end they encountered the problem of password entropy being small and the whole method being weak against guessing attacks (Zhi et al. 2005).

While Qibin Sun, Zhi Li, Xudong Jiang and Alex C. Kot, in their new model, the user will be authenticated to the system by his picture. The server will compare the password entered by the user with his picture which is saved in the database, and he will be granted to login. The password consists of pass-objects combining with different colours which have to be chosen in several rounds. For enhancing the memorability the previous model is used. Two parts are associated together pass-locations to pass-objects and pass-objects to pass-colours. Comparing to recognition-based Graphical Passwords association-based has more password entropy due to more variety of options. Moreover, it is better than recall-based as it gives the user gestures to remember their password easier and faster. For security reasons the server generates not the same hash from the face bit-string each time (Qibin et al. 2008).

V. Jetafida

A model named Jetafida is introduced in “Prototype Usability Survey” in 2008 to achieve a better usability in recognition based Graphical Passwords. It was tested via questionnaire among computer students using the system three times. Memorability depends on several features such as how the user selects and encrypts the password and how he remembers it. While choosing Graphical Passwords, the order of selection and
the image itself have important role. If the points have sense, it will be easier to memorise. The password contains variant pictures from nature, human, animal with different colours and the order of selection. Main drawback of image recognition passwords is limited number of images shown on the screen each time, similar to Passfaces. Executed usability features in this scheme are ease of use, create, memorise, learn and also a good design and layout. To elaborate these terms we can say being easy to use and create the password in any kind of system by any users from those who are not familiar using computer to those who are trained. Easy to memorise and learn by means of the password not being too difficult to remember and the system not being so complicated to learn the process of accessing the secure data by entering username and password. They made several questions under each of these sections and the student is asked to answer after using the prototype of their model. Similar to the other password schemes they have two options in the first page, one for those who already have an account and one for those who does not have an account. When new users enter their username, the system will take them to another page to choose their Graphical Password between varieties of images. Whenever they wish to login, they cannot make mistakes more than three times. Their results show that more percentage of students agreed that usability of Jetafida has been achieved in all those areas mentioned above (Eljetlawi & Ithnin 2008).

VI. 3-D password

Fawaz A. Alsulaiman and Abdumontal El Saddik comprehensively analyse and discuss 3-D password for a more secure authentication. They proposed the scheme in which the user has the option to choose different kinds of authentication models to interact between objects. Therefore, it will be hard for an attacker to intrude due to the large number of choices (Alsulaiman & El Saddik 2008).

In their scheme, they combined recall-, recognition-, biometrics and token-based authentication types. Users are free to choose either a combination of the four models. Memorability, robust against guessing attack, unable to write down or being intrude by social engineering attacks, not difficult to change or cancel the password are part of their goal. Two object groups that play important role in their model are any objects that exist in real-life, such as an ATM or a computer and a fingerprint reader or a biometrical recognition device. Actions toward these objects are different. The location
and sequence is very important in constructing a correct password. They have to build the virtual environment, so the characteristic of the objects are important and this design has affect on password space, usability and performance of the system. The virtual environment has two characteristics, being similar to real life so that the user can memorise easily, the objects are unique so the user can differentiate between them to have a good usability. The size of this environment has direct relation with password space; although choosing password in a small environment is faster, larger size will cause a bigger password space. Moreover correct response and number of objects chosen influences the password space. The 3D authentication can be used in very high security applications, such as in military or important servers because it has a large password space (Alsulaiman & El Saddik 2008).

In their studies they proved that their algorithm is more secured than other schemes because the attacker has to break different authentication methods to find what the password is and various environments such as 3D for different applications. They also found countermeasures for attacks, and tested their system against each attack to proof its security. However they pointed out that still 3D authentication is in its initial steps and needs more research on how to make it resistant against shoulder surfing (Alsulaiman & El Saddik 2008).

VII. A Stroke-based Textual Password Authentication Scheme

The Stroke-based Textual Password Authentication Scheme, in order to have high usability and memorability, strokes on a grid and keyboard for text-based passwords are used. It is proved to be resistant against brute force and shoulder surfing attacks and have a large password space. The user has to click their chosen password which can be a figure, a character or a geometry shape on the grid. The system will save the stroke places and the sequence of clicking. The user can choose the size of the grid. In the login phase a same sized grid will be shown filled up with numbers. The user has to remember his password and enter the numbers in correct order of his password (Ziran et al. 2009).

This scheme is resistant to shoulder surfing because if any attacker wishes to discover the password, he should capture the keyboard as well as the screen of the device. Moreover, it is difficult for the attacker to guess the shape of the password. The
grid for login interface will not have the same selection of numbers so that the string of inputs is different in each login time. Random clicking is also difficult as the attacker does not know the password length. The problems arise because the system is newly proposed and it will take time for users to get used to it and learn how to choose strong passwords. This is when the attacker can guess easier and intrude the system. However, the login phase is more secured. The speed of logging in to the system is lower than other Graphical Password models (Ziran et al. 2009).

VIII. Challenge-Response Identification

In a paper titled “A shoulder-surfing resistant graphical password scheme” published by (Man, Hong, and Mathews 2003), more areas of problems in shoulder surfing were specified. They proposed a technique named challenge-response identification that includes pictures which is called pass-objects with different features for example colours, shapes, etc. Each one has different code which the user has to memorise the one assigned to his password. The user has to enter his password in several phases and screens. Different screens will be shown to the user; each has different pass-objects and a lot of decoy-objects. The user has to key in the code previously chosen in the registration phase in addition to a code signifying the comparative position of the pass-objects in relation to a pair of eyes. The fact is it is very difficult for the attacker to find the code because there is no mouse clicks. However, the user has to memorise the string corresponding to the variant pass-objects (Blonder 1996). Hong with other researchers at a later time modified the system to have more usability, enabling the user to assign his own codes to the pass-objects, but still it is a necessity for the user to memorise a long string and hence suffer from password problems (Alsulaiman 2006).

IX. Cognitive Trapdoor Games

In another paper titled “A PIN entry method resilient against shoulder surfing” published by (Volker, Richter and Freidinger 2004), the problem of shoulder surfing is revisited in such a way that it challenges the user by asking questions that concludes if the user is aware of the right answer or he is an intruder. The graphical interface includes numbers in black and white colours. The user has to choose either one of these colours which indicates the secret number. For each secret digit, the scene will be shown to the user. For example, if the challenge is repeated four times for each number
and if the user has a four digit PIN, the user will be challenged 16 times. Therefore this task will take a long time to be solved. They called it cognitive trapdoor games in which an alternative PIN entry method was proposed (Shushuang et al. 2003).

X. Convex-Hull Scheme

Another interesting paper with the titled of “Graphical passwords” published by (Sobrado & Birget 2002), the authors introduce a technique that developed a Graphical Password dealing with the shoulder-surfing problem. They called it the convex-hull scheme. The user has to choose variable of k icons among N icons that the system will show in the registration screen. Then several scenes will be shown to the user while logging in, in each of which he has to select j icons where 3<j<k and click inside the convex-hull created by those j pass-icons. These icons are spread by chance among n<N. Two crucial drawbacks in this approach include the slow login process and the small probable password space resulting from this authentication scheme. Sobrado and Birget recommended using 1000 objects to make the scheme more resistant against guessing attack but the displaying screen becomes very packed and the objects are hard to recognise. However, using fewer objects might influence the password space being large enough. Earlier, they proposed another algorithm in which the user can relocate the frame including objects to a position that forms a line with another two pass-icons. Repeating the challenge helps reducing the possibility of logging into the system and also by randomly clicking or rotating (Sobrado et al. 2005).

XI. Association-Based Graphical Password

A novel (Zhi et al. 2005) proposed an association-based Graphical Password to overcome the usual problem of both click-based and image selection-based approaches, two principal trends of Graphical Password. Both suffer from comparatively small password entropy. This scheme is based on mnemonics- Method of Loci has parts aligned with Image Based Authentication (IBA) in JPEG committee. It uses the fact that splitting password elements assists the memory and helps users to memorise better. The main rule is based on human perceptive ability of this model. They also used zero-knowledge proof protocol to make their design resistant to shoulder surfing attack.

The three groups who have to play role in this model are Alice, Bob and the machine verifier (MV). Alice logging in through ATM, PDAs, etc and MV has to make
sure that Alice is an authorised user and Bob tries to attack the system and login instead of Alice. There are three elements that Alice has to choose which are location, object and colour. Choosing the above three elements will be repeated several times and they are related to each other, so that Alice can remember them easily as a package. In their analysis they discussed about user-friendliness and security, two important issues for a good authentication procedure.

Noticeable and not too complicated objects and locations can improve memorability. The association-based password is proved to be better than recall-based passwords because it is easier to remember striking images and it is superior to recognition-based passwords as they have more options to choose therefore the password entropy is larger. Their scheme is robust against random guessing as the list of objects and colours has to invariant. To make their scheme resistant to shoulder surfing attack, they used zero-knowledge proof protocol. Thus, Alice has to solve a “hard problem” to prove that he/she is a real user and not impersonating. The question must be indirect so that Bob cannot guess the answer without knowing the secret. This hard problem is to select a subset that contains pass colour. For more security they will give the user an option to choose a set of colours in which the real set is there as a subset. Their result shows that the system is robust against shoulder surfing by counting number of time Bob has to watch Alice inputting the password. Increasing number of rounds and colour list size will make the system more secured. To complete their analysis they compared their system with previous proposed models (Zhi et al. 2005).

Furthermore, more Graphical Password schemes which had been proposed until 2005 are summarised in a survey gathered by (Xiaoyuan et al. 2005).

In Table 2.4 few Graphical Password schemes has been gathered and categorised as recall-based and recognition-based schemes.
Table 0.4: Picture Based Password Methods

<table>
<thead>
<tr>
<th>Picture Based</th>
<th>Recall-Based</th>
<th>Recognition-Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reproducing a Drawing</td>
<td>Repeating a Selection</td>
<td>Déjà Vu</td>
</tr>
<tr>
<td>DAS</td>
<td>Blonder</td>
<td>Passfaces</td>
</tr>
<tr>
<td>Grid Selection</td>
<td>Pass-Logix</td>
<td>Story Scheme</td>
</tr>
<tr>
<td>Pass-doodle</td>
<td>Pass-Points</td>
<td>Challenge-Response</td>
</tr>
<tr>
<td>Syukri</td>
<td>Map Authentication</td>
<td>A WASE-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Convex-Hull</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pass-Pics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cognitive Trapdoor</td>
</tr>
</tbody>
</table>

### 2.5 Conclusion

Based on the reviews conducted in the field of Graphical Password resistant to shoulder surfing, the following points can be stated as a baseline for producing significant research:

1. Human brains can process graphical images easily. Thus, Graphical Password schemes provide a way of making more human-friendly passwords while increasing the level of security compared to other types of passwords (Kirkpatrick 1894; Calkins 1988; Madigan & Lawrence 1980; Wei-Chi & Maw-Jinn 2005).

2. It is difficult to implement automated attacks such as dictionary attacks, brute-force attacks and key loggers. This is because Graphical Password does not use textual data. Textual data is easier to predict compared with graphical data.

3. There are a few proposed methods to shoulder surfing attacks as described earlier in the section 2.4.2. In spite of the limited usage of Graphical Passwords to small screen devises, it is still a place for research.

4. The following is a brief explanation of the proposed system.
RBSR$^4$ stands for Recognition-Based Sequence Reproduction in 4-ways. Recognition-Based techniques depend on human memory to remember a specific secret. Sequence reproduction is to produce a given key according to a pre-known sequence during the registration process. 4-ways is a procedure where users at the Registration module will choose four different combinations of graphic items to represent their Graphical Password. User then base on the odd and even days of the week will choose one of the four dimensional ways. Such a combination of graphic item and the way of reading will be used as the Graphical Password for the users in the phase two of the Login module. After a proper design and validation is conducted, the proposed algorithm is to be implemented as a server application.

RBSR$^4$ is resistant to shoulder surfing because users do not have to click, or draw anything and the images are difficult and a little bit confusing to be captured by a shoulder surfer. Moreover, users are required to provide a Pass-String in which they specify the number of their password in either columns or rows according to the chosen direction in the Registration module. This algorithm relies on server variables and not only on user data. The system includes two phases. In the Registration module, the user chooses 4 icons as his password between N numbers of images shown on the screen. They have to mention which direction they will use for different days, Left to Right, Right to Left, Bottom to Top and Top to Bottom. To increase the security we combine odd and even days (Saturday, Monday, Wednesday and Friday are considered as even days and Sunday, Tuesday and Thursday are considered as odd days) to these directions, for example choosing even days plus Right-Left or odd days plus Left to Right. This remains in the server not to reveal to the intruder. In the Login module the user has to key in his password K times, each time the place of icons will change randomly and according to date they type numbers of icons in each row or column in the specific chosen direction. K and N should be selected to justify high security on one hand and high usability on the other hand.

Upon completion, the system will be tested against known attacks such as shoulder surfing, guessing and social engineering. In addition, a user survey will be conducted to validate the algorithm's usability. According to (Eljetlawi & Ithnin 2008) the set of usability features that has to be considered in Graphical Password techniques includes ease of use, memorise, creation, learning and satisfaction. The password should
be easy for the user to memorise and to recall it after a few weeks. The whole system especially the interface has to be satisfying and acceptable by the user. Learning of how to use the overall system has to be easy and fast (Qibin et al. 2008).

Table 0.5: Summary of Graphical Password schemes

<table>
<thead>
<tr>
<th>Features</th>
<th>Security</th>
<th>Usability</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Multi-Factor</td>
<td>resistant to guessing, traditional key-loggers, weak password, shoulder surfing</td>
<td>not very easy to remember as user choice is not involved</td>
<td>being seized by complex spywares</td>
</tr>
<tr>
<td>A Remote User Authentication Scheme based on Draw-A-Secret</td>
<td>resistant to dictionary attack, replay attack, password-file compromise attack, the denial-of-service attack, the predictable $n$ attack, and the insider attack, it is reparable</td>
<td>good usability</td>
<td>might be hard to remember</td>
</tr>
<tr>
<td>Random Geometric Graphical Password (RGGPW)</td>
<td>resistant to guessing and forgery attacks, shoulder-surfing, phishing, large enough password space to be resistant against brute-force search attack, social engineering, spyware cannot capture mouse clicks, resilient against key logger</td>
<td>easy-to-recall, hard to guess, All images can be created fast whenever they are required, does not need any database</td>
<td>n/a</td>
</tr>
<tr>
<td>An Interactive and Secure User Authentication Scheme for Mobile Devices</td>
<td>resistant to shoulder surfing attack, more password entropy</td>
<td>easy and fast to remember</td>
<td>n/a</td>
</tr>
<tr>
<td>Association-Based Graphical Password</td>
<td>resistant to shoulder surfing attack</td>
<td>easier and faster to remember</td>
<td>password entropy being small, weak against guessing attacks</td>
</tr>
<tr>
<td>Jetafida</td>
<td>they never tested the security of their system but based on my understanding it doesn’t have high security and this is an area to work on in the future</td>
<td>ease of use, easy to create, easy to memorise and learn, good design and layout</td>
<td>limited number of images shown on the screen each time</td>
</tr>
<tr>
<td>Features</td>
<td>Security</td>
<td>Usability</td>
<td>Comments</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td><strong>GP Schemes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3-D password</strong></td>
<td>resistant to guessing attack, social engineering, unable to written down, not difficult to change or cancel the password, large password space</td>
<td>memorise easily, good usability</td>
<td>still not resistant against shoulder surfing</td>
</tr>
<tr>
<td><strong>A Stroke-based Textual Password Authentication Scheme</strong></td>
<td>resistant to brute force, shoulder surfing attacks, difficult to guess, Random clicking is difficult</td>
<td>high usability, good memorability</td>
<td>Low speed, users tend to choose weak passwords</td>
</tr>
<tr>
<td><strong>Challenge-Response Identification</strong></td>
<td>resistant to shoulder surfing</td>
<td>low memorability</td>
<td>hard to memorise</td>
</tr>
<tr>
<td><strong>Cognitive Trapdoor Games</strong></td>
<td>resistant to shoulder surfing</td>
<td>good memorability, not very high usability</td>
<td>long time to be solved</td>
</tr>
<tr>
<td><strong>Convex-Hull Scheme</strong></td>
<td>resistant to shoulder-surfing, randomly clicking or rotating</td>
<td>needs training to memorise faster, good usability</td>
<td>slow login process, small probable password space</td>
</tr>
</tbody>
</table>

The proposed system in this paper:

| **RBSR^4** (Recognition-Based Sequence Reproduction) | resistant to shoulder-surfing attack, resistant to guessing attack and social Engineering | good usability, memorability, user satisfaction | other security and usability measures should be tested |

Table 2.5 summarised all reviewed papers, specifying the usability and security features by mentioning a few comments on each method.
CHAPTER 3  Methodology

In chapter 2 we have reviewed issues about alphanumeric passwords and related literature to identify possible solutions and remaining problems. In this chapter we will present a software methodology which will help us to structure, plan, and control the process of developing the proposed system. The chosen methodology has different phases which will be explained throughout the chapter. Besides that, flowchart will help us to illustrate the algorithm of the stepwise process of our system.

3.1 Software Methodology

There are various types of frameworks. Each one of them is suitable for different projects based on their specific considerations. In developing information systems, the Systems development life cycle (SDLC) is known to be the conventional formalised methodology (Elliott 2004).

3.2 Software Methodology Approach

We need to conduct an approach which reduces the time of developing the system and the same time increases its quality. Therefore, we will summarise our study on few different approaches by indicating their advantages and disadvantages to choose either one. Researchers generally use the following software life cycle models as their software methodology:

- Waterfall: linear framework type
- Prototyping: iterative framework type
- Incremental: combination of linear and iterative
- Spiral: combination of linear and iterative
- Rapid Application Development (RAD): iterative

In the next part linear, iterative and combination if these two development methodologies will be determined throughout the brief discussion on three chosen software life cycle methods.
3.2.1 Waterfall

This model includes requirements analysis phase as the beginning of the development, followed by the design phase and implementation is the next phase. Testing and evaluating of the system comes before integration and maintenance. Each of the phases completes and starts the next phase right after that. Planning, time schedules, target dates, budgets and implementation of an entire system are important at the same time (Royce 1970; Larman & Basili 2003). Figure 3.1 shows a basic waterfall model.

![Waterfall Model](image)

Figure 0.1: Basic Waterfall Model (Smith & Sarfaty 1993) and (Dennis et al. 2006)

3.2.2 Prototyping

It is a framework of the process of the software development when it is yet to be completed. The goal of this method is to make the process of the system simpler by dividing into smaller parts and reducing the risk. This method is useful when the requirements are not cleared at the beginning. To have user satisfied with the final system they are involved in each part of implementation and the development of the system. Three steps of analysis, design and followed by the implementation are carried out continually in a cycle till the completion of the system. Figure 3.2 illustrates a life cycle model of a system with prototyping model (Parida 2006; Shelly et al. 2008). This model is called iterative and in contrast with linear it means, “Rework scheduling strategy in which time is set aside to revise and improve parts of the system” (Rauterberg 1992; Sorensen 1995).
Figure 0.2: Prototyping Model (Parida 2006; Shelly et al. 2008)

3.2.3 Spiral

The model combines both linear and iterative system development methodologies. It includes components of both waterfall and prototyping models. Therefore, the customer’s opinion is involved during the design and the implementation of the system. Researchers use spiral life cycle model for big complicated pricey projects. Figure 3.3 illustrates a simple spiral model (Boehm 1985). Each cycle includes four steps of analysing, designing the system, development, evaluation and planning the next cycle. Finally the concentration of the whole spiral process is on decreasing the risk. Therefore the phases are separated from each other to reduce the risk on developing the system at one time (Sorensen 1995).
3.3 **Waterfall Model as the Software Methodology Approach**

Waterfall model explains a linear development method that is characterised by a regular sequence. It is a top to down development which has independent phases. Ultimately waterfall model has been chosen between all those commonly used methods. It is known as the original SDLC (System Development Life Cycle) method. In this methodology, the long time interval between the analysis phase and the delivery of the system is noticeable and this is because recognising system requirements before starting to program the system takes longer time and any step must be done accurately as we cannot go back over the steps when there is a problem (Dennis et al. 2006). Moreover, our system does not need any iterative development as there is no need to be in communication with the customer during the design phase. Therefore, we did not choose the prototyping model. In addition, it is very important to follow a methodology that saves our time in terms of delivering the model. Therefore we use the waterfall model where the requirements and the implementation of them are clear enough from the beginning to the end. Besides, we did not choose the spiral model as our system is small and there is no complication in it.

Figure 3.4 illustrates an advanced waterfall model (Smith & Sarfaty 1993; Dennis et al. 2006).
For our software methodology we chose to have the four phases in the waterfall life cycle model which are requirement analysis, design, coding (developing and implementation of the system), and its last part is the testing and evaluation of the whole system.

The following Figure 3.5 shows the cycle of the waterfall model for bigger projects. It divides the project to subprojects. Each subproject includes separate design and implementation phases. Finally there is an overall implementation to prepare delivering the whole system.

The project will be divided into different recognisable subprojects to be programmed. However, the overall design is performed before that (Dennis et al. 2006). From Figure 3.5 the reason of the extended time interval between analysis phase and delivering the system is understandable.
The following subsections briefly discuss the tasks involved in each phase of the development cycle.

3.3.1 Phase 1 – Requirements Analysis

In the requirements analysis phase the problem of the system is studied. Based on analysis results the functional requirements, non-functional requirements, hardware, and software requirements from user’s points of view are collected. Subsequently, the functions of the system are discussed in detail according to our objectives. The functional requirements are described using the DFD diagrams with two important phases that are, the Login and the Registration modules. Non-functional requirements specify the quality of the system in term of the systems security, usability probability, and reliability. Overall the analysis results are based on a comparative study on related resources.
3.3.2 Phase 2 – Design

The design phase focuses on the systems architecture design, program design, database design and the user interface design. The process involved in the system is described using diagrams, symbols and lines in detail in Chapter 4.

3.3.3 Phase 3 – System Implementation

In this phase, all design objectives are translated into a language that the machine can perform. The coding in the desired programming language should be done by considering the reliability of the system and the ability to improve it in the future. The chosen programming language is Java which is known as a reliable and a compatible language.

3.3.4 Phase 4 – System Testing

At the end we will evaluate the system according to all the requirements, functional and non-functional respectively. The testing activity includes the involvement of computer technical people and ordinary users who work in a real life environment. For each phase, the Registration and Login modules are tested against shoulder surfing attack and guessing attack separately to ensure error free software. The usability of the system will be tested by the aid of questionnaire forms to test the memorability, ease of use, and user satisfaction of the whole system. The results are gathered and documented carefully.

3.4 Conclusion

The methodology for the new system was reviewed in this stage. We have chosen the waterfall model as our system methodology. The tasks involved in the four phases of the waterfall model have been briefly explained. Chapters 4, 5 and 6 discuss the requirement analysis and system design, implementation and system testing respectively in details.
Requirement Analysis and System Design

Analysis on requirements includes functional and non-functional requirements. After completing the system analysis requirement we will commence the system design part which programs and the interface design are covered. By the aid of flowcharts the overall structure of our system is illustrated. Designing the system is the second part of this chapter. It is very important and essential as it establishes the foundation of our system, as of who will use the system, what the system will do, where and when it will be used. All of this is described in this chapter.

4.1 Requirements

The first part includes identification of what exactly the system needs, besides gathering and illustrating them according to user’s view point as functional requirements. Meanwhile we should keep in mind that the main problem is to define our objectives purely. Physical performance and quality specification of the system will also be part of the requirements analysis. Overall, it includes functional requirements, non-functional requirements, hardware, and software requirements from user’s point of view.

There are several important ways to gather requirements of the system which will help us to build the development bases. These techniques can be studied on similar projects through journals, published articles and specially literature reviews done so far which helps to find differences and similarities in contrast with our own system. Doing research on the Internet and libraries can be counted as another technique. The library of our university UM has provide us different useful databases such as IEEE, ACM, Science Direct, Springer Link and books to be borrowed or browsed inside the campus area. We have been using these valuable sources to document our research as delicately as we can. Not to forget about Google scholar search engine which contains necessary data that is suitable for our research.

4.1.1 Functional Requirements

Functional requirements can be defined by the aid of graphical diagrams. Three forms of representing the logical design of the system are as follows:
Each of these forms includes information on how the system should work, what are the inputs and outputs of the system and what kind of process will be done on the inputs (Yourdon 1970). We have chosen data flow diagrams and we will illustrate the flow of data in the Login and Registration modules in Figure 4.1 and 4.2 respectively. Note that data flow is shown with an arrow combined with a label. The process is the circle with label and boxes are information sources.

Figure 0.1: Data flow in the Login module

Figure 4.2 shows the data flow diagram for the Registration module. The data is stored in the database twice.

Figure 0.2: Data flow in the Registration module
4.1.2 Non-Functional requirement analysis

i. Portability

This aspect refers to the ability of running the system on various platforms. We will use Java programming language to develop our system. As all the operating systems can run software programmed by Java this aspect is guaranteed as long as Java platform exists.

ii. Security

Security refers to the resistance of the system against different kinds of attacks such as dictionary attacks, shoulder surfing attack, guessing, social engineering and several other attacks. In this research we will work on making the system immune as much as we can towards shoulder surfing attacks. We will test the system against some identity thefts like shoulder surfing, guessing and social engineering.

iii. Scalability

It is very easy to enhance the system as Java programming language is scalable enough to be changed and improved. Therefore, the only thing that any operating system needs is to have software and hardware requirements.

iv. Robustness

Our software should be able to respond to false inputs and produce error windows when needed.

v. Usability

This characteristic refers to user satisfaction of the whole system specially the user interface. Usability is one of the two important concepts we need to achieve by developing our system. Improving memorability, recall ability, and ease of use are our goals.

vi. Reliability

Reliability refers to the function of the system according to the requirements and its design. Java programming and MySQL have been widely used through years and there is no doubt that this database management system in communication with Java language delivers a high quality with low failure rates.
vii. Efficiency

The strength of the system that responds to user’s request which is inputting their username and password due to entering the system is called efficiency. At the same time the space that belongs to the database is also important and it comes out to be a major issue when the records stored increases.

viii. User friendliness

It is convenient for users to work with the system. Each page and window of the system will be designed in an easy and understandable way to be worked with. We will provide a short training course for users to understand how to use the system.

4.2 Architecture Design

In this part we will describe hardware, software, and network infrastructure that will be used in the system. Run time requirements are as following.

i. Software

- Windows XP Professional SP3,
- Java SE Development Kit 6 (JDK 6),
- NetBeans,
- MySQL 5.0 Server Edition.

ii. Hardware and Technology Consideration

- Pentium 4 processor or higher,
- Minimum of 2.0 GB of hard disk or higher,
- Minimum of 512 RAM or higher,
- VGA colour monitor,
- Standard keyboard as an input device.
4.3 Program Design

The development tools include the programming language that needs to be written and will be described in this part. We will explain as what they will do and why they have been chosen to develop our system.

4.3.1 Programming Language:

i. Java

Java can be referred to the programming language or Java platform. James Gosling developed the syntax of Java programming language from C and C++, although its object model is simpler (Kabutz 2007). According to a white paper Gosling and McGilton wrote in 1996 this high level language is Write Once, Run Anywhere (WORA) and has the following characteristics

- Simple
- Object Oriented
- Distributed
- Multithreaded
- Dynamic
- Architecture neutral
- Portable: By compiling the Java code to byte code, Java language can run on variety of operating system.
- Robust
- Secure
- Interpreted: An interpreter is a software program that executes the programming language which is not directly executed by the host CPU. In this case, the source code of the program is often translated to a form of machine language for a virtual machine. “Theoretically, any language may be compiled or interpreted. Java is translated to a form that is intended to be interpreted; just-in-time compilation is often used to generate machine code.” (Bangia 2006)
- Platform Independent
- High Performance
Java became the core component of Java platform in SunMicrosystem when it firstly made available to public in 1995. In the Java programming language, firstly we write all source code in plain text files with the .Java extension. They are then compiled into .class files by the javac compiler. A .class file contains byte codes which are the machine language of the Virtual Machine for the Java platform and they are called Java VM. Finally the Java launcher tool runs the application on any Java Virtual Machine with any computer architecture. Figure 4.3 illustrates an overview of the Java programming language we just explained (Gosling & McGilton 1996).

![Diagram](image)

Figure 0.3: An overview of the software development process (Gosling & McGilton 1996)

Sun introduced JDK, the Java Development Kit containing Java compiler, Javadoc, Jar and debugger which are known as development tools. Java Programs are slower and requires more memory comparing to other languages (Jelovic & Dejan 2008). In 1998 by introducing Just-in-time compilation the speed of executing the program improved considerably.

“Java libraries are the compiled byte codes of source code developed by the JRE implementer to support application development in Java. These libraries are as follows: The core libraries, the integration libraries, and user interface libraries.” (Gosling et al. 2005)

4.3.2 Database Design:

1. **MySQL 5.0**

Database management systems, MySQL version 5.0 is our choice for database storage which is widely used in various applications. It is also an open source,
distributed and supported by Sun Microsystems. Figure 4.2 shows our data flow of our system in the Registration module.

- MySQL server is a database management system that is used to have access and process on stored information in a database. Different kinds of data can be collected in the database storage from a character and number of images and pictures. This server can be part of an application or can work as standalone.
- MySQL is a RDBMS which relies on SQL and provides APIs for several languages such as C++, Java, Perl, PHP, and Tcl. SQL is abbreviation for “Structured Query Language.” To have more speed and a flexible large database the way relational databases collect data in distinct tables.
- MySQL software is Open Source means downloading and modifying is available through the internet.
- The MySQL Database Server is known as a dependable secure server that is also reachable from everywhere through the internet and to be changed if needed using a rich set of functions.
- MySQL Server can be client/server system or an embedded one along with supporting any kind of operating systems and APIs and being used for various applications.

4.4 System Design

In this part we will design the technical architecture requires to support the system. In order to make it easier for end users and developers of the system, it is necessary to choose diagrams.

4.4.1 Flowchart as our Modelling Language

System analysers and designers use variety of diagrams to explain how the system works and how the data flows. Between flowcharts, context diagrams, network diagrams, data-flow diagrams and entity-relationship diagrams; Flowchart has been chosen as a schematic representation of an algorithm or a process. It focuses on what the system does and also different steps of the system process attached together. The kind of data for input, output and the stored place is not under consideration when drawing a
flowchart. It is simple to understand the information and follow it. The Registration and Login module are illustrated in Figures 4.5 and 4.6 respectively. The arrows show what step comes first and which one should be taken after it. In this kind of diagram, problems can be figured out easier. Most flow charts contain three major figures namely circle, rectangle, and diamond shapes represent the start or end of the process, rectangles to show actions or instructions, and diamonds are used as decisions that have to be made (Goldstine & Neumann 1947).

4.4.2 RBSR^4 Data Flow Diagrams

Figure 4.4 illustrates an overview of RBSR^4 design that covers both Login and Registration modules.
Figure 4.5 illustrates the process of the Registration module in RBSR system.

Figure 0.5: Register Sequence Flowchart
The second and last module in our system is the Login module where its process is as shown in Figure 4.6.

![Login Sequence Flowchart](image)

**Figure 0.6: Login Sequence Flowchart**

### 4.5 Conclusion

The deliverable of this chapter will be an analysis of the requirements and an initial design for the new system. How the system will operate in terms of the software, hardware, and network infrastructure; and the specific programs, databases and files that will be needed.
CHAPTER 5 Implementation

5.1 Introduction

The implementation phase is the most costly part of the research as it brings the analysis and design part to an action means that it requires buying software and hardware tools. It will take a longer time to program the system and run it as debugging is necessary. The end deliverable of this phase is the RBSR³ system. This chapter describes the implementation phase in details.

In this phase we will transfer the designs to actual development of the system by translating them into code. Compilers, interpreters, and debuggers are the tools that helped us in programming. With respect to the type of application, Java is the right programming language which we have chosen, in regards to the kind of computer program design.

In this part we will explain two main modules of the system; Registration module and Login module. Each module has two phases; phase one and phase two.

Registration module includes the following steps:

1. Filling up the form.
2. Choosing the direction of password.
3. Choosing the password.
4. Checking the availability of the password.
5. Confirming password

If there was no error then the Login module will appear and it includes these steps:

1. Entering the username.
2. Entering number of passwords in each column or row.
3. The user will be authenticated if the password is correct and will be logged into the system and the system will show his information on the screen.
5.2 Registration Module

This is the first window that appears for logging into the system. If the user has already registered, then the user types in his/her username and clicks on the Login button. Otherwise the user has to click on the New User button which will take the user to the New User page illustrated in the Figure 5.2 to create a username and profile.
This is the Registration module. Providing personal information for user profile, the password and its order are two main parts of this phase.
Compulsory fields should be filled up with information. In this system the only field that should not remain empty is the username field and of course the password. The order of password for both odd and even days is on the first option, left to right, by default.
Users have to fill up the form without any compulsory fields remaining empty. The email part must contain @ sign. In the date of birth any dividing characters can be used to show day/month/year.
As you can see the user needs to specify the password order. For more security we combined choosing passwords with the date. In the Login module for example on odd days like Sunday, Tuesday, Thursday the user chooses his password from left to right and for even days like Saturday, Monday, Wednesday and Friday he chooses right to left order. The user has to specify this information in the Registration module which will be saved in the server and never will be revealed again. The way of entering the password in the Login module will be explained later.
Next, the user will choose his password from 16 pictures on the screen. These images appear randomly from the database of 50 images. The last part in this window is checking on the password length and username availability.
Figure 0.7: Error according to choose a duplicate username

Username cannot be duplicated; therefore in case of availability of a username the system will pop up a warning window to the user telling him to change the username. Note that password length should be 4 pictures.
Figure 0.8: Changing the Username

When all parts are done without any errors, the system will go to the next page.
In our system the users have to confirm the password and its order chosen in the first part of the Registration module.
Password should be chosen carefully similar as in the previous window, the first part of Registration module.
Figure 0.11: Reselecting the Sequence of the Password

The figure shows that the order of the password needs to be chosen again after confirming the password.
Figure 0.12: Error due to choosing an incorrect password

An error window appears regarding selecting different information from the previous page.
Wrong information can be the order of the password, the password itself or the length of the password.
Figure 0.14: Error by choosing incorrect sequence for the password
Finally after successfully confirming the password, its order and length, the username will be added to the database and the system is ready to authenticate the user in the Login module.

5.3 Login Module

Figure 0.15: User is successfully added to the database
If the typed username could not be found in the database the system will notify the user by telling him that the username is not valid.
By entering the correct username, the system will take the user to the next page of the Login module. In Figure 5.18 the message is showing not valid username which is from the previous incorrect username.

Figure 0.18: Correct Username
The most important part of our system is entering the correct password which relates to the order of password chosen in the Registration module by the user. We will explain it by a simple example. Assuming today is Monday which is an even day. According to the Registration module of this user for even days the user chose down to top order. Therefore he has to look for number of his passwords from the lowest row of the images.
If the user enters a wrong password, error window will pop up notifying him.
By typing the right numbers of the password which the sum of those numbers gives the password length, the information in the users profile will appear on the screen and the system welcomes the user! There is a logout button which takes the user to the first page of the system that is the main page of the Login module.

5.4 Conclusion

The implementation of this system has been illustrated by the aid of snap-shots in two sections; Registration and Login modules. Each and every step taken in the system by the user has been explained in detail.
CHAPTER 6  Testing and Evaluation

6.1 Introduction

In this chapter the results obtained for testing our system will be presented. This is the final stage in the waterfall life cycle development model. The system is tested to confirm its performance according to the system requirements outlined in Chapter 4. There are two main sections in this chapter. The first section comprises the testing procedures carried out on the system design. The latter part covers the usability and security evaluation.

Both modules were tested during the implementation phase. The system is tested as a whole after the modules were combined and the system is completed.

In our system, both usability and security are of equal significance. Therefore, naturally it was tested by gauging the users’ point of view. At the same time, the system was also tested against shoulder surfing attack and guessing attack. To do so, a questionnaire survey was carried out for usability and security, as well as a form for shoulder surfing attack. The results will be illustrated in separate tables within the chapter.

6.2 Testing the Design of the System

In this part, the performance of RBSR^d (Recognition Based Sequence Reproduction) was tested. For each Registration and Login module and their phases test cases are depicted separately in appropriate tables. Moreover, separate arguments for user the ID and password are also laid out.
<table>
<thead>
<tr>
<th>Test Argument</th>
<th>Expected Result</th>
<th>Actual Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Run Registration page for new user</td>
<td>page displayed</td>
<td>ok</td>
</tr>
<tr>
<td>2. Registration successfully done when all compulsory fields are filled up</td>
<td>error message: username cannot be empty</td>
<td>ok</td>
</tr>
<tr>
<td>a. username should be chosen</td>
<td>a message will be displayed to change the username</td>
<td></td>
</tr>
<tr>
<td>b. duplicate username</td>
<td>will not be able to login to the system</td>
<td></td>
</tr>
<tr>
<td>c. no password chosen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. username and password is stored in the database after registration</td>
<td>information stored in the database</td>
<td>ok</td>
</tr>
</tbody>
</table>

The Registration module was tested during the implementation phase, as well as when the system was completed. This part is used when users do not have any user ID and password. It includes a form to be filled out with the user’s personal information, password, password direction and it will check on the username. The password and username part is depicted in the following tables.

Usernames should be unique, so when the user types in a username, the system will check with the database to ensure that it is not duplicated. The system will also check whether this field is empty or not, and will show an error message to the user in the event that it is left blank.
The password is the primary part of the system. Each module is tested, at the Registration and Login as to how the password is working. As explained before, the system combines password with the odd/even days and the user has to choose different directions for different days (Refer to page 54). The user has to confirm the password in the Registration module after selecting it.

<table>
<thead>
<tr>
<th>Test Argument</th>
<th>Expected Result</th>
<th>Actual Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. display 16 images</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. on the first page of Registration</td>
<td>-page displayed</td>
<td>ok</td>
</tr>
<tr>
<td>b. on the confirmation page</td>
<td>-page displayed</td>
<td>ok</td>
</tr>
<tr>
<td>2. maximum password length 4 characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. password length &lt; 4</td>
<td>-Password allowed</td>
<td>ok</td>
</tr>
<tr>
<td>b. password length =4</td>
<td>-Password allowed, system takes the user to the next page.</td>
<td>ok</td>
</tr>
<tr>
<td>c. password length&gt; 4</td>
<td>-Password not allowed.</td>
<td>ok</td>
</tr>
<tr>
<td>3. password confirmation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in Registration module password confirming images should be same as the first chosen 4 images</td>
<td>-if not the same password, a message will be displayed to inform the user.</td>
<td>ok</td>
</tr>
<tr>
<td>4. password direction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. two directions should be chosen</td>
<td>-by default both directions for odd and even days is on the first option, left to right.</td>
<td>ok</td>
</tr>
<tr>
<td>5. password direction confirmation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. in Registration module password direction should be same as the chosen one in the first page of Registration module</td>
<td>-if not the same direction, a message will be displayed to the user.</td>
<td>ok</td>
</tr>
</tbody>
</table>
Table 0.3: User ID test case

<table>
<thead>
<tr>
<th>Test Argument</th>
<th>Expected Result</th>
<th>Actual Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. valid username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. sign in with blank username field</td>
<td>-error message: username not valid</td>
<td>ok</td>
</tr>
<tr>
<td>b. sign in with wrong username</td>
<td>-username not valid error message will be displayed</td>
<td>ok</td>
</tr>
<tr>
<td>c. sign in with appropriate username</td>
<td>-access allowed to enter the password</td>
<td>ok</td>
</tr>
<tr>
<td>d. sign in as any other username</td>
<td>-cannot setup the password</td>
<td>ok</td>
</tr>
</tbody>
</table>

The username case in Registration module was discussed and tested in Table 6.1. As for Login module the users must provide their own username otherwise the system will show an error message on the screen.

Table 0.4: Login module test parameters

<table>
<thead>
<tr>
<th>Test Argument</th>
<th>Expected Result</th>
<th>Actual Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. run the Login page</td>
<td>-Login page displayed</td>
<td>ok</td>
</tr>
<tr>
<td>2. username</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. if valid username</td>
<td>-takes user to enter password numbers</td>
<td>ok</td>
</tr>
<tr>
<td>b. if not valid</td>
<td>-displaying appropriate message</td>
<td>ok</td>
</tr>
<tr>
<td>3. password numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. if correct</td>
<td>-authenticates the user and displays user’s information with a welcome message.</td>
<td>ok</td>
</tr>
<tr>
<td>b. incorrect password numbers</td>
<td>-displays error message to the user</td>
<td>ok</td>
</tr>
<tr>
<td>4. new user button</td>
<td>-takes the user to the Registration module</td>
<td>ok</td>
</tr>
<tr>
<td>5. logout button</td>
<td>-closes user’s information page and opens the first Login page</td>
<td>ok</td>
</tr>
</tbody>
</table>
This table illustrates the tests done in the Login module. It includes all parameters that were designed and implemented for the Login module of the system. It shows that all the test cases are working properly as expected. The system is now ready to use.

### 6.3 Usability and Security Study

In this part of the system, the results of acceptance testing of the system were gathered according to security and usability measurements as defined in the literature review in Chapter 2. The respondents to our questionnaire survey were 15 IT students and non IT people. The questionnaire is attached as an addendum to this document. In this part, the usability goals evaluated were learnability, memorability, efficiency, security, and user satisfaction.

Learnability: A user manual was provided (See Chapter Five) to guide the user to learn to use the system and at the end, they were asked to respond about their learning process of the system to gauge the level of ease in using the system.

Memorability: It is very important for users of the system to recall their password fast and easily. This parameter was tested right after users created their respective account.

Efficiency: The speed of the Login process has to be considered as the researchers proposed graphical authentication systems to be used as a solution to textual password weaknesses.

Security: The newly designed system is immune from social engineering attacks in a way that users cannot jot down their password or pass on any information about it to anyone.

User Satisfaction: This parameter was tested against the overall user interface of the system and whether or not the users are willing to use such authentication system from then onwards or in the future.
In the table below the results that corresponds to the above usability goals are laid out.

Table 0.5: Security and Usability Questionnaire

<table>
<thead>
<tr>
<th>Questions</th>
<th>Satisfying</th>
<th>50% Satisfying</th>
<th>Not Satisfying</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Easy to follow the steps of Registration?</td>
<td>15</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2. Easy to learn how to use the system?</td>
<td>14</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>3. Fast to register?</td>
<td>13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4. Fast to login to the system?</td>
<td>15</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5. Easy to memorise the password?</td>
<td>11</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>6. User interface design satisfaction?</td>
<td>13</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>7. Easy to create the password?</td>
<td>12</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

It is evident from the table above, users had problems memorising the password. Most of them have not had any experience using Graphical Passwords before. This is the main reason why they had difficulty recalling their passwords. The system was tested among masters and undergraduate students. For the undergraduates more time was spent teaching them to use the system. There were two web design experts among the respondents who made additional comments on the user interface.

We gathered a few users’ specification who commented on our system wisely in the table below. More discussion on the results will be concluded in the last part of this chapter.
<table>
<thead>
<tr>
<th>Users Specification</th>
<th>Comments on usability study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master of Computer Science (Information Technology)- UTM</td>
<td>- I learnt the system fast but I needed time to get used to it.</td>
</tr>
<tr>
<td></td>
<td>- Although the memorability of system decrease, but according to me it will be more resistant to common attacks of GP, so memorability is medium.</td>
</tr>
<tr>
<td>Master lecturer of IT- Limkokwing</td>
<td>- Before this project I did not have any idea about Graphical Password system.</td>
</tr>
<tr>
<td></td>
<td>- Thank you for your friendly relation and inviting us in your project, test and evaluation.</td>
</tr>
<tr>
<td></td>
<td>- It was a good idea and developed with a good design.</td>
</tr>
<tr>
<td>Master of Computer Science- UM</td>
<td>- This is my first time that I used Graphical Password.</td>
</tr>
<tr>
<td>Master of Virtual Reality- UKM</td>
<td>- Sometimes I had difficulty to memorise the pictures.</td>
</tr>
<tr>
<td>Master of Multimedia- UKM</td>
<td>- I had no idea about Graphical Password therefore I had some difficulty at the beginning.</td>
</tr>
<tr>
<td>Master of Augment Reality- UKM</td>
<td>- It was simple to follow the steps.</td>
</tr>
<tr>
<td></td>
<td>- It was simple for me to learn the system.</td>
</tr>
<tr>
<td></td>
<td>- The Registration module was easy.</td>
</tr>
<tr>
<td></td>
<td>- Sorry I am web designer for 5 years then the design was hard to accept.</td>
</tr>
<tr>
<td>Master of Information Security- UKM</td>
<td>- Very easy to follow the steps.</td>
</tr>
<tr>
<td></td>
<td>- Simply fast to register.</td>
</tr>
<tr>
<td></td>
<td>- I am not familiar with this type of passwords but it was okay.</td>
</tr>
<tr>
<td>Master of IT- UITM</td>
<td>- I had problem with images always.</td>
</tr>
<tr>
<td>Master of ICT- Limkokwing</td>
<td>- I think your proposed method is so simple and good.</td>
</tr>
<tr>
<td></td>
<td>- I think it will be secure as well.</td>
</tr>
<tr>
<td></td>
<td>good luck</td>
</tr>
<tr>
<td>Bachelor of Law- Help College and University</td>
<td>- I am not familiar with Graphical Password but it was fun using the system.</td>
</tr>
</tbody>
</table>


| Bachelor of Software Engineering- UM | - The images can be improved. |
| Software Engineering- UM | - Why not improve your system so that users can upload their own familiar pictures. |
| Bachelor of Computer Science- UM | - Sometimes it is confusing to memorise the password. |
| Bachelor of Networking- UM | - It took some time for me to register. |
| Bachelor of Software Engineering- UM | - Too many graphic, we can use simple images maybe. |
| Bachelor of Software Engineering- UM | - Need to understand carefully the instructions given by the developer. |
| Bachelor of Software Engineering- UM | - The images seem similar to each other. |
| Bachelor of Software Engineering- UM | - I had to memorise the pictures, it is quite difficult. |

### 6.4 Shoulder Surfing Attack Test

Eight users were involved to carry out the shoulder surfing attack. The research team had to train and help users to use the system and then perform the attack test. The screen includes 16 images out of 50 from the database which were randomly displayed. One person was assigned as the user of the system who had to login and another person was assigned to stand behind and watch carefully to find out the password. The attack was performed 5 times for 4 users and the results are shown in Table 6.7.

<table>
<thead>
<tr>
<th>Users Attacks</th>
<th>First</th>
<th>Second</th>
<th>Third</th>
<th>Fourth</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Second</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Third</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fourth</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fifth</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The table above shows the results of five attacks to 4 users with different passwords. The rate of success is equal to zero for the whole evaluation. The
comparison results of guessing attacks are presented in the table below. The next section, conclusion will provide our comments and discussion on the security tests.

Table 0.8: Guessing Result for shoulder surfing attack

<table>
<thead>
<tr>
<th>User</th>
<th>First</th>
<th>Second</th>
<th>Third</th>
<th>Fourth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of guessed Password</td>
<td>1 out of 4</td>
<td>0 out of 4</td>
<td>1 out of 4</td>
<td>1 out of 4</td>
</tr>
</tbody>
</table>

6.5 Conclusion

This chapter documents the evaluation results of the implemented Graphical Password authentication system. The purpose of testing is to ensure that the system works properly and the problem statement has been solved. The design of the system, the security, and usability aspects were tested. The results of testing is analysed to increase the quality of the system.

There is a high possibility that in the case of selecting simpler images and using them as current pictures in our system for the password part, the memorability increases and users can memorise and recall better.

Moreover, from the security test, the results show that there is a slight possibility of guessing attacks. As we did not have any camera to capture the passwords the possibility of shoulder surfing attack dropped to zero percent which is very satisfactory.

Regarding the guessing attack issue, it was found out that if the number of pictures in the database increase therefore variety of pictures will be shown in the Login screen as well and eventually the possibility of guessing attack will decrease and it will be difficult for intruders to find out the exact password pictures.

In addition, capturing the mouse click with electromagnetic pulse scanner will not affect the security of our system as there is no place to use the mouse and click on the screen to choose the password in Login module. Although in Registration module the password has to be chosen by clicking on four images which in this case the information will be stored in the database in the server side and will never be used again.
Furthermore, as the image selection was based on variety of colours and shapes. According to our results while observing users in the test it is very difficult for the user to write down their password and share it with others even it is not possible at all.

Finally, the research team has fulfilled the last objective of this research and in the next chapter will bring forth a brief conclusion of the whole research and provide some further research suggestions for possible future work.
CHAPTER 7  Conclusion

This chapter will conclude the research and the results of this research. There will be four parts which will comprise the summary of the research and summary of the research findings and the latter part will discuss further works in the conclusion and recommendations sections.

7.1 Summary of Research

An extensive search had been done on security area to discover what can be the hot topic that recently researchers are working on. Later on we chose to study on the literature review related to authentication systems field to find out the major problem that it is still there for a better solution to be overcome. We have gathered all the information about it in chapter 2. At the end of the chapter we concluded our review in a table that contains security and usability parameters gained in each method and we have written down our comments about each one of them. We also have written several journals and conference papers regarding our topic and related literature review. Those papers include a wide survey on usability, security features in graphical authentication schemes both on recall-based and recognition-based types.

In the third chapter the methodology for this research was introduced and explained. For the purpose of this research, the waterfall model was chosen to complete the system development life cycle. The four phases involved in this process was also discussed briefly.

To follow that, the next chapter includes the requirement analysis and software design. The proper functional and non functional requirements were also gathered and are outlined in this chapter and through the aid of flowcharts the mechanism of the system was illustrated.

Chapter five was further demonstrated every single operation that takes place in the system. A detailed description on the functionality of RBSR was also laid out here.

The main part of the research studied how the system works and whether in its entirety it actually satisfies the requirement analysis described in Chapter 4. More
importantly, this chapter was further detail the steps that have been undertaken to evaluate the system against usability features and security needs in order to ensure that the research objectives have been achieved and that the weaknesses of previous password schemes were overcome.

Finally a brief conclusion of the research shall be discussed here in this last chapter.

7.2 Summary of Findings

The anticipated end result of this research is an authentication system with Graphical Password access control mechanism which can overcome usability and security problems of previous password schemes especially that of textual nature.

i. Objective 1

The authentication system is expected to be robust against shoulder surfing as at the same time difficult for attackers to guess the password. This research strived to take into account the advantages and disadvantages of previous authentication systems especially existing Graphical Password methodologies and finally developed an extensive one unique to the current research. Therefore, it combined other several factors like odd/even days with the password, to gain higher security for making it difficult for an intruder to guess the password as well as, for a shoulder surfing attacker to find out a user’s password.

Furthermore, while testing the system it was found that if the number of pictures in the database increases, various 16 pictures will appear each time on the screen and therefore the guessing will become more difficult for an attacker.

Moreover, as there is no need to click on the screen in the second phase of the Login module to choose the password, therefore the system is not vulnerable to tools which capture mouse clicks.

In addition, there is no possibility of social engineering as the passwords are
difficult to be written down and shared with others.

ii. Objective 2

The features of being easily memorised, easily learned and used were also addressed and evaluated in this research. After spending 5 to 10 minutes training users, they were able to use the system without any problems. Overall, the user study has proven that RBSR is quite easy to memorise as only 16 pictures will be displayed on the screen for the users to choose four pictures as their passwords among them. The system is easy to use and fast to learn as there are only few steps to follow. The research team provided a comprehensive training for the users involved. Moreover, the research team made a concerted effort to design a satisfying user interface and as the results have demonstrated, the team has gained more of the users’ satisfaction with the system.

7.3 Research Contributions

The system has previously been introduced and the followings are the research contributions:

i. Usability: in this research, the team has identified the exact parameters that can be counted as usability variables from review of literature that was carried out and then designed and tested a scheme that contain all the said parameters.

ii. Security: by studying authentication methods possible attacks were identified. The research team selected the most problematic ones for the conventional password and proposed a graphical one to make it robust against known attacks, shoulder surfing and guessing.

iii. In the effort to balance these two features mentioned above, usability and security: the most important goal was the effort made to have both usability and security together in one system, to have a graphical authentication system that is robust against shoulder surfing and at the same time gain user satisfaction in learning while having an appealing user interface.
iv. Practicality: the designed system has an immense potential to be utilised in environments and organisations that require a secure and user-friendly authentication and authorisation system.

### 7.4 Conclusion and Recommendations

In conclusion, from the testing part the researchers have noticed that because most of the users did not have any experience using a graphical authentication system, they noted that simpler pictures can increase their level of recall and some suggested adding a possible feature that is to upload their own pictures makes recalling the password faster. Finally, despite achieving the main objectives, there are still areas to improve within the system in order to achieve better results.

#### 7.4.1 Further Research

Areas that have been identified as possible areas worthy of further study to make future improvements can be:

i. A study of how different kinds of pictures in various colours that can be in the form of animals, objects, shapes used as Graphical Passwords can affect memorability.

ii. Further testing to be carried out on the system against other kinds of attacks such as sniffing, and dictionary attacks.

iii. Improving the user interface of the system to achieve a higher level of user satisfaction.

iv. Developing the reset password part of the system. This is another convenience to provide users using the system to recall their password in the event they forget or lose their password.

v. Finding the password entropy will cause in better realisation of the system strength.
REFERENCES


ISO (1985). *Information processing -- Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts*.


Ramesh bangia 2006, Internet and Web design, 2nd edn, pp. 234.


# Appendix A

<table>
<thead>
<tr>
<th>University:</th>
<th>Degree:</th>
<th>Major:</th>
</tr>
</thead>
</table>

## Usability Questions

<table>
<thead>
<tr>
<th>Usability Questions</th>
<th>Satisfying</th>
<th>Half</th>
<th>Not</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Easy to follow the steps of registration?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Easy to learn how to use the system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Fast to register?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Fast to login to the system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Easy to memorise the password?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. User interface design satisfaction?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B

University:
Degree:
Major:

Shoulder Surfing Attack File

Instructions: - Each attacker has to perform the attack 5 times for 1 user.
- Capture and write down an understandable description of the password.
- The last row of the table will be filled up by user.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>First</th>
<th>Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captured Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Original Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Third</th>
<th>Fourth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captured Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Original Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Fifth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captured Password</td>
<td></td>
</tr>
<tr>
<td>Original Password</td>
<td></td>
</tr>
</tbody>
</table>