A NEW ALGORITHM FOR GRAPHICAL USER AUTHENTICATION BASED ON ROTATION AND RESIZING

ARASH HABIBI LASHKARI

A THESIS SUBMITTED FOR THE MASTER OF COMPUTER SCIENCE IN DATA COMMUNICATION & COMPUTER NETWORKING
FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, UNIVERSITY MALAYA (UM)

Supervision By:

DR. ROSLI SALLEH

May, 2010
To
My unforgettable grandfather,
AHMAD HABIBI LASHKARI

My beloved parents and sister,
BAHMAN, ZEINAB, ZIBA

My lovely wife,
FARNAZ

And my cute son,
KOUROSH

With thanks for all the years of
Caring, love, and support.
Abstract

It is now beyond any doubt that USER AUTHENTICATION is the most critical element in the field of Information Security. To date, Text Based Password Authentication (TBPA) has shown some difficulties that users have tended to write passwords down manually or save them on hard disc. This tendency is caused by the passwords being strong and thus difficult to memorize in most cases. This has inadvertently given rise to security issues pertaining to attack.

Graphical User Authentication (GUA) has two symbiotic pillars as its foundation: USABILITY & SECURITY. The macro-concept of GUA is based on the human psychological factor that is images are more readily committed to memory than would TBPA’s. All GUA algorithms are made up of both usability and security aspects. Unfortunately none of the existing algorithms are able to cover both of these aspects at the same time.

The main purpose of this thesis is an algorithm that combines the usability & security features by Rotating and Resizing the Images. This algorithm process on the images which user select during login phase and show a different picture the original password of the user into a GUA. Whereas previously the GUA’s were at the log-in stage, this algorithm would be at the registration stage. On the other hand, unlike previous graphical user authentication algorithms, in this algorithm the images selected as passwords in the registration phase will be different from the images in log-in phase.

The usability features of implemented algorithm will be checked by a questionnaire survey based on ISO usability features that are defined in literature review. The attack resistance features will be evaluated by calculating the “Password Entropy” and “Password Space” and compared with the previous algorithms. These are the two major evaluation methods for graphical passwords. A comparison table for analysis will be created to compare previous algorithms with the proposed algorithm.
Keywords

Graphical User Authentication, Graphical password, multifactor graphical authentication, Usability Features in graphical password, Security Features in graphical password, Texture, Strong Password.
Acknowledgement

I would like to express my thankful to my supervisor in this research, Dr. Rosli Salleh, who provided valuable insight and the freedom to develop a solution on my own, yet gave excellent advice and guidance on how to focus on my thesis contributions.

My appreciation also goes to all of my teachers and lecturers who help me to understand the importance of knowledge and show me the best way to gain it, especially lecturers in Faculty of Computer Science and Information Technology of University of Malaya (UM) such as Assoc. Prof. Dr. Ling Teck Chaw, Assoc. Prof. Dr. Phang Keat Keong and Dr. Miss Laiha Mat Kiah.

Finally, I’d like to thank my parents who have given me every form of support I could ask for and only asked that I enjoy myself and find happiness in return.

Arash Habibi Lashkari

May, 2010
Publications

Journal Papers:

• “A survey on usability and security features in graphical user authentication algorithms”
  International Journal of Computer Science and Network Security (IJCNSNS), Vol.9, No.9; Special Issues for Computer Science and Communication Network and Security; September, 2009, Korea

• “Shoulder Surfing attack in graphical password authentication”
  International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, No. 2, 2009, USA

• “A wide-range survey on Recall-Based Graphical User Authentication algorithms based on ISO and Attack Patterns”
  International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, No. 3, 2009, USA

Conference Papers:

• “A complete comparison on Pure and Cued Recall Based Graphical User Authentication”
  The 2nd IEEE International Conference on Computer and Electronic Engineering (ICCEE), Publish by IEEE Computer Society and THOMSON ISI indexing, 2009, Dubai
Table of Contents

Chapter 1: Introduction

1.1 Background .................................................................................................................. 2
1.2 Project Motivation ......................................................................................................... 3
1.3 Research Problem Statement ......................................................................................... 3
1.4 Objectives of Project ...................................................................................................... 3
1.5 Project Methodology ..................................................................................................... 4
1.6 Scope of Project .............................................................................................................. 5
1.7 Research Outcome ......................................................................................................... 5
1.9 Project Overview ........................................................................................................... 6

Chapter 2: Literature Review ............................................................................................... 8

2.1 Introduction .................................................................................................................... 8
2.2 Graphical Authentications Methods .............................................................................. 9
    2.2.1 Pure Recall Based Techniques .............................................................................. 10
        2.2.1.1 Passdoodle Algorithm ................................................................................... 10
        2.2.1.2 Draw A Secret (DAS) Algorithm .................................................................. 11
        2.2.1.3 Grid Selection Algorithm ............................................................................ 12
        2.2.1.4 Qualitative DAS (QDAS) Algorithm .............................................................. 13
        2.2.1.5 Syukri et al. Algorithm ................................................................................. 14
    2.2.2 Cued Recall-Based Techniques .............................................................................. 15
        2.2.2.1 Blonder Algorithm ........................................................................................ 15
        2.2.2.2 PassPoint Algorithm ..................................................................................... 15
        2.2.2.3 Background DAS (BDAS) Algorithm .......................................................... 15
        2.2.2.4 PASSMAP Algorithm .................................................................................. 17
        2.2.2.5 Passlogix v-Go Algorithm ............................................................................. 18
        2.2.2.6 VisKey SFR Algorithm ............................................................................... 29
        2.2.2.7 Pass-Go Algorithm ...................................................................................... 20
    2.2.3 Recognition-Based Techniques ................................................................................ 20
3.1 Introduction ........................................................................................................... 41

3.2 Methodology of Research....................................................................................... 41
  3.2.1 Document Retrieval Method ........................................................................... 42
  3.2.2 Comparative Study Method ........................................................................... 42

3.3 Methodology of Design and Implement ................................................................. 43

3.4 Software Development Approach .......................................................................... 44
  3.4.1 Design and Implementing Activities ............................................................... 45
    3.4.1.1 Requirements .............................................................................................. 45
      3.4.1.1.1 Requirements Captures ......................................................................... 45
      3.4.1.1.2 Finding Actors and Use Cases ................................................................. 47
      3.4.1.1.3 Prototype User Interfaces ..................................................................... 47
      3.4.1.1.4 Structure the Use Cases Model ............................................................... 48
    3.4.1.2 Analysis ....................................................................................................... 50
      3.4.1.2.1 Analysis of Architecture ...................................................................... 50
      3.4.1.2.2 Analysis of Use Case ............................................................................ 50
      3.4.1.2.3 Analysis of Classes .............................................................................. 52
    3.4.1.3 Design ........................................................................................................... 53
      3.4.1.3.1 Design of Architecture ...................................................................... 53
      3.4.1.3.2 Use Case Design ............................................................................... 53
      3.4.1.3.3 Class Design ...................................................................................... 55
    3.4.1.4 Implementation ............................................................................................ 56
    3.4.1.5 Test ............................................................................................................. 57

3.5 Hardware and Software Requirements ................................................................. 57

3.6 Methodology of Test and Evaluation ................................................................... 58
3.6.1 Quantitative Approach ................................................................. 58

3.6.2 Qualitative Approach ................................................................. 58

3.7 Conclusion ....................................................................................... 59

Chapter 4: Design ................................................................................. 60

4.1 Introduction ..................................................................................... 60

4.2 Proposed Algorithm Conceptual Framework ....................................... 60

4.3 Proposed System Architecture Module ............................................. 61

4.4 GUABRR System Conceptual Design ............................................... 62

4.4.1 Framework of Proposed System ................................................. 62

4.4.2 Rotation and Resizing in Proposed System .................................... 65

4.4.3 Use Case Diagram ...................................................................... 66

4.4.4 Sequential Diagrams ................................................................... 66

4.4.4.1 “Log-in” Phase Sequence Diagram ...................................... 67

4.4.4.2 “Registration” Phase Sequence Diagram ............................... 68

4.4.5 Class Diagram ............................................................................ 68

4.4.6 Database Design ......................................................................... 70

4.4.6.1 Table Name and Functions ............................................... 70

4.4.6.2 Design of Tables .................................................................. 71

4.4.7 Data Flow Diagram (DFD) ......................................................... 73

4.4.8 Entity Relationship Diagram ...................................................... 75

4.4.9 GUABRR Structure Overview .................................................... 75

4.4.10 GUABRR Interface Design ....................................................... 76

4.5 Conclusion ....................................................................................... 77

Chapter 5: Implementation .................................................................... 78

5.1 Introduction ..................................................................................... 78
Chapter 5: Implementation and Interface Design

5.2 Implementation Model ........................................................................... 78

5.3 Implementation Technology .................................................................. 79
  5.3.1 Web Server ....................................................................................... 79
  5.3.2 Dot NET Technology ........................................................................ 80
  5.3.3 Database Language ......................................................................... 80

5.4 Interface Design ...................................................................................... 82
  5.3.1 Registration Interface (new user) ...................................................... 82
  5.3.2 Log-In Interface (Existing user) ....................................................... 83

5.5 Conclusion ............................................................................................... 86

Chapter 6: Test and Evaluate ....................................................................... 87

6.1 Introduction ............................................................................................ 87

6.2 Usability Test and Analysis ..................................................................... 87
  6.2.1 Questionnaire Structure ................................................................. 88
  6.2.2 Participants and Data Collection ..................................................... 90
  6.2.3 Questionnaire and Answers ............................................................ 90
    6.2.3.1 General Part of Questionnaire ............................................... 91
    6.2.3.2 Rotation Part of Questionnaire ............................................... 100
    6.2.3.3 Resizing Part of Questionnaire ............................................. 104
    6.2.3.4 Rotation and Resizing Part of Questionnaire ......................... 108
  6.2.4 Summary of Questionnaire Results ............................................... 112

6.3 Security test and Evaluation .................................................................. 113
  6.3.1 Graphical Password Space ............................................................. 113
  6.3.2 Graphical Password Entropy .......................................................... 114

6.4 Conclusion .............................................................................................. 116
List of Figures

Figure 2-1: An Example of Passdoodle Algorithm ................................................................. 11
Figure 2-2: Draw a Secret (DAS) Algorithm on a 4*4 Grid .................................................. 12
Figure 2-3: A Sample of Grid Selection Algorithm ............................................................... 13
Figure 2-4: A Sample of Qualitative DAS Algorithm ............................................................. 13
Figure 2-5: A Sample of Syukri Algorithm .............................................................................. 14
Figure 2-6: A Sample of Blonder Algorithm ........................................................................... 15
Figure 2-7: A Sample of Passpoint Algorithm ....................................................................... 16
Figure 2-8: A Sample of BDAS Algorithm .............................................................................. 17
Figure 2-9: A Sample of PASSMAP Algorithm ..................................................................... 18
Figure 2-10: A Sample of Passlogix v.Go Algorithm .............................................................. 19
Figure 2-11: A Sample of VisKey SFR Algorithm .................................................................. 19
Figure 2-12: A Sample of Pass-Go Algorithm ....................................................................... 20
Figure 2-13: A Sample of Passface Algorithm ....................................................................... 21
Figure 2-14: A Sample of Déjà vu Algorithm ......................................................................... 23
Figure 2-15: A Sample of Triangle Algorithm ....................................................................... 24
Figure 2-16: A Sample of Moveable Frame Algorithm ............................................................ 25
Figure 2-17: A Sample of Picture Password Algorithm .......................................................... 26
Figure 2-18: A Sample of Story Algorithm ............................................................................. 26
Figure 2-19: A Sample of WIW Algorithm ............................................................................. 27
Figure 3-1: Methodology of Research Diagram ...................................................................... 43
Figure 3-2: Methodology of Design and Implementation ....................................................... 44
Figure 3-3: Use Case Driven Model ....................................................................................... 45
Figure 3-4: Use Case Model of GUABRR .............................................................................. 47
Figure 3-5: GUABRR User Interface Design ......................................................................... 48
Figure 3-6: State Machine Diagram for “Messages” .............................................................. 48
Figure 3-7: Activity Diagram for “Registration” part ............................................................. 49
Figure 3-8: Four Main Steps of System Analysis .................................................. 50
Figure 3-9: The Communication Diagram For “Registration” Process .................. 51
Figure 3-10: Class Diagram .............................................................................. 53
Figure 3-11: “Registration” Sequence Diagram ................................................ 54
Figure 3-12: “Log-in” Sequence Diagram ....................................................... 55
Figure 3-13: Class Diagram of GUABRR ......................................................... 56
Figure 3-14: GUABRR Implementation Model .................................................. 57
Figure 4-1: The Propose System Architecture Model ....................................... 62
Figure 4-2: Framework of Proposed System ...................................................... 64
Figure 4-3: Rotation Process in the GUABRR Algorithm ................................... 65
Figure 4-4: Resizing Process in the GUABRR Algorithm ................................... 65
Figure 4-5: Rotation and Resizing Process in the GUABRR Algorithm ............... 66
Figure 4-6: Use Case Diagram in Layer 1 ......................................................... 66
Figure 4-7: “Log-in” Phase Sequence Diagram ............................................... 67
Figure 4-8: “Registration” Phase Sequence Diagram ...................................... 68
Figure 4-9: GUABRR Class Diagram .............................................................. 69
Figure 4-10: GUABRR System Database ......................................................... 71
Figure 4-11: “Images_Original” Table of Database ......................................... 72
Figure 4-12: “Images_Rotation” Table of Database ....................................... 72
Figure 4-13: “UsersInfo” Table of Database ................................................... 72
Figure 4-14: DFD Layer One ........................................................................... 73
Figure 4-15: DFD of “Registration” Phase as Layer Two DFD ......................... 74
Figure 4-16: DFD of “Log-in” Phase as Layer Two DFD ................................. 74
Figure 4-17: GUABRR System Entity Relationship Diagram ......................... 75
Figure 4-18: Empty Password Image Grid of GUABRR Algorithm .................. 76
Figure 4-19: Random Rotation and Resizing Images if grid in GUABRR Algorithm .... 77
Figure 5-1: GUABRR Implementation Model .................................................. 79
Figure 5-2: GUABRR Registration Page ......................................................... 83
Figure 5-3a: GUABRR Log-In Page Before Enter Username ........................... 84
Figure 5-3b: GUABRR Log-In Page After Enter Username ........................................ 84
Figure 5-4a: GUABRR Registration and Log-In Page by Using Rotation Technique ........ 85
Figure 5-4b: GUABRR Registration and Log-In Page by Using Resizing Technique ...... 85
Figure 5-4c: GUABRR Registration and Log-In Page by Using R&R Technique .......... 86
Figure 6-1: Data Collection Diagram for Q1................................................................. 91
Figure 6-2: Report of System on Q1 ........................................................................ 92
Figure 6-3: Data Collection Diagram for Q2............................................................. 92
Figure 6-4: Report of System on Q2 ........................................................................ 92
Figure 6-5: Data Collection Diagram for Q3............................................................. 93
Figure 6-6: Report of System on Q3 ........................................................................ 93
Figure 6-7: Data Collection Diagram for Q4............................................................. 94
Figure 6-8: Report of System on Q4 ........................................................................ 94
Figure 6-9: Data Collection Diagram for Q5............................................................. 95
Figure 6-10: Report of System on Q5 ...................................................................... 95
Figure 6-11: Data Collection Diagram for Q6............................................................. 96
Figure 6-12: Report of System on Q6 ...................................................................... 96
Figure 6-13: Data Collection Diagram for Q7............................................................. 97
Figure 6-14: Report of System on Q7 ...................................................................... 97
Figure 6-15: Data Collection Diagram for Q8............................................................. 98
Figure 6-16: Report of System on Q8 ...................................................................... 98
Figure 6-17: Data Collection Diagram for Q9............................................................. 99
Figure 6-18: Report of System on Q9 ...................................................................... 99
Figure 6-19: Data Collection Diagram for Q10............................................................. 100
Figure 6-20: Report of System on Q10 ..................................................................... 100
Figure 6-21: Data Collection Diagram for Q11............................................................. 101
Figure 6-22: Report of System on Q11 ..................................................................... 101
Figure 6-23: Data Collection Diagram for Q12............................................................. 102
Figure 6-24: Report of System on Q12 ..................................................................... 102
Figure 6-25: Data Collection Diagram for Q13............................................................. 103
Figure 6-26: Report of System on Q13 ................................................................. 103
Figure 6-27: Data Collection Diagram for Q14 .................................................. 104
Figure 6-28: Report of System on Q14 ............................................................... 104
Figure 6-29: Data Collection Diagram for Q15 .................................................. 105
Figure 6-30: Report of System on Q15 ............................................................... 105
Figure 6-31: Data Collection Diagram for Q16 .................................................. 106
Figure 6-32: Report of System on Q16 ............................................................... 106
Figure 6-33: Data Collection Diagram for Q17 .................................................. 107
Figure 6-34: Report of System on Q17 ............................................................... 107
Figure 6-35: Data Collection Diagram for Q18 .................................................. 108
Figure 6-36: Report of System on Q18 ............................................................... 108
Figure 6-37: Data Collection Diagram for Q19 .................................................. 109
Figure 6-38: Report of System on Q19 ............................................................... 109
Figure 6-39: Data Collection Diagram for Q20 .................................................. 110
Figure 6-40: Report of System on Q20 ............................................................... 110
Figure 6-41: Data Collection Diagram for Q21 .................................................. 111
Figure 6-42: Report of System on Q21 ............................................................... 111
Figure 6-43: Data Collection Diagram for Q22 .................................................. 112
Figure 6-44: Report of System on Q22 ............................................................... 112
Figure 7-1: Rotation of Image in GUABRR Algorithm .................................... 119
Figure 7-2: Resizing of Image in GUABRR Algorithm ................................. 120
Figure 7-3: Rotation and Resizing of Image in GUABRR Algorithm ........... 120
List of Tables

Table 2-1: Pure Recall Based Techniques Ordered by Date ......................................................... 9
Table 2-2: Cued Recall Based Techniques Ordered by Date ......................................................... 9
Table 2-3: Recognition Based Techniques Ordered by Date ......................................................... 10
Table 2-4: Usability Attributes From ISO Standards ........................................................................ 31
Table 2-5: The Usability Features in Cued Recall-Based Techniques .............................................. 32
Table 2-6: The Usability Features in Pure Recall-Based Techniques .............................................. 32
Table 2-7: The Usability Features in Recognition-Based Techniques .............................................. 33
Table 2-8: The Attacks Resistance in Cued Recall-Based Techniques ........................................... 36
Table 2-9: The Attacks Resistance in Pure Recall-Based Techniques ........................................... 37
Table 2-10: The Attacks Peruse in Recognition-Based Techniques ............................................... 37
Table 2-11: Comparative Table Based on “Graphical Space” ....................................................... 38
Table 2-12: Comparative Table Based on “Password Entropy” ................................................... 39
Table 3-1: Use Cases and Flow of Events of Log-In ..................................................................... 46
Table 3-2: Class Table Analysis .................................................................................................... 52
Table 4-1: The Propose New GUA System Features ..................................................................... 60
Table 6-1: Usability Features Based on ISO Standards (From Chapter two) ................................. 88
Table 6-2: Questionnaire in Usability Test and Analysis................................................................. 89
Table 6-3: Registration and Log-in Date of Users .......................................................................... 90
Table 6-4: Percentage of Each Answer for Calculating the Final Result ...................................... 91
Table 6-5: Data Collection Table for Q1 ......................................................................................... 91
Table 6-6: Data Collection Table for Q2 ......................................................................................... 92
Table 6-7: Data Collection Table for Q3 ......................................................................................... 93
Table 6-8: Data Collection Table for Q4 ......................................................................................... 94
Table 6-9: Data Collection Table for Q5 ......................................................................................... 95
Table 6-10: Data Collection Table for Q6 ....................................................................................... 95
Table 6-11: Data Collection Table for Q7 ....................................................................................... 96
**List of Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ASP</td>
<td>Active Server Pages</td>
</tr>
<tr>
<td>BDAS</td>
<td>Background Draw A Secret</td>
</tr>
<tr>
<td>CAPEC</td>
<td>Common Attack Pattern Enumeration and Classification</td>
</tr>
<tr>
<td>DAS</td>
<td>Draw a Secret</td>
</tr>
<tr>
<td>GP</td>
<td>Graphical Password</td>
</tr>
<tr>
<td>GUA</td>
<td>Graphical User Authentication</td>
</tr>
<tr>
<td>GUABRR</td>
<td>Graphical User Authentication Based on Rotation and Resizing</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Server</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organisation for Standardisation</td>
</tr>
<tr>
<td>LTM</td>
<td>Long-term memory</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PE</td>
<td>Password Entropy</td>
</tr>
<tr>
<td>PS</td>
<td>Password Space</td>
</tr>
<tr>
<td>QDAS</td>
<td>Qualitative Draw A Secret</td>
</tr>
<tr>
<td>TBPA</td>
<td>Text Based Password Authentication</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modeling Language</td>
</tr>
<tr>
<td>UPM</td>
<td>Unified Process Modeling</td>
</tr>
<tr>
<td>USDP</td>
<td>Unified Software Development Process</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

Undoubtedly, there is currently the phenomenon of threats at the threshold of the internet, internal networks and secure environments. Although security researchers have made great strides in fighting these threats by protecting systems, individual users and digital assets, unfortunately the threats continue to cause problems. The principle area of attack is AUTHENTICATION, which is of course the process of determining the accessibility of a user to a particular resource or system.

Today, passive or active users are the key consideration of security mechanisms. The passive user is only interested in understanding the system. The active user, on the other hand, will consider and reflect on ease of use, efficiency, memorability, effectiveness and satisfaction of the system. Generally, authentication methods are classified into three categories:

a. Inherit Based Authentication

The Inherent Based Authentication category which is also known as Biometric Authentication, as the name suggests, is the automated method/s of identity verification or identification based on measurable physiological or behavioral characteristics such as fingerprints, palm prints, hand geometry, face recognition, voice recognition and such other similar methods.

Biometric characteristics are neither duplicable nor transferable. They are constant and immutable. Thus it is near impossible to alter such characteristics or fake them. Furthermore such characteristics cannot be transferred to other users nor be stolen as happens with tokens, keys and cards.

Unlike the security of a user’s password, biometric characteristics, for instance the user’s fingerprint or iris pattern, are no secret. Hence there is no danger of a break in security.
b. Token Based Authentication

The Token Based Method category is again as the name suggests authentication based on a TOKEN such as: a key, a magnetic card, a smart card, a badge and a passport.

Just as when a person loses a key, he would not be able to open the lock, a user who loses his token would not be able to login, as such the token based authentication category is quite vulnerable to fraud, theft or loss of the token itself.

c. Knowledge Based Authentication

The concept of Knowledge Based Authentication is simply the use of conventional passwords, pins or images to gain access into most computer systems and networks. Textual (alphabetical) and graphical user authentications are two methods which are currently used. True textual authentication which uses a username and password has inherent weaknesses and drawbacks which will be discussed in the following section.

1.1 Background

One of the major problems of the textual password is the difficulty of remembering passwords. A survey has shown that most of the users tend to select short passwords or passwords that are easy to remember which unfortunately, can be easily guessed or broken by attackers. Other users select long passwords which are difficult to commit to memory, as well as hard to guess or break. The other drawback with textual passwords is that most users cannot remember a number of passwords for different authentications; they tend to use the same passwords for different accounts. Survey done by Xiaoyum at 2005 has revealed that running a password cracker in a sample network uncovered about 80% of passwords in 30 seconds (Xiaoyuan et al. 2005).

Psychological confirmed that, people can recognize and remember combinations of geometrical shapes, patterns, textures, and colors better than meaningless alphanumeric characters, making the graphical user authentication to be greatly desired as a possible alternative to textual passwords. This type of authentication is formed by combining images, icons or pictures.
1.2 Project Motivation

With the enormous number of users utilising the facilities of the internet today, authentication is fundamental for every secure system.

Traditional text-based passwords have well known weaknesses. Most of the time, people tend to select passwords with foreseeable patterns that correlate with what is easiest to remember which causes the passwords to be guessable for an attacker. On the other hand, memorability is one of the major problems in textual authentication methods. According to these problems of text-based passwords, many new knowledge-based user authentication techniques have emerged that in theory produce higher entropy user authentication wherein Graphical Authentication is one of the most important of them. This project tries to propose a new algorithm which supports both usability and security.

1.3 Research Problem Statement

From the first graphical user authentication which was proposed by Blonder until now, many researchers have worked in order to propose new algorithms, or improve the previous ones with the intention of increasing the security and usability. But unfortunately increasing usability for the users has caused the algorithms to have fewer security features or when the researchers focus on the security they lose the usability features. So, until now the challenge of creating an algorithm which covers both usability and security still remains for the designer (Greg, 1996; Eiji and Nicolas, 2008).

1.4 Objectives of Project

“The primary objective of this research is to design a new Graphical User Authentication namely GUABRR algorithm (Graphical User Authentication Based on Rotation and Resizing), which would be achieved through the following secondary objectives:”
(i) To survey the various algorithms of GUA and compare the usability and security features of all the reviewed algorithms.

(ii) To propose a new algorithm with balanced security and usability features.

(iii) To design and implement the proposed algorithm using .NET platform.

(iv) To test and evaluate the proposed algorithm.

1.5 Project Methodology

The methods which are used in order to achieve the objectives of the project are as follows:

- A complete survey is undertaken which reviews all algorithms in three different categories namely pure recall, cued recall and recognition based. In each category the algorithms are reviewed and the strengths and weaknesses are pointed-out. As a result of these findings, ISO usability standards and common attacks of GUA comparative tables will be created.

- Propose a new algorithm by rotating and resizing the images which a user selects during the registration phase. During the registration phase the user selects several images from a grid of 25 images. In the login stage, the system generates a grid of 25 images which include the user’s password. All the images in the grid are rotated and resized from their original image. Additionally, the placement of all 25 pictures is created randomly. A random three length characters, which include an alphabetic character, number and special character is assigned to each image. The user should identify his/her password from among 25 images and type the related text in the password text box. This will cause the algorithm to be more resistant to Shoulder Surfing attacks.

- The design of the proposed system will use the Object Oriented Analysis (OOA) and will be modeled using the Unified Modeling Language (UML). The implementation will use the selected .NET framework (2.0), with SQL server 2005 for database management.

- In order to test the usability of the system a questionnaire based on ISO usability attributes will be filled in by users on-line. “Password Entropy” and “Password
Space” will be calculated to evaluate the security of system.

1.6 Scope of Project

The new algorithm proposed in this project attempts to have a balance between usability and security in graphical user authentication. Therefore this project not only covers the usability options in GUA but also extends to keeping the algorithm resistant to common attacks of GUA.

The scope of each part in this project is:

(i) Finding the usability features based on ISO 9241, 9126, 13407 and the common attacks on GUA.

(ii) Proposing a new algorithm of GUA while balances the usability and security features.

(iii) Designing and implementing the proposed algorithm using Microsoft .NET platform version 2.0 and Microsoft SQL server 2005 for database management.

(iv) Testing and analyzing the usability features of the proposed system using an on-line questionnaire based on ISO usability attributes.

(v) Evaluating the security feature of the proposed algorithm by calculating the “Password Entropy” and “Password spaces”.

1.7 Research Outcomes

The research contribution algorithm in this project is a new graphical user authentication (GUA) algorithm that is not only resistant to common attacks of GUA such as shoulder surfing or dictionary attack but also has a balance of security and usability features. The proposed algorithm will be developed and implement whereupon the final system will be tested and evaluated on usability features based on ISO standards and security features based on “Password Entropy” and “Password Space”.
The other contribution of this project is to endeavor to study and recognise the strengths and weaknesses of existing graphical algorithms which are categorized as of pure recall, cued recall and recognition based. Last but not least, to make a comparison table for the various graphical user authentication algorithms on usability and attacks.

1.8 Project Overview

This project focuses on graphical user authentication and proposes design and implement a new algorithm using mixed recall and recognition based algorithms with image processing features like resizing and rotating. This project has 7 chapters:

Chapter1: Introduction

This chapter focuses on the introduction to the project that includes the project overview, problems, objectives, methodology and motivation.

Chapter2: Literature Review

This chapter covers the first objective and will be divided into 5 sections as follows: section 2.2 will explain all the algorithms. Followed by section 2.3, which will describe the ISO usability standards (9241, 9126 and 13407) and make a conclusion on the attribute of usability. Section 2.4 starts by reviewing the six common attacks of GUA and then creates a comparison table.

Chapter3: Methodology

The methodologies that are used in each part of this project will be explained as follows: section 3.2 will explain the research methodology which supports the first objective. Then section 3.3 will illustrate the design methodology for this project followed by section 3.4 which elucidates the software technique and approach used in the implementation part. Thereafter section 3.5 will list the requirements of the system in terms of hardware and software parts. In the last section, 3.6 the methods for testing and evaluating the system will be decided upon.
Chapter 4: System Design

This chapter which covers the first part of third objective of this project will be divided to three sections as follows: section 4.2 will explain the conceptual framework of the proposed system. In the next step, section 4.3 will describe the architectural model of the proposed system. In the final step, section 4.4 will elucidate the conceptual design by using a case diagram (4.4.2), sequential diagram (4.4.3), class diagram (4.4.4) and database design (4.4.5).

Chapter 5: Implementation

This chapter aims to fulfill the third objective of this project which is the implementation of the proposed algorithm. It is divided to three sections as follows: Section 5.2 will elucidate the implementation model. The next step, section 5.3, will explain the implementation technology which is divided in three parts: the web server, .NET technology and database language. In the final step, section 5.4 will illustrate the interface design of system.

Chapter 6: Test and Evaluation

This chapter documents the test and analysis of proposed algorithm which is the forth objective of this project. It is divided to three sections as follows: Section 5.2 will elucidate the implementation model. After that, section 5.3 will explain the implementation technology which is divided into three parts namely: web server, .NET technology and database language. Then, section 5.4 will shed light on the interface design of system. Finally, section 2.5 is summary of this chapter.

Chapter 7: Conclusion and Future works

These chapter summaries the project, project contribution and the future works of the project.
Chapter 2: Literature Review

This chapter covers the first objective and will be divided into 5 sections as follows: section 2.2 will explain all the algorithms which are divided into three categories (sections 2.2.1, 2.2.2 and 2.2.3). Followed by section 2.3, which will describe the ISO usability standards (9241, 9126 and 13407) and make a conclusion on the attribute of usability and security. Section 2.4 starts by reviewing the six common attacks of GUA and thereafter creates a comparative table.

2.1 Introduction

The term “Picture Superiority Effect” coined by researchers to describe Graphical-Based Passwords (GBP) reflects the effect of GBP’s as a solution to conventional password techniques. Furthermore, such a term underscores the impact of GBP’s in that the “effect” is on account of the fact that graphics and texts are easier to commit to memory than conventional password techniques.

Initially, the concept of Graphical User Authentication (GUA) described by Blonder (Greg, 1996), one image would appear on the screen whereupon the user would click on a few chosen regions of the image. If the user clicked in the correct regions then the user would be authenticated. Memorability of passwords and the efficiency of input images are two major key human factors. Memorability has two perspectives:

- The process of selecting and the encoding of the password by the user.
- Defining the task that user has to undertake to retrieve the password.

The graphical user authentication (GUA) system requires a user to select a memorable image. Such a selection of memorable images would depend on the nature of the image itself and the specific sequence of click locations. Images with meaningful content will support the user’s memorability.
2.2 Graphical Authentications Methods

Most of articles from 1994 till 2009 describe that Graphical Authentication Techniques are categorised into three groups:

(i) Pure Recall Based Techniques

Users reproduce their passwords, without having the chance to use the reminder marks of system. Although easy and convenient, it appears that users do not quite remember their passwords. Table 2-1 shows some of the algorithms which were created based on this technique.

Table 2-1: Pure Recall Based Techniques Ordered by Date

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Proposed Date</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draw a Secret (DAS)</td>
<td>1999</td>
<td>Jermyn Ian et al.</td>
</tr>
<tr>
<td>Passdoodle</td>
<td>1999</td>
<td>Christopher Varenhorst</td>
</tr>
<tr>
<td>Grid Selection</td>
<td>2004</td>
<td>Juaie Thorpe, P.C. Van Oorschot</td>
</tr>
<tr>
<td>Syukri</td>
<td>2005</td>
<td>Syukri, et al.</td>
</tr>
<tr>
<td>Qualitative DAS (QDAS)</td>
<td>2007</td>
<td>Di Lin, et al.</td>
</tr>
</tbody>
</table>

(ii) Cued Recall Based Techniques

Here, the system provides a framework of reminders, hints and gestures for the users to reproduce their passwords or make a reproduction that would be much more accurate. Table 2-2 lists some of the algorithms which were created based on this technique.

Table 2-2: Cued Recall Based Techniques Ordered by Date

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Proposed Date</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blonder</td>
<td>1996</td>
<td>Greg E. Blonder</td>
</tr>
<tr>
<td>Passlogix v-Go</td>
<td>2002</td>
<td>Passlogic Inc. Co.</td>
</tr>
<tr>
<td>VisKey SFR</td>
<td>2003</td>
<td>SFR Company</td>
</tr>
<tr>
<td>PassPoint</td>
<td>2005</td>
<td>Susan Wiedenbeck, et al.</td>
</tr>
<tr>
<td>Pass-Go</td>
<td>2006</td>
<td>-</td>
</tr>
<tr>
<td>Passmap</td>
<td>2006</td>
<td>Roman V. Vamponski</td>
</tr>
<tr>
<td>Background DAS (BDAS)</td>
<td>2007</td>
<td>Paul Duaphi</td>
</tr>
</tbody>
</table>
(iii) Recognition Based Techniques

Here, users select pictures, icons or symbols from a bank of images. During the authentication process, the users have to recognise their registration choice from a grid of image. Research has shown that “90% of users can remember their password after one or two months” (Saranga and Dugald 2008). Table 2-3 shows some of the algorithms which were created based on this technique.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Proposed Date</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passface</td>
<td>2000</td>
<td>Sacha Brostoff, M. Angela Sasse</td>
</tr>
<tr>
<td>Déjà vu</td>
<td>2000</td>
<td>Rachna Dhamija, Adrian Perrig</td>
</tr>
<tr>
<td>Triangle</td>
<td>2002</td>
<td>Leonardo Sobrado, J-Canille Birget</td>
</tr>
<tr>
<td>Movable Frame</td>
<td>2002</td>
<td>Leonardo Sobrado, J-Canille Birget</td>
</tr>
<tr>
<td>WIW</td>
<td>2003</td>
<td>Shushuang Man, et al.</td>
</tr>
<tr>
<td>Story</td>
<td>2004</td>
<td>Darren Davies, et al.</td>
</tr>
</tbody>
</table>

In the following section the GUA’s algorithms will review and study their strengths and weaknesses.

2.2.1 Pure Recall Based Techniques

2.2.2.1 Passdoodle Algorithm

Passdoodle is a graphical user authentication (GUA) algorithm made up of handwritten designs or text, drawn with a stylus onto a touch sensitive screen. It has been confirmed that doodles are more difficult to crack as there is a theoretically larger number of possible doodle passwords than text passwords (Christopher, 2004). Figure 2-1 shows a sample of the Passdoodle algorithm.

Recognition inhibits the widespread use of the Passdoodle. Length and identifiable features of the doodle provides the boundaries of the system. A definite number of computer differentiable doodles are possible. The doodle here is used as the sole means of identification. A basic floor threshold of likeliness and similarity
for reasons of security, must be set, seeing as the system would refuse to authenticate a user as the user whose recorded doodle is most similar. This prevents guessing to authenticate a random user.

The original pervasive design worked on speed and accuracy as two top priorities. It is counterproductive to have a complicated recognition design requiring a hundred training samples minute of computations to authenticate. A mixture of doodle velocity and distribution mapping to recognise and authenticate a doodle is what the proposed system is about.

A Passdoodle Graphical Authentication algorithm which used the idea of hand written designs or words, drawn with a pen onto a sensitive touchable screen was proposed in 2004 by Goldberg and his college. They confirmed that users were able to remember complete doodle images as they would with textual passwords. (Christopher, 2004)

![Figure 2-1: An Example of a Passdoodle Algorithm](image)

**Weaknesses:** According to (Christopher, 2004), people could recall doodle images as accurately as they would at alphanumeric passwords. However, such people would not be able to recall the order in which they drew a doodle than the resulting image. On the other hand, users were found to be interest by the doodles drawn by other users, and often entered other users’ login details simply to discover a variance of the set of doodles from their own (Karen, 2008).

### 2.2.2.2 Draw a Secret (DAS) Algorithm

This method consisted of an interface that had a rectangular grid of size G * G, which allowed the user to draw a simple picture on a 2D grid as in Figure 2-2. Each cell in this grid is earmarked by discrete rectangular coordinates (x,y). As clearly evidenced in the Figure, the coordinate sequence made by the drawing is:
The stroke should be a sequence of cells which does not contain a pen up event. Hence the password is defined as some strokes, separated by the pen up event. At the time of authentication, the user needs to re-draw the picture by creating the stroke in exactly the same order as in the registration phase. If the drawing hits the exact grids and in the same order, the user is authenticated (Jermyn et al. 1999).

Figure 2-2: Draw a Secret (DAS) Algorithm on a 4*4 Grid

**Weaknesses:** Goldberg in his 2002 survey concluded that the majority of users could not remember their stroke order. Conversely, the user can recall text passwords faster than they would with DAS Passwords. Yet another weakness is that users tend to select extremely weak Graphical Authentications which are susceptible to graphical dictionary attack (Dunphy and Yan, 2007).

2.2.2.3 Grid Selection Algorithm

In 2004, a research was conducted on the complexity of the DAS technique based on password length and stroke count by Thorpe and Orschot. Their study showed that the item which has the greatest effect on the DAS password space is the number of strokes. This means that for a fixed password length, if a few strokes are selected then the password space will significantly decrease. To enhance security, Thorpe and Orschot created a “Grid Selection” technique. As shown in Figure 2-3, the selection grid has a large rectangular region to zoom in on, from the grid which

(2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5, 5)
the user selects their key for their password. This definitely increases the DAS password space (Muhammad Daniel et al. 2008).

![Figure 2-3: A Sample of Grid Selection Algorithm](image)

**Weaknesses**: Whilst this method significantly increases the DAS password space, the deficiencies in DAS have not been resolved (Muhammad Daniel et al. 2008).

### 2.2.2.4 Qualitative DAS Algorithm (QDAS)

The QDAS method was created in 2007 as a boost to the DAS method, by encoding each stroke. The raw encoding consists of its starting cell and the order of qualitative direction change in the stroke vis-a-vie the grid. A directional change is when the pen passes over a cell boundary in a direction in variance to the direction of the pass in the previous cell boundary. Research has shown that the image which has a hot spot is pivotal as a background image (Di et al. 2007). Figure 2-4 shows a sample of QDAS password.

![Figure 2-4: A Sample of Qualitative DAS Algorithm](image)

Albeit this model applies dynamic grid transformation to mask the process of creating the password, this method could be safer than the original DAS in the fight
against shoulder surfing attack and further it has greater entropy than the previous DAS.

**Weaknesses**: According to (Di et al. 2007), the QDAS has less memorability than the original one.

### 2.2.2.5 Syukri et al. Algorithm

In 1998 Syukri et al. proposed a system where authentication is kicked in when the users draw their signatures utilising the mouse. The sample of Syukri can be seen in Figure 2-5 (Ali Mohamed, 2008). This technique has a two step process, registration and verification. During the registration stage, the user will be required to draw his signature with the mouse, whereupon the system will extract the signature area and either enlarge or scale-down the signatures, rotating the same if necessary (Alternatively known as normalising). The information will later be stored in the database. The verification stage initially receives the user input, where upon the normalisation takes place, and then extracts the parameters of the signature. By using a dynamic updateable database and the geometric average means, verification will be performed (Ali Mohamed, 2008).

![Figure 2-5: A Sample of Syukri Algorithm](image)

**Weaknesses**: As not everybody is comfortable with using the mouse as a writing device, the signature is so hard to draw, possibly the use of a pen-like input device would resolve this problem. However such devices are not widely used and the addition of new hardware to the current system can be expensive (Ali Mohamed, 2008). In this study, researchers concluded that such a technique is more pertinent to small devices.
2.2.2 Cued recall-Based Techniques

2.2.2.1 Blonder Algorithm

Greg E. Blonder, in 1966 created a method wherein a pre-determined image is presented to the user on a visual display so that the user should be able point to one or more predetermined positions on the image (tap regions) in a predetermined order as a way of pointing out his or her authorisation to access the resource. Blonder maintained that the method was secure according to the millions of different regions. Figure 2-6 shows a sample of the Blonder password.

![Blonder Algorithm](image)

Figure 2-6: A Sample of Blonder Algorithm

**Weaknesses:** The number of predefined click regions was relatively small in this algorithm as such the password had to be long for it to be secure. Furthermore, the use of the Blonder algorithm necessitates that some special shape similar to a cartoon or artificial image is used in contrast to real pictures (Susan et al. 2005b).

2.2.2.2 PassPoint Algorithm

In 2005, the PassPoint was created in order to cover the image limitations of the Blonder Algorithm. The picture could be any natural picture or painting but at the same time had to be rich enough in order for it to have many possible click points. On the other hand the existence of the image has no role other than helping the user to remember the click point. This algorithm has another flexibility which makes it possible for there to be no need for artificial pictures which have pre selected regions to be clicked like The Blonder algorithm.

During the registration phase the user chooses several points on the picture in a certain sequence. To log in, the user only needs to click close to the chosen click
points, and inside some adjustable tolerable distance, say within 0.25 cm from the actual click point (Susan et al. 2005a). The Passpoint system has enough features for creating a high entropy algorithm. Since any pixel in the image is a candidate for a click point thus there are hundreds of possible memorable points in the challenge image (Ahmet et al. 2007). Figure 2-7 shows a sample of the PassPoint password.

![PassPoint password](image)

Figure 2-7: A Sample of Passpoint Algorithm

**Weaknesses:** The login time, in this method, is longer than in the alphanumeric method. Also the user has more difficulty in learning and memorizing in their password. So, users have to go to several trial session for completing the process (Susan et al. 2005a).

### 2.2.2.3 Background DAS Algorithm (BDAS)

Created in 2007, this method added a background image to the original DAS, such that both the background image and the drawing grid is the key to cued recall (Paul et al. 2007). The user begins by trying to have a secret in mind which is made up of three points from different categories. Firstly the user starts to draw using the point from a background image. Then the next point of user is that the user’s choice of the secret is affected by various characteristics of the image. The last alternative for the user is a mix of the two previous methods. Figure 2-8 shows a sample of BDAS algorithm.
Weaknesses: Research on BDAS showed that memory decaying over a week is one of the major obstacles in this algorithm. Users had no issue in recreating it in the five-minute test. However, a week later they could not produce the secret password as well as they had done the previous week. Further, shoulder-surfing and interference between multiple passwords are concerns for BDAS (Paul et al. 2007).

2.2.2.4 PASSMAP Algorithm

Analysis on passwords has shown that a good password is hard to commit to memory besides this a password which is easy to remember is too short and simple to be secured. A survey in human memory has confirmed that a landmark on a well-known journey is fairly easy.

For example, Figure 2-9 shows a sample of a PassMap password for a passenger who wants to take a trip to Europe as follows: One day a tour in Paris around the Eiffel then a tour in London around Big Ben. After these two tours, the third tour will be in Moscow. The passenger must be able to visit all of them in a map. Referring to the Figure below, it will be easy to memorise the trip in a map (Roman, 2007).
Weaknesses: The PassMap technology is not very susceptible to "shoulder surfing" as can be clearly seen from Figure 2-9, but it is susceptible to Brute Force attacks whilst those mechanisms are great in terms of how memorable they are (Roman, 2007).

2.2.2.5 Passlogix v-Go Algorithm

Passlogix Inc. is a commercial security company located in New York City USA. Their scheme, Passlogix v-Go, utilises a technique known as “Repeating a sequence of actions” meaning creating a password in a chronological sequence. Users select their background images based on the environment, for example in the kitchen, bathroom, bedroom or others (See Figure 2-10). User can click on a series of items in the image as password. For example in the kitchen environment a user can: prepare a meal by selecting a fast food from the refrigerator and put on the hot plate, select some vegetables and wash them, then put them on the launch desk (Muhammad Daniel et al. 2008).

In case another environment such as the cocktail lounge is used, this will allow users to select their favorite vodka, brandy or whiskey and mix it with other cocktails. This type of authentication is easy to remember and fun to use (Muhammad Daniel et al. 2008).
Weaknesses: Inherently there exist disadvantages such as the size of password space being small. After all, the places that one can take vegetables or food from and put into are limited, resulting in the passwords being guessable or predictable (Muhammad Daniel et al. 2008).

2.2.2.6 VisKey SFR Algorithm

VisKey is one of the recall based authentication schemes commercialised by SFR Company in Germany which was created specifically for mobile devices such as PDAs. To form a password, all users need to do is to tap their spots in sequence (Figure 2-11) (Muhammad Daniel et al. 2008).

Weaknesses: Input tolerance is the major drawback of this method. This algorithm permits all input within a certain tolerance area around it, since it is difficult to point to the exact spots on the picture. The size of this area can be pre-defined by users. A certain degree of precaution, related to the input precision, needs to be exercised, as
there is a straightforward correlation between the security and the usability of the password. Practically, the setting of parameters with a four spot VisKey theoretically offers almost 1 billion possibilities to define a password. However, such is not large enough to avoid the off-line attacks by a high-speed computer. A minimum of seven defined spots are needed in order to overcome the brute force attacks (Muhammad Daniel et al. 2008).

2.2.2.7 Pass-Go Algorithm

In 2006, this scheme being created as an improvement of the DAS algorithm, keeping the advantages of the DAS whilst adding some extra security features. Pass-Go is a grid-based scheme which requires a user to select intersections, instead of cells, thus the new system refers to a matrix of intersections, rather than cells as in DAS (Figure 2-12).

![Pass-Go Algorithm](image)

Figure 2-12: Pass-Go Algorithm

Changing the format of typing from cells to intersections grants the user more free choices. The other difference between these two algorithms is that the size of the grid in the enhanced method changes to 9*9.

**Weaknesses:** The intersections in this algorithm do not have boundaries around them, because of this users face error tolerance mechanism. Therefore sensitive areas need to be defined to address this problem.

2.2.3 Recognition-Based Techniques

The fundamental of these techniques is choosing images, icons or symbols from a large collection by the users. During the registration phase, the user has to
recognise and identify his password image among the bank of decoy images. Research shows that around 90% of users can remember their password after one or two months (Saranga and Dugald, 2008).

2.2.3.1 Passface Algorithm

In 2000, this method was developed by the idea to choose a face of humans as a password. Firstly, a trial session starts with the user in order to have an adventure for the real login process. During the registration phase the user chooses whether their image password should be a male or female picture, then chooses four faces from decoy images as the future password.

During the login phase, a grid which contains nine pictures, as in Figure 2-13, is shown to the user. Only one of the user’s passwords among four is shown to user in this grid, and the other eight pictures are decoys which are selected from the bank of pictures. Because the password of user contains four faces so the grid repeats continually for four times and each repetition contains one of the password pictures. If one of the passwords has been shown in one grid, it will not be shown in the next grid. On the other hand the password faces are randomly placed in grids which help to create a more secure environment for the user against shoulder-surfing and packet-sniffing attacks (Sacha and Angela, 2008). The user tries to identify his four passwords among the other pictures twice in a row.

According to research, (Ali Mohamed et al. 2008) this is one of the algorithms which covers most of the usability features like ease of use, and straightforward creation and recognition.

![A Sample of Passface Algorithm](image)

Figure 0.13: A Sample of Passface Algorithm
In 2004, research surprisingly showed that users tend to select their password from faces of their own country and race. In order to come up with this result a category of twelve races was created with different faces collected from Asian males and females, black males and females, white males and females, some Asian male and female models, black male and female models, white male models and white female models. The results showed that most Asian females and white females tend to select fifty percent of the time from their own race; on the other hand sixty percent of the white males choose whites, and ninety percent of time, black males prefer to select blacks as their password (Susan et al. 2005b; Ali Mohamed et al. 2008). But this causes the password to be easier to guess and suggests that the Passface scheme is vulnerable to guessing attack.

A 2006 research worked on the security of Passface algorithm by focusing on the vulnerability of this algorithm according to the usage of a keyboard or mouse. The results showed that if during login the user selects keyboard rather than mouse it would be less vulnerable to shoulder surfing attack because the observer has to check two places at the same time. Therefore keyboard causes Passface to be more resistant to shoulder surfing attack (Furkan et al. 2006).

**Weaknesses:** This algorithm like the others suffers from some weaknesses. Firstly, when the password is selected by the mouse, it is simple for the attacker to observe the password. The other drawback of this algorithm is the long login time and long process through registration phase which causes this algorithm to be slower than textual password authentication (Furkan et al. 2006).

### 2.2.3.2 Déjà vu Algorithm

This algorithm created in 2000, starts by allowing users to select a specific number of pictures from a large image portfolio. The pictures are created by random art which is one of hash visualisation algorithms. One initial seed is given for starters and then one random mathematical formula is generated defining the color value for each pixel in the image. The output will be one random abstract image. The benefit of this method is that as the image depends completely on its initial seed, so there is no need for saving the picture pixel by pixel and only the seeds need to be stored in the trust server. During authentication phase, the user should pass through a challenging set where his portfolio mixes with some decoy images; the user will be
authenticated if he is able to identify his password among the entire portfolio as illustrated in Figure 2-14 (Dhamija and Perrig, 2000). This method causes the algorithm to be less vulnerable to description attack.

Conversely, the number of pictures in the portfolio and the number of random images could very well alter the security of system. Although research has shown that 90% of participants of this method were more successful in login compared to a 70% rate of those who use textual passwords, there are several drawbacks with this method.

**Weaknesses:** Research on Déjà vu algorithms has shown that it has three soft spots. Firstly, creating a textual password requires 25 seconds but with this method a user needs about 60 seconds to create the password. Secondly, the process of selecting pictures from the database can be tedious and time consuming for the user. Finally, the password seeds for each user can just be saved in the plain text format (Rachna et al. 2000).

**2.2.3.3 Triangle Algorithm**

A group in 2002 proposed the triangle algorithm based on several schemes to resist the Shoulder surfing attack. The first scheme named, triangle as shown in Figure 2-15, randomly places a set of N objects (a few hundred or a few thousand) on the screen. Additionally, there is a subset of K pass objects previously chosen and memorised by the user. The system will select the placement of N objects randomly in the log-in phase.
The system initially chooses a patch randomly covering half the screen, and then randomly again places the K password objects in that patch. In the log-in phase, the user must be able to find the location of three pass-objects and then click inside the invisible triangle that is possible to create those three objects. But, for each login this process will be repeated using a different group of n objects. So, it is possible to say that there is a very low probability of randomly clicking in the correct area (Leonardo et al. 2002).

![Figure 2-15: A Sample of Triangle Algorithm](image)

**Weaknesses:** The log-in phase must use a minimum of 1000 images in order to resist shoulder surfing. As a result the log-in will be very crowded and the password will be indistinguishable (Xiaoyuan et al. 2005).

**2.2.3.4 Movable Frame Algorithm**

The moveable frame algorithm proposed in 2002 had a similar idea to that of triangle method. However in its case the user had to select three objects from K objects in the login phase. As it is shown in Figure 2-16, only 3 pass objects are displayed at any given time and only one of them is placed in a movable frame.

The user must move the frame until the three objects line up one after the other. These operations minimise the random movements involved in finding the password (Leonardo et al. 2002).
Weaknesses: Just like in the triangle algorithm, there are many objects involved in this algorithm which can lead to the user being unsatisfied and in most cases will confuse users (Leonardo et al. 2002).

2.2.3.5 Picture Password Algorithm

This algorithm was designed especially for handheld devices like Personal Digital Assistant (PDA) in 2003. According to Figure 2-17, during enrollment, the user selecting a theme identifying the thumbnail photos to be applied and then registers a sequence of thumbnail images that are used as a future password. If the device is powered on, then the user must input the true sequence of images but after successful log-in the user can change the password.

In this algorithm the password space will be small because the number of photos is limited to 30. In order to solve this problem, the designer added a second step to the algorithm. This means the user can select two thumbnails together to compose the new alphabet element by using a shift key to select uppercase or special characters.
The memorability will be more complex when the second part which solves the password space’s problem is added to the algorithm (Wayne et al. 2003).

2.2.3.6 Story Algorithm

The Story Algorithm that was proposed in 2004, categorised the available pictures into nine categories namely animals, cars, women, foods, children, men, objects, natures and sports (Figure 2-18). This algorithm was proposed by Carnegie Mellon University to be used for different purposes. In this method the user selects the password from the mixed pictures in the nine categories in order to make a story (Darren et al. 2004).
Weaknesses: Research showed that the story scheme was difficult to commit to memory in comparison to pass face authentication.

2.2.3.7 Where Is Waldo (WIW) Algorithm

In order to offer resistance against shoulder surfing, in 2003 another algorithm that uses a unique code for each picture was proposed. The user selects some picture as a password. This picture must be found in the log-in phase before the user can type the related unique code in a text box. The argument is that it is very hard to dismantle this kind of password even if the whole authentication process is recorded on video as there is no mouse click to give away the pass-object information. The log-in screen of this graphical password algorithm is shown in Figure 2-19 (Shushuang et al. 2003).

![Figure 2-19: A Sample of WIW Algorithm](image)

Weaknesses: One of the main vulnerabilities of this algorithm is memorising the alphanumeric code for each password by the user.

2.2.4 Proposed Algorithm (GUABRR)

For designing the GUABRR algorithm the usability and security features considered with reference to previous algorithms and prior research.

According to table 2.4, the usability of all graphical password algorithm divides to categories like easy to use, easy to create, easy to memorise, easy to execute, easy to understand, good view and pleasant picture. The GUABRR algorithm covers these features with the following details:
**Easy to Use:** The previous algorithm shows that the users find the algorithm easy to use, when they have the option to works with password. At the same time, using mouse make the algorithm vulnerable to shouldered surfing attack (Tari et al, 2006). To covering both items, the users are free to selects their password by mouse during registration phase, but the mouse usage deleted for login phase for making the algorithm resistant to shoulder surfing attack.

**Easy to Create:** According to previous algorithm, users find the algorithm easy to create when the registration includes simple steps. The existence of several rounds in selecting and creating password (like story password), make the process tedious and slow for the user (Wiedenbeck and Camille Birget, 2005), So in designing the proposed algorithm, the registration needs only one steps to finishes successfully.

**Easy to Memorise:** The research on memorability shows that when a random password is assigned to user, the users had difficulty in remembering their password in compare with the situation where the users can select their own passwords (Yan et al., 2004). Therefore for making the GUABRR password easy to remember, the users can freely select their password. This method covers the lacks of some algorithm like passface which the user do not have any choice to select his password.

**Easy To Execute:** According to previous algorithm, users find the algorithm easy to execute when the login and registration include simple steps. The existence of several rounds in selecting and creating password, make the process tedious and slow for the user (Wiedenbeck and Camille Birget, 2005), So in designing the proposed algorithm the registration and login process designed to be complete in one simple step.

**Easy to Understand:** When learnability and understandability features add to any algorithm, the system will be simpler to comprehend and use, thus decreasing training and support costs, also it enhances user satisfaction and decrease uneasiness and pressure. On the other hand the learability will enhance the productivity of users and the operational effectiveness of organizations (Alain et al., 2003). The GUABBR algorithm registration and login is designed simply in order to bring no difficulty for the user to understand the steps. This makes the algorithm more powerful than cued and pure based algorithms which needs several training session for the users.
**Pleasant:** The users need pictures with acceptable quality in order to be satisfied. To make the quality of passwords pictures acceptable, the pictures designed in 300 dpi formatted, with high quality to make the pleasant interface for the users.

The security features of GUABRR algorithm considered simultaneously to usability, by referring to Table 2.10 which shows that most of recognition based algorithm is vulnerable to shoulder surfing attack except “WIW algorithm” which omitted password selection by mouse during login phase. The research shows that, switching the password selection from mouse to keyboard decreases the vulnerability to the shoulder surfing attack (Tari et al, 2006). With reference to these finding the GUABRR algorithm, designed in the way that the user’s needs to selects their password by using keyboard. Also during login phase each image is assigned as a unique and variant code. So the user needs to enter strings of unique codes corresponding to the images in order to be authenticated (Shushuang et al. 2003).

The second items which considered for the security of GUABRR algorithm is the human ability to recognize a degraded version of a previously seen image. The distorted images can make the algorithm more resilient to social engineering or observation attacks (Eiji and Nicolas, 2008). There are several methods for images processing and degrading image like rotation, resizing, and blurring which increase the “Password Entropy” and “Password Space” of the graphical password algorithm. As the bluing bring a lot of difficulty for the users to recognize the picture after blurring so in designing the proposed algorithm it tries to use other processing features which is rotation and resizing (Beilei et al. 2008).

With reference to all these usability and security features the GUABRR algorithm designs with a mixture of recognition- bases and cued recall-based algorithm based on rotation and resizing. In the registration phase of GUABRR algorithm, 25 images are shown to users. Users can select any number of pictures as their passwords. The main reason for such open boundary is to have a feedback from users to determine how many pictures they prefer to select as their password. For login phase, all 25 images are shown to users again but rotation and resizing will change the interface of each picture. The pictures can rotate in 12 different angles (30, 45, 60, 90, 120, 135, 150, 180, 210, 240, 270 and 315) randomly which cause the algorithm to be more secure since the attacker sees the login phase differently.
each time. Also the picture in the login phase can resize 40 percent. All these two methods are tested separately and users opinions are gathered to see how usable each of these methods were.

2.3 Usability in Graphical User Authentication (GUA)

Up until now, most of the algorithms in graphical authentication have been surveyed and the weaknesses and attacks have been explained. Now, we need to (with regard to usability and security features and all attacks in graphical authentication methods), elaborate the standards and locate the major attributes for each of them. Thereafter we can then make a comparison table of all graphical authentication algorithms as gathered in the previous sections of this chapter.

2.3.1 ISO Usability Methods

The International Organisation for Standardisation defines different models for usability. Each of algorithms discussed above lack a number of the features in these models. This section tries to scrutinise three models in ISO and make a comprehensive table of usability attributes based on these ISO standards.

2.3.1.1 ISO 9241

ISO 9241 is a branch of the ISO standard. It defines the requirement for efficiency in the working environment, for example the office. The detail of this ISO is explained in Appendix A (Alain et al. 2003).

2.3.1.2 ISO 9126

ISO 9126 addresses software quality from a product point of view. It is probably the most extensive software quality model, even if it is not exhaustive. The detail of this ISO is explained in Appendix B (Alain et al. 2003).

2.3.1.3 ISO 13407

This ISO provides the usability attributes of human activities through the computer-based interactions. The detail of this ISO is explained in Appendix C (Alain et al. 2003; ISO 13407, 1999).
2.3.2 Usability Final Attributes

Finally, after studying the three ISO standards (9241, 9126, and 13407) based on usability and other research on usability features in GUA algorithms (Roman, 2008; Ali Mohamed, 2008), this project found additional usability attributes for each feature based on graphical user authentication which can be seen in the table below (Table 2-4).

<table>
<thead>
<tr>
<th>Usability Features</th>
<th>Attributes</th>
<th>Attributes Especially for Graphical User Authentication</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectiveness</td>
<td>Reliability &amp; Accuracy</td>
<td>Reliability &amp; Accuracy</td>
<td>R&amp;A</td>
</tr>
<tr>
<td>Efficiency</td>
<td>The Utilisation In Real World</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>Satisfaction</td>
<td>Easy To Use</td>
<td>Use The Mouse Easily</td>
<td>Mouse Usage</td>
</tr>
<tr>
<td></td>
<td>Easy To Create</td>
<td>Select Simple Way to Create The Password</td>
<td>Simple Creation</td>
</tr>
<tr>
<td></td>
<td>Easy To Memorise (Memorability)</td>
<td>Meaningful User Assign Image Freedom Of Choice</td>
<td>Meaningful Assignable Image</td>
</tr>
<tr>
<td></td>
<td>Easy To Execute</td>
<td>Select Simple Steps of Registration And Login</td>
<td>Simple Steps</td>
</tr>
<tr>
<td></td>
<td>Good View</td>
<td>Select Good Interface</td>
<td>Nice Interface</td>
</tr>
<tr>
<td></td>
<td>Easy To Understand</td>
<td>Simple Training Session</td>
<td>Simple Training</td>
</tr>
<tr>
<td></td>
<td>Pleasant</td>
<td>Pleasant Picture</td>
<td>Pleasant Picture</td>
</tr>
</tbody>
</table>

With reference to this literature review the major reasons why most of graphical authentication researchers cannot concentrate on systems with balanced security and usability features are:

- The researchers tend to focus more on the ability of attackers to break or crack the password solutions for authentication with modest prominence given to the usability features necessities.

- The researchers tend to focus on the usability more than the implementation of security which needs to be given the necessary attention.
Herein are the results of the usability features on recall and recognition based algorithms (Table 2-5). All algorithms cover the effectiveness and efficiencies features but in satisfaction some of them did not cover the all relative features.

Table 2-5: The Usability Features in Cued Recall-Based Techniques

<table>
<thead>
<tr>
<th>Cued Recall-Based Algorithm</th>
<th>Satisfaction</th>
<th>Efficiency</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passdoodle</td>
<td>Mouse usage, Meaningful, Simple Steps, Simple Training</td>
<td>Applicable</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>DAS</td>
<td>Mouse usage, Simple Steps, Simple Training</td>
<td>Applicable</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>Grid Selection</td>
<td>Mouse usage, Simple Steps, Simple Training</td>
<td>-</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>QDAS</td>
<td>Mouse usage, Simple Steps, Simple Training</td>
<td>Applicable</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>Syukri Algorithm</td>
<td>Mouse usage, Meaningful, Memorability, Simple Steps, Nice Interface, Simple Training</td>
<td>Applicable</td>
<td>Reliability &amp; Accuracy</td>
</tr>
</tbody>
</table>

In a same process, Table 2-6 shows a comparative of Pure Recall-Based techniques based on usability features. Regarding to table 2-6 some of the algorithms did not cover the effectiveness and efficiency features completely.

Table 2-6: The Usability Features in Pure Recall-Based Techniques

<table>
<thead>
<tr>
<th>Pure Recall-Based Algorithm</th>
<th>Satisfaction</th>
<th>Efficiency</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blonder</td>
<td>Mouse Usage, Simple Creation, Clickable Points, Memorability, Simple Steps, Simple Training</td>
<td>Applicable</td>
<td>-</td>
</tr>
<tr>
<td>PassPoint</td>
<td>Mouse Usage, Simple Creation, Clickable Points, Memorability, Simple Steps, Nice Interface, Simple Training, Pleasant Picture</td>
<td>Applicable</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>BDAS</td>
<td>Mouse Usage, Meaningful, Memorability,</td>
<td>-</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>PASSMAP</td>
<td>Mouse Usage, Simple Creation, Meaningful, Clickable Points,</td>
<td>Applicable</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 2-7 shows a comparative of Recognition-Based techniques based on usability features. As same as table 2-6 in this table some of the algorithms did not cover the effectiveness or efficiency features together.

<table>
<thead>
<tr>
<th>Recognition-Based Algorithm</th>
<th>Satisfaction</th>
<th>Efficiency</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>PassFace</td>
<td>Mouse usage, Simple Creation, Assignable Image, Memorability, Simple Steps, Nice Interface, Simple Training, Pleasant Picture</td>
<td>Applicable</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>Dejavu</td>
<td>Mouse usage, Simple Creation, Assignable Image, Simple Steps, Simple Training,</td>
<td>-</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>Triangle</td>
<td>Mouse usage, Simple Creation, Memorability, Simple Steps, Simple Training,</td>
<td>-</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>Movable Frame</td>
<td>Mouse usage, Simple Creation, Memorability, Simple Steps,</td>
<td>-</td>
<td>Reliability &amp; Accuracy</td>
</tr>
<tr>
<td>Password</td>
<td>Mouse usage, Simple Creation, Assignable Image, Memorability, Simple Steps, Nice Interface, Simple Training, Pleasant Picture</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|----------|---------------------------------------------------------------------------------------------------------------------------------
| Story Password | Mouse Usage, Simple Creation, Meaningful, Assignable Image, Memorability, Simple Steps, Nice Interface, Pleasant Picture |
| WIW | Mouse usage, Simple Creation, Assignable Image, Memorability, Simple Steps, Simple Training, |
| Proposed Algorithm (GUABRR) | Mouse Usage, Simple Creation, Clickable Points, Meaningful, Simple Steps, Nice Interface, Simple Training, Pleasant Picture |

### 2.4 Security and Attacks in Graphical User Authentication (GUA)

In security test of GUA algorithm, at first in this project the common attacks faced by the GUA (CAPEC Standard 2009) are presented and then two major attributes of security measurement will explained.

### 2.5.1 Attacks

#### 2.5.1.1 Brute Force Attack

This is an attack which tries every possible combination of password status in order to break the password. Text-based passwords have a password space of $94^N$, where $N$ is the length of the password, ninety four is the number of printable characters excluding “space”. Computationally, this attack is always successful.
because it checks all possible passwords in the password length; therefore users should try to select strong passwords to be more resistant to brute force attack.

It is more difficult for this attack to be successful in graphical passwords than textual passwords because the attack programs must create all mouse motions to imitate the user password, especially for recall based graphical passwords. The main item which helps in the resistance to brute force attacks is having a large password space. Some graphical password techniques have proved to have a larger password space in comparison with textual passwords.

2.5.1.2 Dictionary Attack

This is an attack in which the attacker starts by using the words in the dictionary to test whether the user choose them as a password or not. The brute force technique is used to implement the attack. Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical password. This sort of attack is more successful in the textual password. Although the dictionary attack is proved to be in some of the recall base graphical algorithm (Rachna et al. 2000 and Susan et al. 2005a), an automated dictionary attack will be much more complex than a text based dictionary attack.

2.5.1.3 Spyware Attack

This is a special kind of attack where tools are initially installed on a user’s computer and then start to record any sensitive data. The movement of the mouse or any key being pressed will be recorded by this sort of malware. All the data that has been recorded without notifying the user is then reported back out of the computer. Except for a few instances, using only key logging or key listening spyware cannot be used to break graphical passwords as it is not proved whether the movement of the mouse spyware can be an effective tool for breaking graphical passwords. Even if the mouse tracking is saved, it is not sufficient for breaking and finding the graphical password. Some other information such as window position and size, as well as timing information are needed to complete this kind of attack.
2.5.1.4 Shoulder Surfing Attack

It is obvious from the name of this attack, that sometimes it is possible for an attacker to find out a person’s password by looking over the person’s shoulder. Usually this kind of attack can be seen in a crowded place where most people are not concerned about someone standing behind them when they are entering a pin code. The more modern method of this attack can be seen when there is a camera in the ceiling or wall near the ATM machine, which records the pin numbers of users. So it is really recommend that users try to shield keypad to protect their pin number from attackers.

2.5.1.5 Social Engineering Attack (Description Attack)

This is an attack in which an attacker, through interaction with one of the employees about the organization, manages to impersonate an authorised employee. This may lead the ‘impersonator’ to gain an identity which is the first step of his hacking process. Sometimes the attacker cannot gather enough information about the organisation or a valid user. In such a situation the attacker will most likely try to contact another employee. The cycle is repeated until the attacker manages to get an authorized identity of one of the personnel. In the following section we put together the comparison table for these attacks based on the surveys. Some parts of the table are filled in based on the previous survey and papers (Greg 1996; Paul et al. 2007 and Qiang et al. 2006) even as much as we try to complete them, the parts that are still not filled will be considered as future work.

Table 2-8, 2-9 and 2-10 shows a comparative three GUA algorithms based on common attacks which gathered with previous survey (Suo et al., 2005; Wiedenbecka et al., 2005; Roman, 2007).

Table 2-8: The Attack Resistance in Cued Recall-Based Techniques

<table>
<thead>
<tr>
<th>Cued Recall-Based Algorithm</th>
<th>Resistance</th>
<th>Non-resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passdoodle</td>
<td>Dictionary</td>
<td>Brute Force</td>
</tr>
<tr>
<td>DAS</td>
<td>Dictionary, Guessing, Shoulder Surfing</td>
<td>Brute Force, Spyware, Social Engineering</td>
</tr>
<tr>
<td>Grid Selection</td>
<td>Dictionary</td>
<td>Brute Force</td>
</tr>
<tr>
<td>QDAS</td>
<td>Dictionary</td>
<td>Brute Force</td>
</tr>
<tr>
<td>Syukri Algorithm</td>
<td>Dictionary, Guessing, Shoulder Surfing</td>
<td>Brute Force, Spyware, Social Engineering</td>
</tr>
</tbody>
</table>
The Table 2.8 and 2.9 shows that, quit a vast survey needs to find out the vulnerabilities of each graphical password algorithm to five common attacks, which recommends to be done in future. All cued based algorithms are vulnerable to brute force attack, but at the same time pure based algorithm are resistant to this attack. Most pure recall based algorithms are vulnerable to dictionary and spyware attack. Most of algorithms in both category are resistant to shoulder surfing attack.

Table 2-9 shows a comparative of Pure Recall-Based techniques based on common attacks.

<table>
<thead>
<tr>
<th>Pure Recall-Based Algorithm</th>
<th>Resistance</th>
<th>Non-Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blonder</td>
<td>Brute Force, Guessing, Shoulder Surfing</td>
<td>Dictionary, Spyware, Social Engineering</td>
</tr>
<tr>
<td>PassPoint</td>
<td>Brute Force, Guessing, Shoulder Surfing</td>
<td>Dictionary, Spyware, Social Engineering</td>
</tr>
<tr>
<td>Background DAS</td>
<td>Guessing</td>
<td>Brute Force</td>
</tr>
<tr>
<td>PASSMAP</td>
<td>Brute Force, Shoulder Surfing</td>
<td>Dictionary, Spyware, Social Engineering</td>
</tr>
<tr>
<td>Passlogix v-Go</td>
<td>Brute Force, Guessing,</td>
<td>Dictionary, Spyware, Social Engineering</td>
</tr>
<tr>
<td>VisKey SFR</td>
<td>Brute Force, Guessing, Shoulder Surfing</td>
<td>Dictionary, Spyware, Social Engineering</td>
</tr>
<tr>
<td>Pass-Go</td>
<td>Brute Force</td>
<td>Social Engineering</td>
</tr>
</tbody>
</table>

Table 2-10 shows a comparative of Recognition-Based techniques based on common attacks.

<table>
<thead>
<tr>
<th>Recognition-Based Algorithm</th>
<th>Resistance</th>
<th>Non-Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PassFace</td>
<td>Brute Force, Guessing, Shoulder Surfing,</td>
<td>Dictionary, Social Engineering,</td>
</tr>
<tr>
<td>Dejavu</td>
<td>Brute Force, Guessing, Shoulder Surfing,</td>
<td>Dictionary, Social Engineering,</td>
</tr>
<tr>
<td>Triangle</td>
<td>Brute Force, Guessing,</td>
<td>Dictionary, Shoulder Surfing, Social Engineering</td>
</tr>
<tr>
<td>Movable Frame</td>
<td>Brute Force, Guessing,</td>
<td>Dictionary, Shoulder Surfing, Social Engineering</td>
</tr>
<tr>
<td>Picture password</td>
<td>Brute Force, Guessing,</td>
<td>Shoulder Surfing</td>
</tr>
<tr>
<td>Story password</td>
<td>Brute Force, Guessing,</td>
<td>Shoulder Surfing</td>
</tr>
<tr>
<td>WIW</td>
<td>Brute Force, Guessing,</td>
<td>Dictionary, Shoulder Surfing, Social Engineering</td>
</tr>
<tr>
<td>Proposed Algorithm (GUABRR)</td>
<td>Brute Force, Guessing, Shoulder Surfing, Social Engineering,</td>
<td>Dictionary</td>
</tr>
</tbody>
</table>

37
According to the table most algorithm in this category are resistant to brute force and guessing attack, but at the same time vulnerable to shoulder surfing attack. According to table, the GUABBR algorithm is not resistant to dictionary attack but the algorithm is resistant to other common attacks of GUA.

2.5.2 Security

This section shows the two methods of security testing and evaluation on GUA algorithms. The initial part defines the “Graphical Password Space” as one of the methods and then makes a comparison in a table between some previous algorithms and the newly proposed algorithm. Then the second part defines the “Graphical Password Entropy” and makes comparison between some previous algorithms and newly proposed algorithm.

2.5.2.1 Graphical Password Space

Users can pick any element for their password in GUA; the raw size of password space is an upper bound on the information content of the distribution that users choose in practice. It is not possible to define a formula for password space but for all algorithms it is possible to calculate the password space or the number of passwords that can be generated by the algorithm. Now, this section will define and calculate the password space for previous algorithms and GUABRR, then make a comparative analysis. Table 2-11 shows the comparison between previous algorithms and the newly proposed algorithm based on password space.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets)</td>
<td>$52^6$</td>
</tr>
<tr>
<td>Textual (6 characters: capital and small alphabets and numbers)</td>
<td>$62^6$</td>
</tr>
<tr>
<td>Image selection similar to Passface (4 runs, 9 pictures)</td>
<td>$9^4$</td>
</tr>
<tr>
<td>Click based algorithm similar to Passpoint (4 loci and assuming 30 salient points)</td>
<td>$30^4$</td>
</tr>
<tr>
<td>GUABRR (select 3 images from 25 images and 3 characters for each image in Log-in part)</td>
<td>$(25^3) * (66^3)$</td>
</tr>
</tbody>
</table>
2.5.2.2 Graphical Password Entropy

Password entropy is usually used to measure the security of a generated password, which conceptually means how hard to blindly guess out the password. For simplicity, assume all passwords are evenly distributed, the password entropy of a graphic password can then be calculated as follows.

$$\text{Entropy} = N \log_2 (|L||O||C|)$$

In other words, Graphical password entropy tries to measure the probability that the attacker obtains the correct password based on random guessing. In the above formula, $N$ is the length or number of runs, $L$ is locus alphabet as the set of all loci, $O$ is an object alphabet and $C$ is color of the alphabet (Zhi et al. 2005). Table 2-12 shows the comparison between previous algorithms and the new proposed algorithm.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Formula</th>
<th>Entropy (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets)</td>
<td>$6 \times \log_2(52)$</td>
<td>34.32</td>
</tr>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets and numbers)</td>
<td>$6 \times \log_2(62)$</td>
<td>35.70</td>
</tr>
<tr>
<td>Image selection similar to Passface (4 runs, 9 pictures)</td>
<td>$4 \times \log_2(9)$</td>
<td>12.74</td>
</tr>
<tr>
<td>Click based algorithm similar to Passpoint (4 loci and assuming 30 salient points)</td>
<td>$4 \times \log_2(30)$</td>
<td>19.69</td>
</tr>
<tr>
<td>GUABRR (select 5 images from 25 images and 12 degrees rotation and 2 resizing options)</td>
<td>$5 \times \log_2(25 \times 12 \times 2)$</td>
<td>46.37</td>
</tr>
</tbody>
</table>

2.5 Conclusion

We have reviewed 12 algorithms from Recall-Based method (including 7 algorithms from Pure Recall-Based and 5 algorithms from Cued Recall-Based) and 8 algorithms from Recognition-Based algorithms. We have further identified several weaknesses in all these algorithms which could cause attacks. It can be concluded that the common weaknesses on these algorithms were:
- It has been seen that some users are interested to see which pictures have been selected or what is the shape which has been drawn as a password by other users.
- For the pure recall-based and cued recall-based some users have difficulty in remembering the sequence of the drawing after registration.
- Not all the users are familiar with using the mouse as a drawing input device for the graphical password.
- Some algorithms have common drawbacks with memorability and usability.
- Most users prefer to select weak passwords which help the attacker to guess the password successfully. On the other hand, graphical dictionary attack is more successful by having this special weakness.

Further, in the second part of this chapter, the major attributes in usability based on ISO standards (9241, 13407 and 9126) have been collected and the attacks based on standard attacks in GUA have defined. By reviewing various algorithm, two security features namely, password entropy and password space defined. Then a comparison tables made on usability and vulnerability of algorithms to GUA attacks.
Chapter 3: Methodology

The methodologies that are used in each part of this project will be explained as follows: section 3.2 will explain the research methodology for first objective which is the survey of various algorithms of GUA. Then section 3.3 will illustrate the design methodology for this project followed by section 3.4 which elucidates the software technique and approach used in the implementation part. Thereafter section 3.5 will list the requirements of the system in terms of hardware and software parts. In the last section, 3.6 the methods for testing and evaluating the system will be decided upon.

3.1 Introduction

In this chapter, the main strategy is to develop the usability and security elements of the new algorithm. It is quite important to outline the overall plan in order to ensure that the progress of the project will not stray from its main objective and the outcome can be achieved in a desirable way. This chapter is divided into three sections.

3.2 Methodology of Research

In the methodology of research, a searching and gathering of the needed information for the project, verification of the requirements and method are important steps to go through for the project to get the expected results. There are three steps usually in the research strategy namely:

- Researching
- Data Gathering
- Finding

There are two methods for achieving these three objectives of research which will be explained in the following section:
3.2.1 Document Retrieval Method

A document retrieval system consists of a database of documents, a classification algorithm to build a full text index, and a user interface to access the database. A document retrieval system has two principal tasks:

- To find the relevant documents to user queries.
- To evaluate the matching results and sort them according to relevance, using some algorithms.

For example, Internet search engines are classical applications of document retrieval.

3.2.2 Comparative Study Method

The design of comparative research is simple. The comparative method does not need any earlier model or theory to start with. Therefore, it is well suited for conducting studies where scientists try to migrate from the initial level of case study to a more advanced level like causality or evaluation.

In this research, the comparison study is used to make a comparative table of the usability and security elements. The goal of this comparative study is to identify all usability elements based on ISO Standards and common attacks that can be implemented in the new scheme. Figure 3-1 shows the diagram of this part of the methodology.
3.3 Methodology of Design and Implement

In this section, the methodology of designing a new algorithm that has a balance in usability and security will be described. A design of the prototype will be applied and the final prototype will be created. Testing the prototype is required to check the usability and security features. The usability testing will be done by questionnaires, and the security testing will be done by calculating the “password entropy” and “password space”. Some revisions need to make the new scheme more reliable, and then the final prototype will be implemented by the project researcher. Figure 3-2 shows the steps of this section of the methodology.
3.4 Software Development Approach

The software development approach that will be utilised is the unified software development process or in short, the unified process. The Unified Process is component-based, implying that the software being built is made up of software components interconnected via well-defined interfaces. Besides that, the Unified Process uses Unified Modeling Language (UML) in preparation of blueprints for the software. Before we start the approach structure, two major concepts of UML need to be explained:

- Use-Case Model
  Use case model has been one of the choices of the Unified Process which includes the following items:
  - Use cases, which represent a piece of functionality in the system
  - Actors, which represent the users and any external system that the current system interacts with.
The Use-case model, states requirements that are value added to the user. Use-cases have been adopted universally for the capturing of the requirements of software systems in general but more specifically for component-based systems.

- **Use-Case Driven**
  
  The use-case driven, imports a development process through a series of workflows that are initiated from the use cases, in other words, they drive the whole development process. Figure 3-3 illustrates the models of the unified process where all the models have dependencies with the use-case model. This means use cases are traceable through all the models.

![Use Case Driven Model](image)

**Figure 3-3: Use Case Driven Model**

### 3.4.1 Design and Implementing Activities (DIA)

DIA proscribes the five main activities which are requirements, analyse, design, implement and testing which will be discussed in detail in the following sections.

#### 3.4.1.1 Requirements

The purpose of the requirements activity is to ensure that the development is toward the right system as specified by user. This activity will be explained below:

**3.4.1.1.1 Requirements Captures**

The needed requirements of the project are as follows:

- The context in which the system is set upon is required.
• GUABRR is a user authentication system that can be utilised as a subsystem to other secure systems such as the banking system, accounting system or online payment system.

• Identifying requirements based on use cases.

Table 3-1 shows a log-in use case with the definitions, actor involved, post and pre-condition, and the flow of events.

Table 3-1: Use Cases and Flow of Events of Log-In

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
</table>
| Log-in   | A USER needs to login before performing any transaction.  
Actors: USER  
Pre-condition: A registered user.  
**Main flow of events:**  
1. The USER clicks the LOG-IN button from Left menu of home page.  
2. The Log-In page will be show.  
3. The USER enters his/her username.  
4. The USER use Enter or Tab key.  
5. The system checks the username from database in table “UserInfo”.  
6. Username exists; the system refreshes the page and shows the password selection part in Log-In page.  
7. The system request user to find the three images from his/her registered password and write the code (appear under each images) of them in password textbox.  
8. The USER enters his/her password.  
9. The USER clicks the “Submit” button.  
10. The system validates the password code information against the “UserInfo” table from the database and the generated codes under password images.  
11. USER is an authorised user; the system redirect to the Questionnaire page for collecting the feedback of users. |
3.4.1.1.2 Finding Actors and Use Cases

All types of system users and external systems need to be identified in the requirement activity. Actors identified from the previous steps are used to identify candidate use cases for each actor or may also come from customers and users. These candidates are then revised to produce a set of use cases that have an appropriate scope.

Each use case briefly describes the actions and a step-by-step description of what the system needs to do when interacting with its own actors. These descriptions are summarized into a few sentences. Diagrams and description to explain the use-case model as a whole are prepared with emphasis on how the use cases relates to each other and to the actors. Figure 3-4 shows the use case model of the GUABRR system.

![Use Case Model of GUABRR](image)

3.4.1.1.3 Prototype User Interfaces

The purpose of this activity is to produce a set of user interface sketches and prototypes for the most important actors. On the other hand, this step identifies the user interface elements that are needed for users to interact with a use case. The use cases will be examined individually to identify the proper user interface elements. During this step, sketches of user interface elements will be combined to form the physical user interface. Then, executable prototypes are built for the important user interface elements.

These sketches and prototypes will be validated through user interface review and will work as a specification of the user interface when the real user interface is constructed. GUABRR user interface design is shown in Figure 3-5.
3.4.1.4 Structure the Use Cases Model

This activity extracts general and shared use-case description of functionality that can be used by more specific use-case descriptions. The state machine and activity diagrams can be used for illustrating the structure use-case model. Figure 3-6 shows one of the state machine diagrams and Figure 3-7 shows one of the activity diagrams.
Figure 3-7: Activity Diagram for “Registration” Part
3.4.1.2 Analysis

The analysis activity as the name suggests, analyses the requirements such as:

- To acquire an in-depth and precise understanding of the requirements,
- To acquire a description of the requirements that is easy to maintain,
- To assist us in the structuring of the system in its entirety.

The result of this analysis will contribute to a stable architecture and make an in-depth whole picture from the requirements. Figure 3-8 shows the four main steps of the analysis that is explained in the next four sections.

![Diagram of System Analysis Steps]

Figure 3-8: Four Main Steps of System Analysis

3.4.1.2.1 Analysis of Architecture

Architectural analysis outlines the architectural models and their analysis. The objective of this step is achieving the indexing of class or use-case analysis by identifying the common requirements.

3.4.1.2.2 Analysis of Use Case

This activity identifies classes whose objects are needed to:

- Perform the use case’s flow of events,
- Distribute the behaviour of the use case to interacting analysis objects,
- The capturing of special requirements on the realisation of the use case.

The original name of this analysis is use case refinement because in this analysis each use case refinement acts as a contribution of classes’ analysis. For
example in the analysis of a class, the control, entity and class boundary must be defined and also the attributes, responsibility and relationships have to be clarified.

The communication diagram describes the interaction between objects that contain the actors, objects, and links with the reason for the links. Figure 3-9 shows the communication diagram for the proposed system.

1: User sends Registration Request
2: System will open the registration page
3: System sends the request of “Filling the Form”
4: User fills up the form
5: System checks the detail of form
6: Result of form checking will be process?
7:1: form is not completed and shows the related message to user
7:2: form was completed and request for record add to Database
8: Record added in Database
9: Send the finish message to User

Figure 3-9: The Communication Diagram for “Registration” Process
3.4.1.2.3 Analysis of classes

Analysing a class identifies and maintains the responsibilities of an analysis object, the attributes and relationships of the analysis class, and captures special requirements on the realisation of the analysis class.

Indeed, responsibilities and attributes of a class are assembled by examining the wide range of roles that it plays in different use case realisations and its behaviour. There are three relations between classes which define the structure of classes namely: Associations, Aggregations and Generalisations. Table 3-2 shows the analysis and attributes of “UserInfo” and “Image_Origin” class as sample and Figure 3-10 shows the class diagram for GUABRR.

![Class Table Analysis](image)

Table 3-2: Class Table Analysis

<table>
<thead>
<tr>
<th>Analysis Class</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cls_UserInfo</td>
<td>User Id</td>
</tr>
<tr>
<td></td>
<td>User name</td>
</tr>
<tr>
<td></td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>First Name</td>
</tr>
<tr>
<td></td>
<td>Last Name</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
</tr>
<tr>
<td></td>
<td>Birth Date</td>
</tr>
<tr>
<td></td>
<td>Country</td>
</tr>
<tr>
<td></td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td>E-mail</td>
</tr>
<tr>
<td>Cls_Image_Original</td>
<td>Image Id</td>
</tr>
<tr>
<td></td>
<td>Image Address</td>
</tr>
<tr>
<td>Cls_Image_Rotation</td>
<td>Image Id</td>
</tr>
<tr>
<td></td>
<td>Rotation Degree</td>
</tr>
<tr>
<td></td>
<td>Image Address</td>
</tr>
</tbody>
</table>
3.4.1.3 Design

The design workflow sets out the parameters of:
1. Understanding issues in-depth based on non-functional requirements.
2. Creating an input to and output from the activities implementation.
3. Being able to break down implementation into component elements.
4. Being able to visualise the design.
5. Creating a seamless abstraction of the system’s implementation.

In the following sections, three different design which are architectural design, use case design and class design will be discuss.

3.4.1.3.1 Design of Architecture

The architectural design is designing the development model and system architecture that results in elements that are incorporated into the design model. In other words, architectural design partitions the functional requirements of a system
into a manageable set of interacting elements. Actually, before any coding and implementation the attributes of qualification such as usability and security can be appraised and approved in this stage.

### 3.4.1.3.2 Use Case Design

This activity identifies the design classes needed. For instance:

- To perform the use case’s flow of events,
- To distribute the behavior of the use case to interacting design objects,
- To define requirements on the operations of design classes and their interfaces,
- To capture implementation requirements for the use case.

There are many diagrams for use case design which show the objects, actors, classes and interaction among them. The sequence diagram, containing the actor instances and design objects that try to describe the interactions among objects. In other words, in sequence diagram all requirements for use case realisation will be illustrated. In the proposed system there are two main sequence diagrams namely “Registration” and “Log-in” that are illustrated in Figure 3-11 and 3-12 respectively.

![Sequence Diagram of Registration Process](image-url)

**Figure 3-11: “Registration” Sequence Diagram**
The class design focuses on the non-functional requirements. Figure 3-13 shows the class design of the GUABRR system. The main steps to be carried out in this section are as follows:

1. Identifying the operations and describing the programming language syntax.
2. Identifying the required attributes and describing the programming language syntax.
3. Identifying the associations and aggregations among design classes.
4. Identifying the generalisations (Actually defined by programming language).
5. Specifying the realisation of operations.
6. Defining the states of objects especially by state diagram.

![Class Diagram of GUABRR](image)

**3.4.1.4 Implementation**

This section highlights the main purpose of implementation and the detailed implementation will be discussed in Chapter 6. There are many purposes of the implementation design such as:

1. Planning the requirements of system integration.
2. Implementing the classes which were designed during the design step.
3. Running the test operation on units and then running it on an integrated system.
4. Deployment of the model to explain the system distribution structure.

Figure 3-14 shows the GUABRR deployment model.
3.4.1.5 Test

After the implementation stage all the design will be developed and coded thereafter the coding must be test one by one. The first type of test is the coding test that shows that the code is clear from error. This is then followed by the second type of test which is the user test which user and developer will discuss the bordering and critical data of the system then the functions of the system will be modified, deleted or new functions will be added.

Thereafter, these small parts of system must be joined in order to start the system test. In this particular test the system will test for its complexity. If any errors occur, the system must be returned back to the previous stage for fixing. Then the result will go through the system test again. This procedure must be repeated and followed until all of errors are covered and handled. In the Chapter 7 the testing procedures will be discussed in more detail.

3.5 Hardware and Software Requirements

In order to create a suitable environment for the implementation of the project there are several requirement that will needed. Listed below are the requirements.

The Software requirements:
1. Windows XP
2. .NET Framework
3. Microsoft Visual Studio.NET
4. ASP.NET
5. Microsoft SQL Server 2005
6. Microsoft Internet Information Services (IIS)
7. Microsoft Office
8. Microsoft Project

The Hardware requirements:
1. PC with high performance processor 3.5 GHZ.
2. DDR Memory minimum 3 GB.
3. HDD for large data storage especially images (240 GB).

3.6 Methodology of Test and Evaluation

The two approaches for evaluating research are the qualitative and quantitative methods. They check whether the research result is compatible with the requirements or the variation of the result from the proposed system.

3.6.1 Quantitative Approach

Quantitative method is an approach based on measuring and dealing with numbers. For example the number of answers to a question is one of the common forms of quantitative approach. In this approach the result will be a number or a set of numbers which will be illustrated by tables, diagrams or other statistical forms.

3.6.2 Qualitative Approach

Qualitative research tries to understand the behaviour of the research and indeed have faith in the various aspects of behavior. In other words, the quantitative approach will produce numbers which will be used to derive meaning and analysis by the qualitative approach. With regard to these two approaches this project selected both method for testing and evaluating the research result:

- Questionnaire

This project is using a questionnaire for collecting the feedback of users in usability part of the design. When the system is implemented and uploaded on a web site, users will be able to register and login to the system. The ones
who login to the system successfully can complete the questionnaire form. Finally the collected data will be analysed and the resulting graph will be generated.

- **Technical Analyses**
  
  To evaluate the security of this project two technical analysis techniques based on mathematical computation will be used namely: Password Entropy and Password Space.

### 3.7 Conclusion

This chapter has provided the methodology of research which is based on the comparison study method. Then the methodology of design and implementation based on UML is discussed. The next step, explained all relative activities such as, analysing use case, analysing classes, design and implementation. Finally, the qualitative and quantitative approaches explained for testing and evaluation of the system.
Chapter 4: System Design

4.1 Introduction

This chapter, which covers the first part of second and third objectives of this project, will be divided into three sections as follows: section 4.2 will explain the conceptual framework of the proposed system. In the next step, section 4.3 will describe the architectural model of the proposed system. In the final step, section 4.4 will elucidate the conceptual design by using a case diagram (4.4.2), sequential diagram (4.4.3), class diagram (4.4.4) and database design (4.4.5).

4.2 Proposed Algorithm Conceptual Framework

Chapter 2 provides a mapping table based on usability and security features based on ISO standards for usability and attacks standard for security which helps to design features for the new prototype of the GUA. The usability and security final features that will be implemented in the proposed new GUA system prototype are shown in Table 4-1 (Refer to the section 2.2.4).

Table 4-1: The Propose New GUA System Features

<table>
<thead>
<tr>
<th>Usability / Security Features</th>
<th>Attributes</th>
<th>Attributes Especially for Graphical User Authentication</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usability (Effectiveness)</td>
<td>Reliability &amp; Accuracy</td>
<td>Reliability &amp; Accuracy</td>
<td>R&amp;A</td>
</tr>
<tr>
<td>Usability (Efficiency)</td>
<td>The utilisation in real world</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>Usability (Satisfaction)</td>
<td>Easy to use</td>
<td>Use the mouse easily</td>
<td>Mouse usage</td>
</tr>
<tr>
<td></td>
<td>Easy to create</td>
<td>Select simple way to create the password</td>
<td>Create Simply</td>
</tr>
<tr>
<td></td>
<td>Easy to memorise (memorability)</td>
<td>Meaningful</td>
<td>meaningful</td>
</tr>
<tr>
<td></td>
<td>Easy to execute</td>
<td>Select simple steps of registration and login</td>
<td>Simple Steps</td>
</tr>
<tr>
<td>Good view</td>
<td>Select good interface</td>
<td>Nice interface</td>
<td></td>
</tr>
<tr>
<td>Easy to understand</td>
<td>Simple training session</td>
<td>Training simply</td>
<td></td>
</tr>
<tr>
<td>Pleasant</td>
<td>Pleasant picture</td>
<td>Pleasant picture</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Resistant on Attacks</td>
<td>Password Spaces, Password Entropy</td>
<td>-</td>
</tr>
</tbody>
</table>
In Table 4-1, there are three main usability categories which are efficiency, effectiveness and satisfaction. In the next step some of the subcategories of these three classifications will be explain:

- **Ease of use feature**: Defines how the user can use the system easily without any complication, for instance the usage of a mouse or keyboard affect how simply the system constructed, easily followed and accepted by the users.
- **Ease to create feature**: Define how the user can easily create the graphical password, for instance the ease in choosing the pictures, saving the pictures and the ease create.
- **Ease to memorise feature**: Define how the user can easily remember the pictures used as the password.
- **Good view**: Define how the interface of the system satisfies the user.
- **Ease to understand feature**: Defines how the user can use the system easily and without complications by giving some hints to the user like opening message windows during execution.
- **Pleasant**: Defines how the selection of pleasant pictures cultivates eagerness in the users so that they continue working with GUA.
- **Security features covered by “Password Entropy” and “Password Space”**. Password space is the raw size of password which calculated by formula. The password entropy is used to measure how hard to blindly guess out the password.

### 4.3 Proposed System Architecture Module

In the prototype system architecture module we have two actors and two prototypes:

- User (Actor)
- System Administrator (Actor)
- System Interface (Application Prototype)
- System Database (Database Prototype)

Figure 4.1 below shows the structure of the architecture with the main operation in each section. The password space, is the raw size of
4.4 Graphical User Authentication Based on Rotation and Resizing (GUABRR) System Conceptual Design

With regard to chapter three, this project uses the UML technique and unified processing for the design and implementation management. So, this chapter will explain the flow process of the prototype and the relation of each actor to the prototype. In this prototype we have three actors namely administrator, new user and existing user. This section will make a framework picture from the operations of proposed system, then we will show the detail of the system based on sequence diagrams using the UML technique.

4.4.1 Framework of Proposed System

Refer to the Figure 4.2 (framework diagram), the operational framework of the design process will be divided into two stages namely Log-in and registration that will explain in-depth below.

1. The proposed system starts with the user choosing “Log-in” or “Registration” page.
2. If user select the “Registration” page he should:
   2.1 Enter the “User Name”
   2.2 Select some images for his as password (minimum two images)
   2.3 Enter complete information like “Name”, “Family”, “Country”, Address”, “Email”, … (if necessary fields not complete then an error message will be appear)
   2.4 System save the password and user information in database.
   2.5 “Congratulation” page will be appear and Registration phase finish.
3. Else user select the “Log-in” page:
   3.1 User enter the “User Name”
   3.2 If user name is not valid, a message appears that must be register first, if the username is valid the images matrix for finding password will be created.
   3.3 User tries to find his/her password images that selected in registration phase from the new images matrix that system generated. (images will be changed by rotation and resizing in system)
   3.4 User writes the three characters which is under each images of his/her password, for example if number of password images is three then the number of characters will be nine.
   If password was not true then user can tries again as shown in Figure 4.2 (framework diagram). The operational framework of the design process will be divided into two stages namely Log-in and registration. The in-depth explanation is given below.
The main idea of the project is that in the log-in phase, password images will appear differently from what is shown to the user during the registration phase. These images have a special process to create this deferential which is rotation and resizing of images. As the size of database is one of the major weaknesses in GUA algorithms, new proposed systems only save the original images in the database. The processing like random rotation and resizing of images and random text creating of each image are generated by the proposed system during run time. So, the processed images does not save in the database which cause the total size of the database to be small but the processing on the system will be high.
4.4.2 Rotation and Resizing in the Proposed System

In the log-in page two different processes run on all 25 images in the grid which are rotation and resizing. These two processes cause the images show differently from registration phase. In the rotation, the image can rotate in twelve different angles randomly which are 30, 45, 60, 90, 120, 135, 150, 180, 210, 240, 270 and 315 (Figure 4-3).

![Rotation Process in GUABRR Algorithm](image)

**Figure 4-3: Rotation Process in GUABRR Algorithm**

In the resizing as shown in Figure 4-4, the system change the size of image 40 percent from the original size which user can see through registration phase. All pictures have 50 pixels through registration, but in the login phase the images size change to 70 pixels.

![Resizing Process in GUABRR Algorithm](image)

**Figure 4-4: Resizing Process in GUABRR Algorithm**
For using the rotation and resizing simultaneously, the system combine these two methods which cause 24 different statuses for each image (Figure 4-5).

\[12 \text{ possible rotation status} \times 2 \text{ possible size (50 pixel or 70 pixel)} = 24\]

![Figure 4-5: Rotation and Resizing Process in GUABRR Algorithm](image)

### 4.4.3 Use Case Diagram

A use case defines and specifies the behavior of a proposed system and it will be used to capture intended behaviour (functional requirements) of the proposed system that is being developed. Therefore this section explains the details of the use case using one diagram in layer one and the other two diagrams in layer two. Figure 4-6 shows the use case diagram of the GUABRR system.

![Figure 4-6: Use Case Diagram in Layer 1](image)

### 4.4.4 Sequential Diagrams

A sequence diagram is an interaction diagram that emphasises the time ordering of the messages among system parts. Now after designing the whole framework in use case diagram layer one, this section will design the sequence diagrams in layer two for the “Registration” and “Log-in” phases which show the
collaboration of design objects. Figures 4-7 and 4-8 show the GUABRR sequence diagrams.

4.4.4.1 “Log-in” Phase Sequence Diagram

Figure 4-7: “Log-in” Phase Sequence Diagram
4.4.2 "Registration" Phase Sequence Diagram

4.4.5 Class Diagram

The main idea of this part is to specify the class diagram of the GUABRR system which is extracted from the previous subsection. This diagram provides a clear picture of the design classes by describing each use case realisation as collaboration of design objects using two sequence diagrams. Figure 4-9 shows the class diagram of GUABRR system.
Based on the class diagram standard in UML, there are three kinds of objects. The objects are Boundary Object, Control Object and Entity Object. The Boundary object can be visualised as the user interface which is divided into three in the proposed system:

- Login page
- Register page
- Home page

Also, there are three entity objects in the system that can be seen as tables, represented in a database these are:

- “UserInfo” that hold the information of user specially username and password
- “Image-Original” that hold the information of images specially ID and address of image on Hard disk.
• “Image-Rotation” that hold the information about three main rotation information of images.

4.4.6 Database Design

The database design converts the main model and structure of the system after the final analysis of the data structure that will be required in the implementation phase. In this project, Microsoft SQL 2005 Server Express Edition is selected to develop the database system because it is compatible with Microsoft .NET framework. For performing the operation such as adding, updating and deleting the data from the database the application will be connected to the database based on the internal techniques of .net framework.

4.4.6.1 Table Name and Functions

The GUABRR database consists of three tables. The name for each table and a short description of each table’s function which are described below:

1. “UserInfo”: Keeps personal record of the user, inclusive of username, name, Password, Gender and so on.

2. “Images_Orginal”: Stores Id and Address of Images for GUABRR system.

3. “Images_Rotation”: as in implementation system use .net framework and this framework can just handle rotation at 90,180, and 270 degrees, so this table keeps the -30 and +3- degree rotation of Images address and images ID which cover twelve rotations of an image as: 0, 30, 45 ,60 ,75 ,90 ,120 ,150 ,180 ,210 ,240 ,270. The proposed system handles two sizes 0, +20% by itself in order for it to resize.

Figure 4-10 shows the three tables of the GUABRR system.
Unlike most of previous systems, this system does not use a password table for saving the users’ password. In the GUABRR system the password will be generated by a function from the concatenation of images ID that will be explained in the next section in the table “UserInfo”. The result of this design is a simple database with the complex programming and implementation but the user can not see any complexity and all of it will be handled by the system automatically.

### 4.4.6.2 Design of Tables

GUA systems use databases for saving images and need huge size and complex management for the database. Thus data storage is considered to be the most important part of a GUA system. In the GUABRR system, unlike the previous GUA systems the table of images is small because it just saves one Id for each Image and address of the image file in the hard disk and for each image the ID for the three rotated versions on -30,+30 and 45 degree will be saved in another table (“Images_Rotation”). Figures 4-11, 4-12 and 4-13 show the Database’s tables and their fields in the GUABRR system.
Also, unlike most of the GUA systems, in the GUABRR system the password of a user is not saved in a table. The GUABRR system uses a simple method for generating a string of images’ ID from the users images password, in a way that, for each image that a user selects as password, the system saves the image ID with a ‘-‘ as a separator in the password field of “UsersInfo” table. For example for a user with three images as password the system has “12-3-24” or for a user with four images as password the system has “22-9-34-17”. The function that will be handling this part will be explained in the implementation phase.
4.4.7 Data Flow Diagram (DFD)

A Data Flow Diagram is a technique used to graphically illustrate the flow of data through a system and the process performed by the system. DFD gives an overview of four objects in each process. The four objects are:

- Inputs
- Outputs
- Processes
- Data Flow

A DFD shows data flowing by using four symbols:

- Processes
- Data flows
- Data stores
- Entity

In the first level of the DFD Figure 4-11 shows the DFD diagram Layer one for the proposed system then Figure 4-12 and 4-13 shows the Registration DFD and the Log-in DFD as Layer two diagrams. Each part will be explained completely after the Figures.

- User will need to register in the system by supplying some user details such as Name, Family, Address, and Email.
- The system will register the user.
- If the user is a registered user then the user can login to the system.
- A User can login by providing his/her username and password.
• If the username and password is approved by system, the system will allow the user to access the appropriate services, which should include completing the questionnaire and completing the feedback information to the system test and analysis chapter.

![DFD of “Registration” Phase as Layer Two DFD](image)

Users can register by supplying their user information. The system will create a record in the “Users_Info” table in the database. The system will then return the user to the log-in page.

![DFD of “Log-in” Phase as Layer Two DFD](image)

Users can login by supplying their username and password. The system will check the authentication of the supplied username and password as compared to information in the “Users_Info” table in the database. If the username and password provided is correct then permission to access the services is granted.
4.4.8 Entity Relationship Diagram

Figure 4-17 shows an entity relationship diagram for user Information. There are eight fields for user namely First name, Last Name, Gender, Birth Date, Postal Address, Username, and Password. In implementation part this entity relation diagram will design by a user information table that has eight fields.

![Entity Relationship Diagram](image)

Figure 4-17: GUABRR System Entity Relationship Diagram

4.4.9 GUABRR Structure Overview

The GUABRR system has two tier architecture, a client layer and a server layer. Client layer provides pages and interface for servicing the user like registration and log-in pages via a web browser such as Internet Explorer. The Client layer forwards all requests to the server layer and awaits acknowledgement from server.

The server layer provides the necessary services for client side such as authentication service and user information retrieval. The Server layer is handled based on the Microsoft Internet Information Server (IIS) and .net framework. Requests and acknowledgements are handled by the server which transacts with a database manager.

4.4.10 GUABRR Interface Design

The GUABRR system has a two tier architecture, a client layer and a server layer. Client layer provides pages and interface for servicing the user like registration and log-in pages via a web browser such as Internet Explorer. The Client layer forwards all requests to the server layer and awaits acknowledgement from server.
The server layer provides the necessary services for client side such as authentication service and user information retrieval. The Server layer is handled based on the Microsoft Internet Information Server (IIS) and .net framework. Requests and acknowledgements are handled by the server which transacts with a database manager. Figure 4.18 shows the empty password image grid in GUABRR algorithm.

Figure 4-18: Empty Password Image Grid of GUABRR Algorithm
4.5 Conclusion

This chapter has presented the design model of the GUABRR project which is divided into three main categories: conceptual framework, architecture module and conceptual design. In the conceptual framework, the security and usability features of new algorithm listed and described. The architectural module, showed the main operation in the actor and prototype of the system. The conceptual design of this chapter explained and illustrated the system framework, Database design, DFD diagram, class diagram and entity diagram of proposed system. Finally the log-in and registration interface of the proposed system explained.
Chapter 5: Implementation

This chapter aims to fulfill the second part of third objective of this project which is the implementation of the proposed algorithm which divided to three sections as follows: Section 5.2 will elucidate the implementation model. The next step, section 5.3, will explain the implementation technology which is divided in three parts: the web server, .NET technology and database language. In the final step, section 5.4 will illuminate the interface design of system.

5.1 Introduction

This chapter presents the steps of project implementation. In the software life cycle, the focus on implementation is divided into three points:

- During the construction iterations,
- During elaboration phase to create executable architectural baseline,
- During the transition phase to handle late defects.

The rest of the sections of this chapter will cover the GUABRR implementation based on the software life cycle.

5.2 Implementation Model

The main purpose of the implementation model is illustrating the architecture of the system by recognising, defining and explaining the consequential components (executable components) and mapping them. Figure 5-1 illustrates the design, deployment and architecture model by highlighting operators, the administrator and the architecture of system.
As shown in the above diagram, the GUABRR has a collection of nodes with dependencies and associations. Also, the system has an administrator who can connect to the system through the internet. The three conceptual components of this system are web browser (client side), GUABRR server (Server side) and database.

Client side users use an internet browser for accessing the system. They can see the interface and using the registration and log-in part of the system. All of the web user requests will be sent to the server side and the acknowledgement will be sent back by the server. This type of implementation is named “Independent implement” because the user can use the system without requiring any special software or equipment.

5.3 Implementation Technology

5.3.1 Web Server

When a user in a client/server system based on hypertext transfer protocol (HTTP) sends a request, the request must be answered by a web server. In other words every computer on the Internet that hosts a web site must have a web server program for handling the clients’ requests. There are many web servers based on the different operating systems (OS). As this project is running on Microsoft windows OS then the web server will be Microsoft’s Internet Information Server (IIS) which will be demonstrated in the next subsection.
Microsoft Internet Information Server 6.0 (IIS)

Nowadays most of the web companies use the Microsoft windows operating system which leads this company to quickly establish its Internet Information Server (IIS) as one of the premier Web servers on the Internet. IIS is included in most of windows server packages which enabled the transformation of the windows platform into a feasible solution for delivering Web-based applications. Unlike many web servers based on other operating systems the IIS is very easy to install and maintain.

5.3.2 Dot NET Technology

.NET Framework

The .NET platform is divided to some subsystem such as .net frameworks. Indeed, .NET platform comprises libraries of classes such as ASP.NET, VB.NET and more.

ASP.NET History

After ASP, Microsoft delivered ASP.net as an enterprise-generation programming language. This application is accessible on a global basis leading to efficient information management. The advantage ASP.NET offers is more than just the next version of ASP.

Shifting from Windows-Based to Internet-Based platform was one of Microsoft’s constant focuses since 1995. To start with, Microsoft introduced ASP in November 1996, but ASP script was an interpreted script consisting of unstructured code which was difficult for users to debug and maintain. These days most of those developing software are moving toward internet based programming, therefore programming of web applications will:

- Complicate development
- Make it difficult to understand the many different technologies
- Growing in size
- More complex
- Increase the number of source code dramatically
So, the .NET Framework was introduced with a very flexible foundation which makes developing internet applications very easy. Unlike ASP, ASP.NET it uses the Common Language Runtime (CLR) provided by the .NET framework that manages execution of the programming codes. CLR allows interaction among different language objects to make development simpler.

Advantages of ASP.NET

- Dramatically reduces the amount of code in large applications.
- Simpler and easier to maintain the system using Client/Server programming model.
- Easy to write and design web-based systems by mixing the source code and HTML.
- Has lots of power and flexibility by executing the code in server side.
- Fast answer to client side request by saving the compilation result at first request.
- The HTML produced will be sent back to the browser but the source code will not be sent back.
- Easy deployment by built-in the configuration information.
- As the web server monitors the pages continuously, when a memory leak, infinite loops or other illegal activities happen then web server will kill them and restart the page.

5.3.3 Database Language

SQL is a programming language that is used in manipulation and retrieval of data from relational databases. SQL enables a programmer or database administrator to do the following:

- Modification of a database structure,
- Changing of system security settings,
- Adding of user permissions on databases or tables,
- Querying of database for information,
- Updating contents of a database.
Microsoft SQL 2005 Server Express Edition

SQL Server 2005 Express Edition, is a free and easy-to-use database product that is based on SQL Server 2005 technology. It is designed to provide a database platform that offers ease of use and enables fast deployments for its target scenarios. SQL Server Express uses the same reliable and high-performance database engine as the other versions of SQL Server 2005. It also uses the same data access APIs such as ADO.NET, SQL Native Client, and T-SQL. In fact, it is differentiated from the rest of the SQL Server 2005 editions only by the following (Microsoft Corporation 2008):

- Lack of enterprise features support
- Limited to one CPU
- One GB memory limit for the buffer pool
- Maximum 4 GB size for databases

5.4 Interface Design

Interface design will help users to interact and communicate with the system; it also can be used as a presence of retrieving and sending information between the users and the computer. GUABRR has two interface pages for registration and login.

5.4.1 Registration Interface (new user)

Figure 5-2 shows the registration interface of the GUABRR system. Included is the username, password images matrix and user information such as name, address, Email and etc. As shown in Figure 5-2, user can select between two to five images for his/her password. This open boundary is used for finding the best number of images in GUA system by the user feedback in the questionnaire.
Figure 5-2: GUABRR Registration Page

5.4.2 Log-In interface (Existing user)

Figures 5-3a and 5-3b shows the Log-In interface of the GUABRR Algorithm. The first Figure shows the empty grid when user has not enter his username. Whenever he enter his username and press “Tab”, the grid will fill with user password, mix with decoy images.

Figure 5-3b also shows that for each image the system generates three characters randomly. The user must enter the character below his password in the password textbox. The main reason for selecting these text boxes was to create an environment to be resistant for the shoulder surfing attacks and keep the system simple in the way that user do not need to memories his password.
Figure 5-3a: GUABRR Log-In page Before Enter Username

Figure 5-3b: GUABRR Log-In Page after Enter Username

There are three Log-in pages in this system to show the rotation and resizing techniques separately (Figure 5-4a, 5-4b and 5-4c).
Figure 5-4a: GUABRR Registration and Log-In Page by Using Rotation Technique

Figure 5-4b: GUABRR Registration and Log-In Page by Using Resizing Technique
5.5 Conclusion

This chapter has focused on the implementation phase of the GUABRR project. In the first step the implementation model was explained followed by the description of the technology used in the implementation (Microsoft .Net based on MS SQL 2005). Finally the interface design section tried to show the final interface of the system especially by the snapshot from the on-line system. The Appendix E shows the source code of GUABRR implementation in .NET platform.
Chapter 6: Test and Evaluate

The purpose of this chapter is to describe the final objective of this project which is the testing and evaluation of proposed algorithm. This chapter is divided into two sections. The first section will explain the usability test and analysis by designing a questionnaire, data collection in an on-line page from users and analysis of the result of the users’ answers. The second section will elucidate the “Password Entropy” and “Password Spaces” as two major attributes of security analysis in GUA algorithms. The formula of these two features will use for measuring the password entropy and password space of GUABRR algorithm and the other algorithm. In the last step, a comparative analysis created between the propose algorithm and the previous methods.

6.1 Introduction

This chapter will run two groups of tests and evaluations on the proposed algorithm, one is usability testing on the system and the other one is security analysis on the algorithm. The first test is a usability test using the questionnaire method together with results of the usability features which were found in chapter 2. The second test is the major evaluation of security by calculating the “Password Entropy” and thirdly calculating the “Password Space”. Then the result of these three tests will be analyzed and compared with some of the previous algorithms.

6.2 Usability Test and Analysis

With regard to literature review findings on the usability feature, this section will use the result of that survey. This is shown in table 6-1.
Table 6-1: Usability Features Based on ISO Standards (From Chapter Two)

<table>
<thead>
<tr>
<th>Usability Features</th>
<th>Attributes</th>
<th>Attributes Especially For Graphical User Authentication</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectiveness</td>
<td>Reliability And Accuracy</td>
<td>Reliability &amp; Accuracy</td>
<td>R&amp;A</td>
</tr>
<tr>
<td>Efficiency</td>
<td>The Utilisation in Real World</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>Satisfaction</td>
<td>Easy to Use</td>
<td>Use The Mouse Easily</td>
<td>Mouse Usage</td>
</tr>
<tr>
<td></td>
<td>Easy to Create</td>
<td>Select Simple Way to Create The Password</td>
<td>Create Simply</td>
</tr>
<tr>
<td></td>
<td>Easy to Memorise (Memorability)</td>
<td>Meaningful</td>
<td>Meaningful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Assign Image</td>
<td>Assignable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Freedom of Choice</td>
<td>Image</td>
</tr>
<tr>
<td></td>
<td>Easy to Execute</td>
<td>Select Simple Steps of Registration And Login</td>
<td>Simple Steps</td>
</tr>
<tr>
<td></td>
<td>Good View</td>
<td>Select Good Interface</td>
<td>Nice Interface</td>
</tr>
<tr>
<td></td>
<td>Easy to Understand</td>
<td>Simple Training Session</td>
<td>Training Simply</td>
</tr>
<tr>
<td></td>
<td>Pleasant</td>
<td>Pleasant Picture</td>
<td>Pleasant Picture</td>
</tr>
</tbody>
</table>

6.2.1 Questionnaire Structure

Since a website was developed for system, the questionnaire will also be designed and uploaded as a part of the system. This will enable the user to fill in the questionnaire online after successful log-in in three phases as Rotation, Resizing and both. In the first phase the user will see the log-in page that is generated by the Rotation process. In the second phase the user will see the log-in page that is generated by the Resizing process and finally in the last phase the user will see the log-in page that is generated by both the rotation and Resizing processes on the images (Figures 5-4a, 5-4b, 5-4c). When the user successfully passes these three phases then he/she will see the on-line questionnaire page. Table 6-2 shows the list of questions in the questionnaire based on Table 6-1. The snapshot of the questionnaire page shows in appendix D.
<table>
<thead>
<tr>
<th>Row</th>
<th>Phase</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All</td>
<td>Can you create easily your graphical password through registration part?</td>
</tr>
<tr>
<td>2</td>
<td>All</td>
<td>Does Login through new graphical password authentication easy?</td>
</tr>
<tr>
<td>3</td>
<td>All</td>
<td>Does Login through new graphical password authentication quick?</td>
</tr>
<tr>
<td>4</td>
<td>All</td>
<td>According to you was the system interface pleasant enough?</td>
</tr>
<tr>
<td>5</td>
<td>All</td>
<td>How do you think the mouse and keyboarded usage are well enough?</td>
</tr>
<tr>
<td>6</td>
<td>All</td>
<td>According to you was the password applicable enough?</td>
</tr>
<tr>
<td>7</td>
<td>All</td>
<td>According to you how many percent the training part helps you?</td>
</tr>
<tr>
<td>8</td>
<td>All</td>
<td>How many images you want to select as your graphical password?</td>
</tr>
<tr>
<td>9</td>
<td>All</td>
<td>Do you like to use this algorithm as log-in part of your on-line systems?</td>
</tr>
<tr>
<td>10</td>
<td>All</td>
<td>Do you prefer graphical password to textual password?</td>
</tr>
<tr>
<td>11</td>
<td>Rotation</td>
<td>According to you does your graphical password easy enough to remember?</td>
</tr>
<tr>
<td>12</td>
<td>Rotation</td>
<td>According to you was the password reliable enough?</td>
</tr>
<tr>
<td>13</td>
<td>Rotation</td>
<td>Was the system easy to understand?</td>
</tr>
<tr>
<td>14</td>
<td>Rotation</td>
<td>In your opinion how many percent this algorithm is secure?</td>
</tr>
<tr>
<td>15</td>
<td>Resizing</td>
<td>According to you does your graphical password easy enough to remember?</td>
</tr>
<tr>
<td>16</td>
<td>Resizing</td>
<td>According to you was the password reliable enough?</td>
</tr>
<tr>
<td>17</td>
<td>Resizing</td>
<td>Was the system easy to understand?</td>
</tr>
<tr>
<td>18</td>
<td>Resizing</td>
<td>According to you how many percent this algorithm is secure?</td>
</tr>
<tr>
<td>19</td>
<td>Rotation &amp;</td>
<td>According to you does your graphical password easy enough to remember?</td>
</tr>
<tr>
<td></td>
<td>Resizing</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Rotation &amp;</td>
<td>According to you was the password reliable enough?</td>
</tr>
<tr>
<td></td>
<td>Resizing</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Rotation &amp;</td>
<td>Was the system easy to understand?</td>
</tr>
<tr>
<td></td>
<td>Resizing</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Rotation &amp;</td>
<td>According to you how many percent this algorithm is secure?</td>
</tr>
<tr>
<td></td>
<td>Resizing</td>
<td></td>
</tr>
</tbody>
</table>
6.2.2 Participants and Data Collection

Since the new proposed algorithm implemented as a on-line system then the data collection will be simple because the questionnaire will be filled in online. The address of this system was e-mailed to some students at the University of Malaya (N=50). The participants included twenty three males and twenty seven females.

The questionnaire contains a simple plan for checking the memorability of GUABRR password. After the user registers and completes the registration form, he/she must wait for two days before he/she can log-in to the system. Table 6-3 shows the time of the users’ registration and login based on this plan.

Table 6-3: Registration and Log-in Date of Users

<table>
<thead>
<tr>
<th>Days</th>
<th>Registration (users)</th>
<th>Log-in and Complete the Questionnaire (users)</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Day</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>Second Day</td>
<td>20</td>
<td>-</td>
</tr>
<tr>
<td>Third Day</td>
<td>18</td>
<td>27</td>
</tr>
<tr>
<td>Fourth Day</td>
<td>-</td>
<td>21</td>
</tr>
<tr>
<td>Fifth Day</td>
<td>-</td>
<td>2</td>
</tr>
</tbody>
</table>

6.2.3 Questionnaire and Answers

This section shows the answers provided by the users for each question and their analysis. As the answers to the questions are different then one by one for each question, there is a Pie Chart that shows the percentage of the answers and then there is a result summary for the collected data. To calculate the final percentage of each question, this section uses the percentage for each answer then calculates the total result from the feedback data. Table 6-4 shows the related percentage for each answer.
<table>
<thead>
<tr>
<th>Unsatisfied/ No, Definitely Not/ Poor</th>
<th>Not Sure/ No, Not Really/ Fair</th>
<th>Satisfied/ Yes, Generally/ Good</th>
<th>Completely Satisfied/ Yes, Definitely/ Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>50%</td>
<td>70%</td>
<td>100%</td>
</tr>
</tbody>
</table>

### 6.2.3.1. General Part of the Questionnaire

**Q1: Can you create easily your graphical password through registration part?**

This question is designed for testing the “easy to create” feature of usability. The Table 6-5 and Figure 6-1 shows the result of the data collected.

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>18</td>
<td>32</td>
</tr>
</tbody>
</table>

**Result summary:** As the graph shows, 36% of users were generally satisfied with the “easy to create” question and 64% were completely satisfied. In total it means (according to table 6-5) about 89% of users agreed that the registration part was easy. Figure 6-2 shows the result in a report from the automatic report generator of system.
Q2: Does Login thought new graphical password authentication easy?

This question was designed to test the “easy to log-in” feature of usability. The table 6-6 and Figure 6-3 shows the results of the data collected.

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>11</td>
<td>35</td>
</tr>
</tbody>
</table>

Result summary: The graph shows that 2% of users were unsatisfied by the “easy to log-in” question, 6% were note sure, 22% were satisfied by log-in system and 70% were completely satisfied with this question. With regard to table 6-6, it means in total about 92% of users agreed that the log-in phase was easy. Figure 6-4 shows the result of report from the system’s automatic report generator.
Q3: Does Login through new graphical password authentication quick?

This question was designed for testing the “log-in quickly enough” feature of system usability. Table 6-7 and Figure 6-5 shows the results of data collected.

Table 6-7: Data collection table for Q3

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4</td>
<td>17</td>
<td>26</td>
</tr>
</tbody>
</table>

Figure 6-5: Data Collection Pie Chart for Q3

**Result summary:** As the graph shows, 6% of users were not in agreement with the “easy to log-in” question, 8% were not really in agreement with this question, 34% generally agreed to this question and 52% were completely agreement with this question. With regard to table 6-7, it means in total about 81% of users accepted that the log-in phase was quick enough. Figure 6-6 shows the result in a report from the system’s automatic report generator.

3- Does Login through new graphical password authentication quick?
1- No, definitely not: 6%
2- No, not really: 8%
3- Yes, generally: 34%
4- Yes, definitely: 52%

Figure 6-6: Report of System on Q3
Q4: According to you was the system interface pleasant enough?

This question was designed to test the “interface design” feature of system’s usability. Table 6-8 and Figure 6-7 shows the results of data collected.

Table 6-8: Data Collection Table for Q4

<table>
<thead>
<tr>
<th>Poor Design</th>
<th>Fair</th>
<th>Good</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>28</td>
<td>22</td>
</tr>
</tbody>
</table>

Figure 6-7: Data Collection Pie Chart for Q4

Result summary: As the graph shows, 56% of users were satisfied with the “interface pleasant enough” question and 44% were completely satisfied, which means that in total (table 6-8) about 83% of users was satisfied with the interface of the system. Figure 6-8 shows the result of report from the automatic report generator of the system.

Q5: How do you think the mouse and keyboarded usage are well enough?

This question was designed to test the “mouse and keyboard usage” feature of usability. Table 6-9 and Figure 6-9 shows the result of the data collection.
Table 6-9: Data collection table for Q5

<table>
<thead>
<tr>
<th>Poor</th>
<th>Fair</th>
<th>Good</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>31</td>
<td>19</td>
</tr>
</tbody>
</table>

Figure 6-9: Data Collection Pie Chart for Q5

**Result summary:** As shown in the graph, 62% of users were satisfied with the mouse and keyboard usage in the system and 38% were completely satisfied with this question. With regard to table 6-9, it means in totality about 81% of users accepted the usage of the mouse and keyboard in the system. Figure 6-10 shows the result of report from the automatic report generator of the system.

**Table 6-10: Data Collection Table for Q5**

<table>
<thead>
<tr>
<th>Poor</th>
<th>Fair</th>
<th>Good</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>19</td>
<td>24</td>
</tr>
</tbody>
</table>

**Figure 6-10: Report of System on Q5**

**Q6: According to you was the password applicable enough?**

This question was designed to test the “system applicability” feature of usability. The table 6-10 and Figure 6-11 shows the result of the data collection.
Result summary: The graph shows that: 4% of users approved that the system was poor in terms of applicability, 10% found the applicability fair, while 38% thought that the applicability was good and 48% thought that the system was completely applicable. It means in total with regard to table 6-10, about 80% of users accepted this part of system. Figure 6-12 shows the report from the automatic report generator of the system.

6- According to you was the password applicable enough?
1- Poor: 4 %
2- Fair: 10 %
3- Good: 38 %
4- Excellent: 48 %

Q7: According to you how many percent the training part helps you?

This question was designed to test the “functionality of the training page of system”. Table 6-11 and Figure 6-13 shows the result of the data collection.

<table>
<thead>
<tr>
<th>60%-70%</th>
<th>70%-80%</th>
<th>80%-90%</th>
<th>90%-100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>7</td>
<td>29</td>
<td>5</td>
</tr>
</tbody>
</table>
Result summary: As shown in the graph, 18% of users approved 50-70% of the training page functionality, 14% of users approved 50-70% of training page functionality, 58% of users approved 80-90% of training page functionality and 10% of users approved the functionality of training page 90-100%. It means in total that 86% of users accepted the functionality of training page. Figure 6-14 shows the result of report from the automatic report generator of the system.

Q8: How many images you want to select as your graphical password?
This question was designed to test the “graphical password length” usability feature. Table 6-12 and Figure 6-15 shows the result of the data collection.

Table 6-12: Data collection table for Q8

<table>
<thead>
<tr>
<th>Images</th>
<th>2 Images</th>
<th>3 Images</th>
<th>4 Images</th>
<th>5 Images</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14</td>
<td>21</td>
<td>12</td>
<td>3</td>
</tr>
</tbody>
</table>
**Result summary:** The graph shows that 28% of users preferred to select two images as password then type six characters for log-in, 42% of users preferred to select three images as password then type nine characters as password to Log-in, 24% of users preferred four images and just 6% of users preferred five images as password. It means that in total most of the users would rather select three or two images for their password. Figure 6-16 shows the result of report from the automatic report generator of the system.

<table>
<thead>
<tr>
<th>0: How many images you want to select as a your graphical password?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- 2 images: 28 %</td>
</tr>
<tr>
<td>2- 3 images: 42 %</td>
</tr>
<tr>
<td>3- 4 images: 24 %</td>
</tr>
<tr>
<td>4- 5 images: 6 %</td>
</tr>
</tbody>
</table>

Figure 6-16: Report of System on Q8

**Q9:** Do you like to use this algorithm as log-in part of your on-line authentication systems?

This question was designed to test the “user total idea” about the system. Table 6-13 and Figure 6-17 shows the result of the data collection.

<table>
<thead>
<tr>
<th>Table 6-13: Data Collection Table for Q9</th>
</tr>
</thead>
<tbody>
<tr>
<td>60%-70%</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>7</td>
</tr>
</tbody>
</table>
Result summary: As shown in the graph, 14% of users prefer to use this system as an on-line login system between 50-60%, 4% of users prefer to use the system as online system between 60-70%, 28% of users prefer to use the system as online system between 80-90% and 54% of users prefer to use the system 100% as online login system. It means that in total 92% of users prefer to use the system as an online log-in system. Figure 6-18 shows the result of report from the automatic report generator of the system.

Table 6-14: Data Collection Table for Q10

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0</td>
<td>12</td>
<td>33</td>
</tr>
</tbody>
</table>
**Result Summary:** As the graph shows, 10% of users not prefer to use this system as on-line login system, 24% of users generally prefer to use the system as online system and 66% of users definitely prefer to use the system as online login system. It means totally 92% of users prefer to use the system as on-line log-in system. Figure 6-20 shows the result of report from the automatic report generator of system.

**Table 6-15: Data Collection Table for Q11**

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8</td>
<td>9</td>
<td>31</td>
</tr>
</tbody>
</table>

**6.2.3.2. Rotation Part of the Questionnaire**

**Q11:** According to you does your graphical password easy enough to remember?

This question was designed to test the “easy to memorize” feature of usability. Table 6-15 and Figure 6-21 shows the result of the data collection.
**Result summary:** As shown in the graph, only 4% of the users were definitely not in agreement with the “easy to memorize” feature of the system, 16% did not really agree with this question, 18% were generally in agreement while 62% were completely in agreement with this question. With regard to table 6-15, it means that in total about 83% of users accepted that the system and algorithm was memorable enough. Figure 6-22 shows the result of report from the automatic report generator of the system.

**11- Does your graphical password was easy to remember?**
1: No, definitely not: 4 %
2: No, not really: 16 %
3: Yes, generally: 18 %
4: Yes, definitely: 62 %

**Q12: According to you was the password reliable enough??**

This question was designed to test the “reliability” feature of usability. The table 6-16 and Figure 6-23 shows the result of the data collection.
**Result summary:** As shown in the graph, 20% generally agreed to the system’s reliability and 54% completely agreed with this question. It means in total about 78% of the users accepted that the system and algorithm was reliable enough. Figure 6-24 shows the result of report from the automatic report generator of the system.

**Figure 6-24: Report of System on Q12**

<table>
<thead>
<tr>
<th>12- According to you was the password reliable enough?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. No, definitely not: 10 %</td>
</tr>
<tr>
<td>2. No, not really: 16 %</td>
</tr>
<tr>
<td>3. Yes, generally: 20 %</td>
</tr>
<tr>
<td>4. Yes, definitely: 54 %</td>
</tr>
</tbody>
</table>

**Q13: Was the system easy to understand?**

This question was designed to test the “easy to understand” feature of usability. The table 6-17 and Figure 6-25 shows the result of the data collection.

**Table 6-17: Data collection table for Q13**

<table>
<thead>
<tr>
<th>Not Understandable at All</th>
<th>Few Understanding Points</th>
<th>Have Some Ambiguities</th>
<th>Completely Understandable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
<td>9</td>
<td>34</td>
</tr>
</tbody>
</table>
Result summary: The graph shows that, 12% of users could little understand the system, 18% understood but with some ambiguities and 68% completely understood. According to table 6-17, in total about 87% of users understand the algorithm and system completely. Figure 6-26 shows the result of report from the automatic report generator of the system.

Q14: According to you how many percent this algorithm is secure?

This question was designed to test the “security test according to user”. Table 6-18 and Figure 6-27 shows the result of the data collection.

<table>
<thead>
<tr>
<th>60%-70%</th>
<th>70%-80%</th>
<th>80%-90%</th>
<th>90%-100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>12</td>
<td>11</td>
<td>18</td>
</tr>
</tbody>
</table>
Result summary: The graph shows that, 18% of users approved that system is secure between 60-70%, 24% of users approved that system is secure between 70-80%, 22% of users approved that system is secure between 80-90% and 36% of users approved that system is completely secure. It means in total 87% of users think that the system is secure. Figure 6-28 shows the result of report from the automatic report generator of the system.

<table>
<thead>
<tr>
<th>14- According to you how many percent this algorithm is secure?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- 60-70%: 18 %</td>
</tr>
<tr>
<td>2- 70-80%: 24 %</td>
</tr>
<tr>
<td>3- 80-90%: 22 %</td>
</tr>
<tr>
<td>4- 90-100%: 36 %</td>
</tr>
</tbody>
</table>

6.2.3.3. Resizing Part of the Questionnaire

Q15: According to you does your graphical password easy enough to remember?

This question was designed to test the “easy to memorize” feature of usability. Table 6-19 and Figure 6-29 shows the result of the data collection.

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>35</td>
</tr>
</tbody>
</table>
**Result summary:** The graph shows that, 2% of users definitely did not agree to the “easy to memorize” feature of the system, 10% did not really agree with this question, 18% were generally agreement with this question and 70% were completely in agreement with this question. According to table 6-15 it means a total of about 88% of users accepted that the system and algorithm was memorable enough. Figure 6-30 shows the result of report from the automatic report generator of the system.

![Pie Chart](image)

Figure 6-29: Data Collection Pie Chart for Q15

**Q16: According to you was the password reliable enough??**

This question was designed to test the “reliability” feature of usability. Table 6-16 and Figure 6-20 shows the result of the data collection.

![Table](image)

Figure 6-30: Report of System on Q15

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes , Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>8</td>
<td>19</td>
<td>19</td>
</tr>
</tbody>
</table>

Table 6-20: Data collection table for Q16
Result summary: The graph shows that, 38% generally agreed with the reliability in this system and 38% completely agreed with this question. It means in total according to table 6-16 about 74% of users accepted that the system and algorithm was reliable enough. Figure 6-32 shows the result of report from the automatic report generator of the system.

![Data Collection Pie Chart for Q16](image)

Figure 6-31: Data Collection Pie Chart for Q16

Q17: Was the system easy to understand?

This question was designed to test the “easy to understand” feature of usability. Table 6-21 and Figure 6-33 shows the result of the data collection.

<table>
<thead>
<tr>
<th>Not Understandable at All</th>
<th>Few Understanding Points</th>
<th>Have Some Ambiguities</th>
<th>Completely Understandable</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>10</td>
<td>37</td>
</tr>
</tbody>
</table>

Table 6-21: Data collection table for Q17
Result summary: The graph shows that, 6% of users could little understand the system, 20% understood but with some ambiguities and 74% completely understood. It means in total according to table 6-4 about 91% of users understand the algorithm and system completely. Figure 6-34 shows the result of report from the automatic report generator of the system.

Q18: According to you how many percent this algorithm is secure?

This question was designed to test the “security test according to user”. Table 6-18 and Figure 6-22 shows the result of the data collection.
Result summary: The graph shows that, 18% of users approved that system is secure between 50-70%, 22% of users approved that system is secure between 50-70%, 28% of users approved that system is secure between 80-90% and 22% of users approved that system is completely secure. It means that in total 85% of users think that system was secure. Figure 6-36 shows the result of report from the automatic report generator of the system.

6.2.3.4. Rotation and Resizing Part of the Questionnaire

Q19: According to you does your graphical password easy enough to remember?

This question was designed to test the “easy to memories” feature of usability. Table 6-23 and Figure 6-37 shows the result of the data collection.

Table 6-23: Data Collection Table for Q19

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>17</td>
<td>32</td>
</tr>
</tbody>
</table>
Result summary: The graph shows that, 2% of users did not really agree with the “easy to memorize” feature of the system, 34% generally agreed to this question and 64% completely agreed with this question. It means in total according to table 6-15 about 88% of users accepted that the system and algorithm was memorable enough. Figure 6-38 shows the result of report from the automatic report generator of the system.

19- Does your graphical password was easy to remember?
1- No, definitely not: 0 %
2- No, not really: 2 %
3- Yes, generally: 34 %
4- Yes, definitely: 64 %

Q20: According to you was the password reliable enough??

This question was designed to test the “reliability” feature of usability. Table 6-16 and Figure 6-24 shows the result of the data collection.

Table 6-24: Data Collection Table for Q20

<table>
<thead>
<tr>
<th>No, Definitely Not</th>
<th>No, Not Really</th>
<th>Yes, Generally</th>
<th>Yes, Definitely</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>11</td>
<td>37</td>
</tr>
</tbody>
</table>
Result summary: The graph shows that, 22% generally agreed with the reliability in this system and 74% completely agreed with this question. It means in totality according to table 6-16, about 91% of users accepted that the system and algorithm was reliable enough. Figure 6-40 shows the result of report from the automatic report generator of the system.

<table>
<thead>
<tr>
<th>20- According to you was the password reliable enough?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- No, definitely not: 0 %</td>
</tr>
<tr>
<td>2- No, not really: 4 %</td>
</tr>
<tr>
<td>3- Yes, generally: 22 %</td>
</tr>
<tr>
<td>4- Yes, definitely: 74 %</td>
</tr>
</tbody>
</table>

Q21: Was the system easy to understand?

This question was designed to test the “easy to understand” feature of usability. Table 6-25 and Figure 6-41 shows the result of the data collection.

<table>
<thead>
<tr>
<th>Not Understandable at All</th>
<th>Few Understanding Points</th>
<th>Have Some Ambiguities</th>
<th>Completely Understandable</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>11</td>
<td>31</td>
</tr>
</tbody>
</table>
**Result summary:** The graph shows that, 14% of users could little understand the system, 22% understood but with some ambiguities and 62% completely understand the system. It means in total according to table 6-17, about 84% of users understand the algorithm and system completely. Figure 6-42 shows the result of report from the automatic report generator of the system.

![Data Collection Pie Chart for Q21](image)

**Q22:** According to you how many percent this algorithm is secure?

This question was designed to test the “security test according to user”. Table 6-18 and Figure 6-26 shows the result of the data collection.

<table>
<thead>
<tr>
<th>60%-70%</th>
<th>70%-80%</th>
<th>80%-90%</th>
<th>90%-100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>12</td>
<td>16</td>
<td>19</td>
</tr>
</tbody>
</table>

Figure 6-42: Report of System on Q21
**Result summary:** The graph shows that, 6% of users approved that system is secure between 50-70%, 24% of users approved that system is secure between 50-70%, 32% of users approved that system is secure between 80-90% and 38% of users approved that system is completely secure. It means that in total, 90% of users think that system is secure. Figure 6-44 shows the result of report from the automatic report generator of the system.

<table>
<thead>
<tr>
<th>22- According to you how many percent this algorithm is secure?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- 60-70%: 6 %</td>
</tr>
<tr>
<td>2- 70-80%: 24 %</td>
</tr>
<tr>
<td>3- 80-90%: 32 %</td>
</tr>
<tr>
<td>4- 90-100%: 38 %</td>
</tr>
</tbody>
</table>

Figure 6-44: Report of System on Q22

### 6.2.4 Summary of Questionnaire Results

With reference to the above questionnaire results, 92% of users prefer to use graphical password to the textual password. This group of users voted for the system based on three different parts of the questionnaire which Table 6-19 shows in detail.

<table>
<thead>
<tr>
<th></th>
<th>Rotation (%)</th>
<th>Resizing (%)</th>
<th>Rotation and Resizing (%)</th>
<th>Generally (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy of create</td>
<td></td>
<td></td>
<td></td>
<td>89</td>
</tr>
<tr>
<td>Easy to log-in</td>
<td></td>
<td></td>
<td></td>
<td>88</td>
</tr>
<tr>
<td>Easy to memories</td>
<td>83</td>
<td>88</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>Easy to understand</td>
<td>87</td>
<td>91</td>
<td>84</td>
<td></td>
</tr>
<tr>
<td>Reliability</td>
<td>78</td>
<td>74</td>
<td>91</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>87</td>
<td>85</td>
<td>90</td>
<td></td>
</tr>
</tbody>
</table>
With reference to the above table, most of the users approved that the algorithm that uses both the methods of Rotation and Resizing is more reliable, memorable and secure than the other two algorithms. However understanding this method is harder than the other two algorithms.

Also, referring to the Q12 most of the users like to select three or two images for their password, in other words, users do not like to select long passwords for either a GUA or textual password.

6.3 Security Test and Evaluation

As is explained in section 2.5.2, there are two methods of security evaluation in GUA algorithms. The initial part defines the “Graphical Password Space” as one of the methods and then makes a comparison in a table between some previous algorithms and the newly proposed algorithm. Then the second part defines the “Graphical Password Entropy” and makes comparison between some previous algorithms and newly proposed algorithm.

6.3.1 Graphical Password Space

Users can pick any element for their password in GUA; the raw size of password space is an upper bound on the information content of the distribution that users choose in practice. It is not possible to define a formula for password space but for all algorithms it is possible to calculate the password space or the number of passwords that can be generated by the algorithm. Now, this section will define and calculate the password space for previous algorithms and GUABRR, then make a comparative analysis.

For example, in textual passwords with length of 6 characters that can select the capital and small characters, the password space will be:

\[ \text{Space} = 6^{52} \]

In the Passface algorithm with \( N \) rounds and \( M \) pictures in each round, the password space will be:

\[ \text{Space} = M^N \]

In the Blonder algorithm and Passlogix with \( N \) number of pixels on the image and \( M \) number of locations to be clicked, the password space will be:
Space = N^M

In the Syukri algorithm with unlimited patterns for drawing, the password space will be infinity.

In the GUABRR algorithm which includes 25 images in the images matrix, 3 to 5 images can be selected for the password, 3 characters for each password (alphabetic 26, numbers 10, special characters 30), and the password space will be:

\[
\text{Space (Based on 3 images)} = (25^3) \times (66^3) \\
\text{Space (Based on 5 images)} = (25^5) \times (66^5)
\]

Now, Table 6-28 shows the comparison between previous algorithms and the newly proposed algorithm based on password space.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets)</td>
<td>(52^6)</td>
</tr>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets and numbers)</td>
<td>(62^6)</td>
</tr>
<tr>
<td>Image selection similar to Passface (4 runs, 9 pictures)</td>
<td>(9^4)</td>
</tr>
<tr>
<td>Click based algorithm similar to Passpoint (4 loci and assuming 30 salient points)</td>
<td>(30^4)</td>
</tr>
<tr>
<td>GUABRR (select 3 images from 25 images and 3 characters for each image in Log-in part)</td>
<td>((25^3) \times (66^3))</td>
</tr>
</tbody>
</table>

6.3.2 Graphical Password Entropy

Password entropy is usually used to measure the security of a generated password, which conceptually means how hard to blindly guess out the password. For simplicity, assume all passwords are evenly distributed, the password entropy of a graphic password can then be calculated as follows.

\[
\text{Entropy} = N \log_2 ([L][O][C])
\]
In other words, Graphical password entropy tries to measure the probability that the attacker obtains the correct password based on random guessing (Zhi et al. 2005).

In the above formula, N is the length or number of runs, L is locus alphabet as the set of all loci, O is an object alphabet and C is color of the alphabet. For example in a point click GUA algorithm that runs for four rounds and has 30 salient points with 4 objects and 4 colors then:

\[
\text{Entropy} = 4 \times \log_2 (30 \times 4 \times 4) = 35.6
\]

In an image selection algorithm with 5 runs and in each run selects 1 from 9 images then:

\[
\text{Entropy} = 5 \times \log_2 (9) = 15.8
\]

For the proposed algorithm, 3 to 5 images will be selected as passwords from 25 images, each image can rotate at 12 different degrees and resizes in 2 different sizes. So the entropy will be:

\[
\begin{align*}
\text{Entropy (based on 3 images)} &= 3 \times \log_2 (25 \times 12 \times 2) = 27.7 \\
\text{Entropy (based on 5 images)} &= 5 \times \log_2 (25 \times 12 \times 2) = 46.3
\end{align*}
\]

Now, table 6-29 shows the comparison between previous algorithms and the new proposed algorithm.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Formula</th>
<th>Entropy (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets)</td>
<td>(6 \times \log_2 (52))</td>
<td>34.32</td>
</tr>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets and numbers)</td>
<td>(6 \times \log_2 (62))</td>
<td>35.70</td>
</tr>
<tr>
<td>Image selection similar to Passface (4 runs, 9 pictures)</td>
<td>(4 \times \log_2 (9))</td>
<td>12.74</td>
</tr>
<tr>
<td>Click based algorithm similar to Passpoint (4 loci and assuming 30 salient points)</td>
<td>(4 \times \log_2 (30))</td>
<td>19.69</td>
</tr>
<tr>
<td>GUABRR (select 5 images from 25 images and 12 degrees rotation and 2 resizing options)</td>
<td>(5 \times \log_2 (25 \times 12 \times 2))</td>
<td>46.37</td>
</tr>
</tbody>
</table>
6.4 Conclusion

This chapter tested and evaluated the proposed algorithm and system using usability and security features. For usability evaluation, an online questioneer designed based on ISO usability standard attributes. Around 50 participants form university of Malaya, includes twenty three males and twenty seven females complete the online questioneer. According to the feedback, the GUABRR is usable especially in easy to memories, easy to understand and reliability.

For security features, two distincts items named the “Password Entropy” and “Password Spaces” were described and calculated. The result shows the proposed algorithm is more time secure than the previous algorithms.

Finally, the result of the testing and evaluation shows that the proposed system not only covers the usability features but also was secure in comparison with other algorithms. In other words, the GUABRR algorithm can successfully balance the usability and security features.
Chapter 7: Conclusion and Future works

7.1 Thesis Summary

User authentication is the most critical element in the field of Information Security. There are three different authentication categories which are Inherit Based Authentication, Token Based Authentication and Knowledge Based Authentication (Rachna and Adrian, 2000).

Knowledge based authentication is widely used since it is cheaper and does not require special tools and devices. There are two different methods within this category which are Textual Password and Graphical Password. A setback in textual password is the length of a selected password by a user. If a particular user selects a short password, it can be discovered by any attacker easily while a long password is hard to remember. Meanwhile, users may prefer to select the same password for different purposes which reduce the security drastically.

It is proven that people are able to recognize and remember combinations of geometrical shapes, patterns, textures and colors better than meaningless alphanumeric characters, making the graphical user authentication to be greatly desired as a possible alternative to textual passwords. The graphical password algorithm is categorised into three groups as followings:

(i) **Pure recall based techniques:** The user password is a painted shape drawn by the users in an empty screen however there is no possibility of using reminder and marks.

(ii) **Cued recall based techniques:** The system prescribes a framework of reminders, hints and gestures for the users to help them reproduce their passwords.

(iii) **Recognition based techniques:** Users have to select their passwords from a grid of images which are retrieved from a database of images.
All the algorithms in these three categories are reviewed in this project through explaining their definitions and weaknesses. In the next step the usability and security features of all these algorithms are compared with each other. The table 7.1 shows the algorithms which are reviewed in this project.

Table 7.1: Algorithms in Three Categories of GUA

<table>
<thead>
<tr>
<th>Technique (s)</th>
<th>Name of Algorithm (s)</th>
<th>Year</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognition Base</td>
<td>Passface</td>
<td>2000</td>
<td>Sacha Brostoff, M. Angela Sasse</td>
</tr>
<tr>
<td></td>
<td>Déjà vu</td>
<td>2000</td>
<td>Rachna Dhamija, Adrian Perrig</td>
</tr>
<tr>
<td></td>
<td>Triangle</td>
<td>2002</td>
<td>Leonardo Sobrado, J-Canille Birget</td>
</tr>
<tr>
<td></td>
<td>Movable Frame</td>
<td>2002</td>
<td>Leonardo Sobrado, J-Canille Birget</td>
</tr>
<tr>
<td></td>
<td>WIW</td>
<td>2003</td>
<td>ShushuangMan, et al.</td>
</tr>
<tr>
<td></td>
<td>Story</td>
<td>2004</td>
<td>Darren Davies, et al.</td>
</tr>
<tr>
<td>Cued Recall Based</td>
<td>Blonder</td>
<td>1996</td>
<td>Greg E. Blonder</td>
</tr>
<tr>
<td></td>
<td>Passlogix v-Go</td>
<td>2002</td>
<td>Passlogic Inc. Co.</td>
</tr>
<tr>
<td></td>
<td>VisKey SFR</td>
<td>2003</td>
<td>SFR Company</td>
</tr>
<tr>
<td></td>
<td>PassPoint</td>
<td>2005</td>
<td>Susan Wiedenbeck, et al.</td>
</tr>
<tr>
<td></td>
<td>Pass-Go</td>
<td>2006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passmap</td>
<td>2006</td>
<td>Roman v. yamponski</td>
</tr>
<tr>
<td></td>
<td>Background DAS (BDAS)</td>
<td>2007</td>
<td>Paul duaphi</td>
</tr>
<tr>
<td>Pure Recall Based</td>
<td>Draw a secret (DAS)</td>
<td>1999</td>
<td>Jermyn Ian et al.</td>
</tr>
<tr>
<td></td>
<td>Passdoodle</td>
<td>1999</td>
<td>Christopher varenhorst</td>
</tr>
<tr>
<td></td>
<td>Grid Selection</td>
<td>2004</td>
<td>Juaie thorpe, p.c. van oorschot</td>
</tr>
<tr>
<td></td>
<td>Syukri</td>
<td>2005</td>
<td>Syukri, et al.</td>
</tr>
<tr>
<td></td>
<td>Qualitative DAS (QDAS)</td>
<td>2007</td>
<td>Di Lin, et al.</td>
</tr>
</tbody>
</table>

The main aim of the project is to propose a new graphical user authentication based on rotation and resizing (GUABRR Algorithm). There are two important options which should be considered in designing the GUABRR algorithm which cause the algorithm to be accepted or rejected. These options are Usability and Security.

Usability is “A set of attributes that bear on the effort needed for use and on the individual assessment of such use, by a stated or implied set of users”. This project
reviews three ISO named, 13407, 9126 and 9241 to find the usability features and considers them in designing the GUABRR algorithm. The summary of this part reveals that in order to fulfill the usability of our new algorithm, effectiveness, efficiency and satisfaction of users should be considered.

Security features should certainly consider the algorithm to be resistant against common attacks of GUA. Brute force attacks, Dictionary, Spyware, Shoulder surfing and Social engineering attacks are five most common attacks in authentication phase. By reviewing and analysing these attacks, the project attempts to design the algorithm to be secure against the mentioned attack types.

**GUABRR Algorithm**

The GUABRR algorithm is a new scheme which is a mixture of recognition-based and cued recall-based algorithm based on rotation and resizing. In the registration phase of GUABRR algorithm, 25 images are shown to users. Users can select any number of pictures as their passwords. The main reason for such open boundary is to have a feedback from users to determine how many pictures they prefer to select as their password.

For login phase, all 25 images are shown to users again but three special processes change the interface of each picture.

(i) **Rotation:** As it is shown in Figure 7.1, the pictures can rotate in 12 different angles (30, 45, 60, 90, 120, 135, 150, 180, 210, 240, 270 and 315) randomly which cause the algorithm to be more secured since the attacker sees the login phase differently each time.

![Figure 7.1: Rotation of Image in GUABRR Algorithm](image-url)
(ii) **Resizing:** As the resizing process is shown in Figure 7.2, the picture in the login phase can resize 40 percent.

![Figure 7.2: Resizing of Image in GUABRR Algorithm](image)

(iii) **Rotation and Resizing:** The two methods are mixed with each other causing the algorithm to rotate and resize at the same time (Figure 7.3).

![Figure 7.3: Rotation and Resizing of Image in GUABRR Algorithm](image)

All three methods are tested separately and user’s opinions are gathered to see how usable each of these methods was. As the algorithm is designed for a website named “http://www.graphicalpassword.net”, the questionnaire on the website is filled by the users who tested all three methods. This helps to find which methods were most usable. The summary of questionnaire is shown in table 7.2.

<table>
<thead>
<tr>
<th></th>
<th>Rotation</th>
<th>Resizing</th>
<th>Rotation and Resizing</th>
<th>Generally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy of creation</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>89</td>
</tr>
<tr>
<td>Easy to log-in</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>88</td>
</tr>
<tr>
<td>Easy to memorise</td>
<td>83</td>
<td>88</td>
<td>88</td>
<td>-</td>
</tr>
<tr>
<td>Easy to understand</td>
<td>87</td>
<td>91</td>
<td>84</td>
<td>-</td>
</tr>
<tr>
<td>Reliability</td>
<td>78</td>
<td>74</td>
<td>91</td>
<td>-</td>
</tr>
<tr>
<td>Security</td>
<td>87</td>
<td>85</td>
<td>90</td>
<td>-</td>
</tr>
</tbody>
</table>
The results show that combining Rotation and Resizing method is a more secure and reliable method compared to two others, but the two other algorithms are easier to understand by the users.

In order to test the security of the GUABRR algorithm, “Password Entropy” and “Password Space” are calculated and the results are concluded in the table 7-3 and 7-4.

Table 7-3: Comparative Table Based on “Password Space”

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets)</td>
<td>$52^6$</td>
</tr>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets and numbers)</td>
<td>$62^6$</td>
</tr>
<tr>
<td>Image selection similar to Passface (4 runs, 9 pictures)</td>
<td>$9^4$</td>
</tr>
<tr>
<td>Click based algorithm similar to Passpoint (4 loci and assuming 30 salient points)</td>
<td>$30^4$</td>
</tr>
<tr>
<td><strong>GUABRR (select 3 images from 25 images, and 3 characters for each image in Log-in part)</strong></td>
<td>$(25^3) * (66^3)$</td>
</tr>
</tbody>
</table>

Table 7-4: Comparative Table Based on “Password Entropy”

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Formula</th>
<th>Entropy (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets)</td>
<td>$6 \times \log_2(52)$</td>
<td>34.32</td>
</tr>
<tr>
<td>Textual (with 6 characters length include capital and small alphabets and numbers)</td>
<td>$6 \times \log_2(62)$</td>
<td>35.70</td>
</tr>
<tr>
<td>Image selection similar to Passface (4 runs, 9 pictures)</td>
<td>$4 \times \log_2(9)$</td>
<td>12.74</td>
</tr>
<tr>
<td>Click based algorithm similar to Passpoint (4 loci and assuming 30 salient points)</td>
<td>$4 \times \log_2(30)$</td>
<td>19.69</td>
</tr>
<tr>
<td><strong>GUABRR (select 5 images from 25 images, and 12 degrees rotation and 2 resizing options)</strong></td>
<td>$5 \times \log_2((25<em>12</em>2))$</td>
<td>46.37</td>
</tr>
</tbody>
</table>
The results demonstrate that the proposed algorithm is more secure when compared with previous ones. The result of test and evaluation shows that the proposed system not only covers the usability features but was also more secure in comparison with other algorithms. In other words, the GUABRR algorithm is successfully balanced between the usability and security features.

7.2 Thesis Contribution

Although unfortunately from 1996 many researchers have been done on creating various graphical password authentications, none of these algorithms can be used widely in compare the textual password. This is because the designers could not cover the usability and security at the same time.

The most important contribution of the project is covering the usability and Security features by new proposed algorithm. This algorithm will increase the security of GUA by using the Rotation and Resizing process on the images. The new algorithm can be run as Log-In part on all secure websites such as Bank, Police, Companies, Universities and Schools.

Another contribution of the project is increasing the security which are resistant to common attacks like shoulders surfing and guessing attack. Also the proposed algorithm covered the usability features such as easy to creation, easy to Log-in, easy to understand, easy to memorise, and reliability as third contribution.

For proving the corrective of security the designer calculate the password entropy and password space through mathematical calculation which is the result for the last contribution.

7.3 Future Works

The current project showed simple processing on image like Rotation and Resizing create the giant step for making the algorithm more secure. This research found many other ways for making the GUA algorithms more secure and usable such as:
7.4 Thesis Conclusion

Balancing Usability and Security will always be an issue in GUA. There are new challenges to overcome faults in authentication systems. On the other hand, advances are being made to overcome such issues. This thesis introduces a new GUA algorithm for recognition base graphical password based on Rotation and Resizing process on images as recall based algorithms. Studies on usability features based on ISO standards (9241, 9126, 13407) and common attacks based on attacks standards were performed and a comparative table for GUA algorithms was prepared. The usability and security features extracted from this study were used to build a new algorithm called GUABRR to make the algorithm more usable and secure. The test and evaluation of the GUABRR algorithm was done by analysing usability and security. To determine the usability of GUABRR algorithm, an on-line questionnaire system designed based on ISO features. Password Spaces and Password Entropy were employed to test the security of the GUABRR algorithm. The result of two categories of evaluation indicates that proposed algorithm performed very well, not only covering the usability and security but also providing improvement on both of them. It means the proposed algorithm provides a good balance between usability and security features in GUA algorithms.
References


Alain Abran, Witold Sury, Adel Khelifi, Juergen Rilling, Ahmed Seffah; 2003, “Consolidating the ISO Usability Models”; Concordia University, Montreal, Canada.


Qibin Sun, Zhi Li, Xudong Jiang, Alex Kot; 2008, “An Interactive and Secure User Authentication Scheme for Mobile Devices”; supported by the A-STAR SERC Mobile Media TSRP Grant No 062 130 0056, IEEE.


Sacha Brostoff, M. Angela Sasse; 2008, “Are Passfaces More Usable Than Passwords? (A Field Trial Investigation)”, Department of Computer Science, University College London, WC1E 6BT.


Zhi Li, Qibin Sun, Yong Lian, and D. D. Giust; 2005, “AN ASSOCIATION-BASED GRAPHICAL PASSWORD DESIGN RESISTANT TO SHOULDER-SURFING ATTACK”; University of Cagliari, Cagliari 09123, Italy; IEEE.
Appendix A: Summary of ISO Standard 9241

ISO 9241 is a branch of ISO standard; define the requirement for efficiency in the working environment like office. The 17 separate parts contain in this ISO which part eleven define the usability. According to this definition usability encompasses effectiveness, efficiency and satisfaction. (Alain Abran et al. 2003):

- Effectiveness that describes the interaction from a process point of view;
- Efficiency that is the attention for results and resources implied;
- Satisfaction that refers to a user point of view.

There are some recommendations for the environment attribute, software or hardware ISO 9241 provides requirements and recommendations concerning hardware, software and environment attributes that contribute to usability, and subjacent ergonomic principles. Parts 3 to 9 deal with hardware design requirements and guidelines that can have implications on software. Parts 10 to 17 deal with software attributes (Alain Abran et al. 2003). The Figure below shows the structure of this ISO.
ISO 9241
Ergonomic requirements for office work visual display terminals (VDTs)

Structure of ISO 9241 with 17 Parts of it

9241-11 Especially for Usability:

Part 11 of this standard explains how to identify the information that it is necessary when specifying or evaluating usability in terms of measures of user performance and satisfaction. Guidance is given on how to describe the context of use of the product and the measures of usability in an explicit way. In spite of the name, the definitions of part 11, under Usability Guideline, are also known to be applicable to other situations where a user interacts with a product to achieve certain objectives. This extension makes usability a general concept, of application outside
its conventional applications in information technology. According to this standard, the measurement of system usability consists of three usability attributes:

1. **Effectiveness**: How well do the users achieve the goals they set out to achieve using the system?

2. **Efficiency**: The resources consumed in order to achieve their goals.

3. **Satisfaction**: How the users feel about their use of the system?

   ISO 9241-11 recommends a process oriented approach for usability, by which the usable interactive system is achieved through a human centered design process (Alain Abran *et al.* 2003).
Appendix B: Summary of ISO Standard 9126

ISO 9126 addresses software quality from a product point of view. It is probably the most extensive software quality model, even if it is not exhaustive. Initially published in 1991, the approach of its quality model is to present quality as a whole set of characteristics. It divides software quality into six general categories: functionalities, reliability, usability, effectiveness, maintainability and portability (Alain Abran et al. 2003). Figure below shows the structure of this ISO.

<table>
<thead>
<tr>
<th>External and internal quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
</tr>
<tr>
<td>Suitability</td>
</tr>
<tr>
<td>Accuracy</td>
</tr>
<tr>
<td>Interoperability</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Functionality</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
</tbody>
</table>

The Structure of ISO 9126 with 6 Parts of it

Part four of ISO 9126 defines the usability as "A set of attributes that bear on the effort needed for use and on the individual assessment of such use, by a stated or implied set of users". It proposed then a product oriented usability approach. Usability was seen as an independent factor of software quality. It treated software attributes, mainly its interface that makes it easy to use. As you see in Figure 2-31, the major attributes are: Understandability, Learnability, Operability, Atractiveness (Alain et al. 2003).
Appendix C: Summary of ISO Standard 13407

This International Standard provides guidance on human-centered design activities throughout the life cycle of computer-based interactive systems. It is aimed at those managing design processes and provides guidance on sources of information and standards relevant to the human-centred approach (International Standard ISO 13407 first edition). This International Standard:

- Is concerned with both hardware and software components of interactive systems. NOTE Computer-based interactive systems vary in scale and complexity. Examples include off-the-shelf (shrink wrap) software products, custom office systems, plant monitoring systems, automated banking systems and consumer products (International Standard ISO 13407 first edition).

- Addresses the planning and management of human-centred design. It does not address all aspects of project management (International Standard ISO 13407 first edition).

- Provides an overview of human-centred design activities. It does not provide detailed coverage of the methods and techniques required for human-centred design, nor does it address health and safety aspects in detail (International Standard ISO 13407 first edition).

- The main users being project managers, therefore addresses technical human factors and ergonomics issues only to the extent necessary to allow managers to understand their relevance and importance in the design process as a whole. Such issues are dealt with more fully in ISO 9241 which is complementary to this International Standard and is aimed at system developers, specifiers and purchasers of systems. Nonetheless, all parties involved in human-centred system development, including the end-users of systems, should find the guidance in this International Standard relevant (International Standard ISO 13407 first edition).

For the purposes of this International Standard, the following terms and definitions apply (International Standard ISO 13407 first edition).
**Term1: Interactive system**

Combinations of hardware and software components that receive input from, and communicate output to, a human user in order to support his or her performance of a task.

NOTE the term “system” is often used rather than “interactive system”.

**Term2: Prototype**

Representation of all or part of a product or system that, although limited in some way, can be used for evaluation.

**Term3: Usability**

Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (Alain et al. 2003).

**Term4: Effectiveness**

Accuracy and completeness with which users achieve specified goals (Alain et al. 2003).

**Term5: Efficiency**


**Term6: Satisfaction**

Freedom from discomfort, and positive attitudes to the use of the product (Alain et al. 2003) (International Standard ISO 13407 First edition)

**Term7: Context of use**

Users, tasks, equipment (hardware, software and materials), and the physical and social environment in which a product is used (Alain et al. 2003) (International Standard ISO 13407 First edition).
**Term8: User**

Individual interacting with the system (Alain *et al.* 2003) (International Standard ISO 13407 First edition)

Finally, The Usability Model that is defined by ISO 13407 comprises of five stages, which are implicitly joined in a loop. Figure below proscribes this model graphically (International Standard ISO 13407 First edition).

![ISO 13407 Model With 5 Parts of it](image-url)
Appendix D: Snapshot of On-line Questionnaire Page (Own Questionnaire)

1- Can you create easily your graphical password through registration?
   1- No, definitely not: 0 %
   2- No, not really: 0 %
   3- Yes, generally: 36 %
   4- Yes, definitely: 64 %

2- Does Login through new graphical password authentication easy?
   1- No, definitely not: 2 %
   2- No, not really: 6 %
   3- Yes, generally: 22 %
   4- Yes, definitely: 70 %

3- Does Login through new graphical password authentication quick?
   1- No, definitely not: 6 %
   2- No, not really: 8 %
   3- Yes, generally: 34 %
   4- Yes, definitely: 52 %

4- According to you was the system interface pleasant enough?
   1- Poor design: 0 %
   2- Fair: 0 %
   3- Good: 56 %
   4- Excellent: 44 %

5- How do you think the mouse and keyboard usage are well enough?
   1- Poor design: 0 %
   2- Fair: 0 %
   3- Good: 62 %
   4- Excellent: 38 %

6- According to you was the password applicable enough?
   1- Poor: 4 %
   2- Fair: 10 %
   3- Good: 38 %
   4- Excellent: 48 %

7- According to you how many percent the training help you?
   1- 60-70%: 18 %
   2- 70-80%: 14 %
   3- 80-90%: 58 %
   4- 90-100%: 18 %

8- How many images you want to select as a your graphical password?
   1- 2 images: 28 %
   2- 3 images: 42 %
   3- 4 images: 24 %
   4- 5 images: 6 %

9- Do you like to use this algorithm as login part of your online authentication system?
   1- 60-70%: 14 %
   2- 70-80%: 4 %
   3- 80-90%: 28 %
   4- 90-100%: 54 %

10- Do you prefer graphical password to textual password?
    1- No, definitely not: 10 %
    2- No, not really: 0 %
    3- Yes, generally: 24 %
    4- Yes, definitely: 66 %
Login by Rotation

11- Does your graphical password was easy to remember?
1- No, definitely not: 4 %
2- No, not really: 16 %
3- Yes, generally: 18 %
4- Yes, definitely: 52 %

12- According to you was the password reliable enough?
1- No, definitely not: 10 %
2- No, not really: 16 %
3- Yes, generally: 20 %
4- Yes, definitely: 54 %

13- Was the system easy to understand?
1- Not understandable at all: 2 %
2- Few understanding points: 12 %
3- Have some ambiguities: 18 %
4- Completely understandable: 68 %

14- According to you how many percent this algorithm is secure?
1- 60-70%: 13 %
2- 70-80%: 24 %
3- 80-90%: 22 %
4- 90-100%: 30 %
Login by Resizing

15- Does your graphical password was easy to remember?
1- No, definitely not: 2 %
2- No, not really: 10 %
3- Yes, generally: 18 %
4- Yes, definitely: 70 %

16- According to you was the password reliable enough?
1- No, definitely not: 8 %
2- No, not really: 16 %
3- Yes, generally: 38 %
4- Yes, definitely: 38 %

17- Was the system easy to understand?
1- Not understandable at all: 0 %
2- Few understanding points: 6 %
3- Have some ambiguities: 20 %
4- Completely understandable: 74 %

18- According to you how many percent this algorithm is secure?
1- 60-70%: 18 %
2- 70-80%: 32 %
3- 80-90%: 28 %
4- 90-100%: 22 %
19- Does your graphical password was easy to remember?
1- No, definitely not: 0 %
2- No, not really: 2 %
3- Yes, generally: 34 %
4- Yes, definitely: 64 %

20- According to you was the password reliable enough?
1- No, definitely not: 0 %
2- No, not really: 4 %
3- Yes, generally: 22 %
4- Yes, definitely: 74 %

21- Was the system easy to understand?
1- Not understandable at all: 0 %
2- Few understanding points: 14 %
3- Have some ambiguities: 22 %
4- Completely understandable: 62 %

22- According to you how many percent this algorithm is secure?
1- 50-70%: 5 %
2- 70-80%: 24 %
3- 80-90%: 32 %
4- 90-100%: 30 %

Total Users: 50
Appendix E: Source Code of GUABRR System in Registration and Log-in Phase

Login-Both.aspx

```<%@ Page Language="VB" AutoEventWireup="false" CodeFile="Login-Both.aspx.vb" Inherits="Login" MasterPageFile="~/MasterPage.master" ValidateRequest="false" %>
<asp:content ID="Content1" ContentPlaceHolderID="ContentPlaceHolder1" runat=server>
<form id=frm_Login runat=server>
<TABLE border=0 align=center cellPadding=0 width="100%" style="border-collapse: collapse" class=Txt_Black_Normal cellspacing=0>
<tr>
<TABLE border=0 align=center cellPadding=0 width="100%" style="border-collapse: collapse" class=Txt_Black_Normal cellspacing=0>
<tr style="height: 5px;"><td align=left></td></tr>
<tr>
        <td align=left valign=top>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&n...```
<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="~/images/Images/Password.jpg" alt="Image" /></td>
<td><img src="~/images/Images/Password.jpg" alt="Image" /></td>
<td><img src="~/images/Images/Password.jpg" alt="Image" /></td>
<td><img src="~/images/Images/Password.jpg" alt="Image" /></td>
<td><img src="~/images/Images/Password.jpg" alt="Image" /></td>
<td></td>
</tr>
</tbody>
</table>

**Image Url:** ~/images/Images/Password.jpg

---

**Image Url:** ~/images/Images/Password.jpg

---

**Image Url:** ~/images/Images/Password.jpg

---

**Image Url:** ~/images/Images/Password.jpg

---

**Image Url:** ~/images/Images/Password.jpg

---

*Note: The table represents a layout with images and labels.*
<table>
<thead>
<tr>
<th>ID</th>
<th>Runat</th>
<th>Width</th>
<th>BackColor</th>
<th>Style</th>
<th>Image URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>lbl_password_7</td>
<td>server</td>
<td>50</td>
<td>White</td>
<td></td>
<td>~/images/Images/Password.jpg</td>
</tr>
<tr>
<td>lbl_password_8</td>
<td>server</td>
<td>50</td>
<td>White</td>
<td></td>
<td>~/images/Images/Password.jpg</td>
</tr>
<tr>
<td>lbl_password_9</td>
<td>server</td>
<td>50</td>
<td>White</td>
<td></td>
<td>~/images/Images/Password.jpg</td>
</tr>
<tr>
<td>lbl_password_10</td>
<td>server</td>
<td>50</td>
<td>White</td>
<td></td>
<td>~/images/Images/Password.jpg</td>
</tr>
</tbody>
</table>
<tr><td style="vertical-align:middle">
<asp:label ID="lbl_password_11" runat="server" Width=50></asp:label></td></tr>
<tr><td style="vertical-align:middle">
<asp:label ID="lbl_password_12" runat="server" Width=50></asp:label></td></tr>
<tr><td style="vertical-align:middle">
<asp:label ID="lbl_password_13" runat="server" Width=50></asp:label></td></tr>
<tr><td style="vertical-align:middle">
<asp:label ID="lbl_password_14" runat="server" Width=50></asp:label></td></tr>
<tr><td style="vertical-align:middle">
<asp:label ID="lbl_password_15" runat="server" Width=50></asp:label></td></tr>
<tr><td style="vertical-align:middle"
bgcolor=#26231e>
<asp:image Width=70 Height=70 ID="Img_Password_16" runat="server" ImageUrl="/images/Images/Password.jpg" />
</td></tr>
<tr><td style="vertical-align:middle"
bgcolor=#26231e>
<asp:image Width=70 Height=70 ID="Img_Password_17" runat="server" ImageUrl="/images/Images/Password.jpg" />
</td></tr>
<tr><td style="vertical-align:middle"
bgcolor=#26231e>
<asp:image Width=70 Height=70 ID="Img_Password_18" runat="server" ImageUrl="/images/Images/Password.jpg" />
</td></tr>
<tr><td style="vertical-align:middle"
bgcolor=#26231e>
<asp:image Width=70 Height=70 ID="Img_Password_19" runat="server" ImageUrl="/images/Images/Password.jpg" />
</td></tr>
<asp:image Width=70 Height=70 ID="Img_Password_24" runat="server" ImageUrl="~/images/Images/Password.jpg" />
</td>
<td width=2></td>
<td style="vertical-align:middle" bgcolor="#26231e">
<asp:image Width=70 Height=70 ID="Img_Password_25" runat="server" ImageUrl="~/images/Images/Password.jpg" />
</td>
</tr>
<tr>
<td style="vertical-align:middle">
<asp:label ID="lbl_password_21" runat="server" Width=50></asp:label>
</td>
<td width=2></td>
<td style="vertical-align:middle">
<asp:label ID="lbl_password_22" runat="server" Width=50></asp:label>
</td>
<td width=2></td>
<td style="vertical-align:middle">
<asp:label ID="lbl_password_23" runat="server" Width=50></asp:label>
</td>
<td width=2></td>
<td style="vertical-align:middle">
<asp:label ID="lbl_password_24" runat="server" Width=50></asp:label>
</td>
<td width=2></td>
<td style="vertical-align:middle">
<asp:label ID="lbl_password_25" runat="server" Width=50></asp:label>
</td>
</tr>
</table>
<tr><td style="height:10px"></td></tr>
<tr>
<td align=center>
<table border=0>
<tr>
<td>Password:&nbsp;&nbsp;&nbsp;&lt;asp: textbox ID="Txt_Password" runat="server"
TextMode="Password"></asp: textbox&gt;
<td><asp:label Visible=false Text="Dear User, Your password is wrong" ForeColor="Red" runat=server ID="lbl_error"></asp:label></td>
<td><asp:requiredfieldvalidator ID="RequiredFieldValidator2" runat="server"
ErrorMessage="Please enter Password" ControlToValidate="Txt_username"></asp:requiredfieldvalidator></td>
</tr>
</table>
</td>
</tr>
---

Project Name: Graphical User Authentication Algorisme (GUABRR) 

Author: Arash Habibi Lashkari 

Page Name: Login-Both.aspx 

---

imports System.Drawing
imports System.Data
imports System.IO

Partial Class Login
Inherits System.Web.UI.Page

Private Obj_User as new CLS_UserInfo
Private Obj_ImageOriginal as new CLS_Image_Original
Private Obj_Function as New CLS_Functions

Private bln_flag as Boolean
Private Int.Counter as Integer
Private Int.Counter.Password as Integer = 0
Private Int.Arr_RandomAscii.Counter as Integer = 0
Private count as Integer
Private Int_Password_Lenght as Integer
Private Img_temp as System.Drawing.Image
Private Arr_Random_PasswordandDecoy() = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}
Private Arr_Random_Ascii() = {"",","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","","

Private sub Login_Decoy_Random()

'Objective: Create unrepeated Random number
'
'Input: -
'
'Output:create an array of 25 unreapeted number

Dim Rand_Number As new Random
Dim Rand_Image As Integer
Dim Flag_Loop As Integer
Dim Int.LoopCounter As Integer

Rand_Image = Rand_Number.Next (1,26)
Flag_Loop = 1

while (Flag_Loop = 1)
    Flag_Loop = 0
    for Int.LoopCounter = 0 to count
        if (Arr_Random_PasswordandDecoy(Int.LoopCounter) = Rand_Image) or Rand_Image > 25
            Flag_Loop = 1
            Rand_Image = Rand_Number.Next(1, 26)
exit for
end if
next
end while

Arr_Random_PasswordandDecoy(count) = Rand_Image
count = count + 1

End sub

Protected Sub ImgBtn_Submit_Click(ByVal sender As Object, ByVal e As System.Web.UI.ImageClickEventArgs) Handles ImgBtn_Submit.Click
'
'Objective: Trace the password textbox to check if it is correct or not. The textbox compare with an array which contain the password of user
'
'Input: All controls of the page
'
'Output: Set 25 images URL randomly
'
Dim Flag_Find_Password as Boolean = true
Dim Arr_Password as String() = session ("Arr_Password")
Int_Password_Lenght = session ("Int_PasswordLenght")

for Int_Counter_Password = 0 to Int_Password_Lenght - 1
    Dim Int_Position as Integer = me.Txt_Password.Text.IndexOf(Arr_Password(Int_Counter_Password))
    if Int_Position = -1 then
        Flag_Find_Password = False
        exit For
    else
        Arr_Password(Int_Counter_Password) = ""
    End If
Next
if Flag_Find_Password = "true" then response.Redirect ("Login-success.aspx?UserID=" & Session("Int_UserID")) else
lbl_error.Visible = True
End Sub

Protected Sub Txt_Username_TextChanged(ByVal sender As Object, ByVal e As System.EventArgs) Handles Txt_Username.TextChanged
Dim Str_QueryCreator as String = ""
Dim Str_Password as String = ""

if me.Txt_Username.Text <> "" then
    '_________________________________________________
    'Retreive the password
    '_________________________________________________
    Obj_User.Select_User_ByUsername (me.Txt_Username.Text)
    if obj_User.str_username = "" then
        lbl_username.Visible=True
        exit Sub
    else
        lbl_username.Visible=false
    End If
    Session("Int_UserID") = Obj_User.Int_ID
  end if
end while

Arr_Random_PasswordandDecoy(count) = Rand_Image
count = count + 1
End sub
Dim Arr_Password() as string = Obj_User.str_Password.ToString.Split("-")
Int_Password_Lenght = Arr_Password.Length - 1
for Int.Counter = 0 to Int_Password_Lenght - 1
  'Set first cells of array with user password
  Arr_Random_PasswordandDecoy(Int.Counter) = Arr_Password(int_counter)
Next

count = Int_Password_Lenght
for Int.Counter = 0 to 25-Int_Password_Lenght -1
  'Set the other cell of array with decoy id
  Login_Decoy_Random()
Next

Dim Arr_Random_Location = Obj_Function.RandomNumberCreator(26)
Arr_Random_Ascii = Obj_Function.Random_Ascii_Generator()
for Int.Counter=0 to 24
  'Fetch from database the name of picture
  Select case Arr_Random_Location(Int.Counter)
    Case 1
      me.Img_Password_1.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_1.Text= Arr_Random_Ascii(Int.Counter)
    Case 2
      me.Img_Password_2.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_2.Text= Arr_Random_Ascii(Int.Counter)
    Case 3
      me.Img_Password_3.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_3.Text= Arr_Random_Ascii(Int.Counter)
    Case 4
      me.Img_Password_4.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_4.Text= Arr_Random_Ascii(Int.Counter)
    Case 5
      me.Img_Password_5.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_5.Text= Arr_Random_Ascii(Int.Counter)
    Case 6
      me.Img_Password_6.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_6.Text= Arr_Random_Ascii(Int.Counter)
    Case 7
      me.Img_Password_7.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_7.Text= Arr_Random_Ascii(Int.Counter)
    Case 8
      me.Img_Password_8.ImageUrl = "imageprocess.aspx?RandID=" & Arr_Random_PasswordandDecoy(Int.Counter)
      me.lbl_password_8.Text= Arr_Random_Ascii(Int.Counter)
Case 9
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_9.Text= Arr_Random_Ascii(Int_Counter)
Case 10
me.Img_Password_10.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_10.Text= Arr_Random_Ascii(Int_Counter)
Case 11
me.Img_Password_11.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_11.Text= Arr_Random_Ascii(Int_Counter)
Case 12
me.Img_Password_12.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_12.Text= Arr_Random_Ascii(Int_Counter)
Case 13
me.Img_Password_13.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_13.Text= Arr_Random_Ascii(Int_Counter)
Case 14
me.Img_Password_14.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_14.Text= Arr_Random_Ascii(Int_Counter)
Case 15
me.Img_Password_15.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_15.Text= Arr_Random_Ascii(Int_Counter)
Case 16
me.Img_Password_16.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_16.Text= Arr_Random_Ascii(Int_Counter)
Case 17
me.Img_Password_17.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_17.Text= Arr_Random_Ascii(Int_Counter)
Case 18
me.Img_Password_18.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_18.Text= Arr_Random_Ascii(Int_Counter)
Case 19
me.Img_Password_19.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_19.Text= Arr_Random_Ascii(Int_Counter)
Case 20
me.Img_Password_20.ImageUrl =
    "imageprocess.aspx?RandID=" &
    Arr_Random_PasswordAndDecoy(Int_Counter)
me.lbl_password_20.Text= Arr_Random_Ascii(Int_Counter)
Case 21
End Sub
End Class
Registration.aspx

<%@ Page Language="VB" AutoEventWireup="false"
CodeFile="Registration.aspx.vb" Inherits="Registration"
MasterPageFile="/~/MasterPage.master" %>

<asp:content ContentPlaceHolderID="ContentPlaceHolder1" runat=server />

<form id="form1" runat="server">

<table border=0 cellPadding=0 style="height:290px;border-collapse:collapse;align=center" class=Txt_Black_Normal cellSpacing=0>

<tr><% if request.QueryString("ID") <> "success" then %></tr>
<tr><td><table border=0 cellPadding=0 width=100% height=100% align=left style="border-collapse: collapse;" class=TXT_Black_Normal cellSpacing=0><tr style="height:10px"><td></td></tr><tr style="height:5px"><td style="font-size:14pt; color:#A41E28" colspan=2 align=left><b>Registration</b></td></tr><tr style="height:10px"><td></td></tr><tr><td colspan=2 style="text-align:justify; line-height:1.6">Welcome to registration section. We'll help you sign up on Graphical password new algorithm in easy steps! Just answer a few simple questions, select an username and your graphical password, and you'll be all set. Please be noted that your password should be at least 2 symbol.</td></tr></table></td></tr><tr style="height:20px"></tr><tr><td><table border=0 cellPadding=0 width=670><tr style="height:10px"></tr><tr><td align=left valign=center>Username:<asp:requiredfieldvalidator ID="Requiredfieldvalidator1" runat="server" ControlToValidate="Txt_Email" ErrorMessage="Please Enter Username"></td></tr><tr style="height:10px"></tr><tr><td align=left style="font-size:14pt" colspan=2 align=left>Username:</td></tr><tr style="height:10px"></tr><tr><td align=left valign=top>Password:&nbsp;&nbsp;&nbsp;</td></tr><tr style="height:10px"></tr><tr><td align=left><table id=tbl_password runat=server width=400 >
<tr><td align=left style="width:70px; height:70px; background-color:#26231e;"><asp:imagebutton ID="ImgBtn_Password_1" runat="server" ImageUrl="/~/images/images/1-0.jpg" /></td>
<td align=left style="width:70px; height:70px; background-color:#26231e;"><asp:imagebutton ID="ImgBtn_Password_2" runat="server" ImageUrl="/~/images/images/2-0.jpg" /></td>
</tr></table></td></tr>

</table></td></tr>

</form>
<table>
<thead>
<tr>
<th>ID</th>
<th>Width</th>
<th>Runat</th>
<th>ImageUrl</th>
<th>BorderColor</th>
<th>BorderStyle</th>
<th>BorderRadius</th>
</tr>
</thead>
<tbody>
<tr>
<td>ImgBtn_Password_11</td>
<td>50</td>
<td>server</td>
<td>~/images/images/11-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_12</td>
<td>50</td>
<td>server</td>
<td>~/images/images/12-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_13</td>
<td>50</td>
<td>server</td>
<td>~/images/images/13-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_14</td>
<td>50</td>
<td>server</td>
<td>~/images/images/14-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_15</td>
<td>50</td>
<td>server</td>
<td>~/images/images/15-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_16</td>
<td>50</td>
<td>server</td>
<td>~/images/images/16-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_17</td>
<td>50</td>
<td>server</td>
<td>~/images/images/17-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_18</td>
<td>50</td>
<td>server</td>
<td>~/images/images/18-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>ImgBtn_Password_19</td>
<td>50</td>
<td>server</td>
<td>~/images/images/19-0.jpg</td>
<td>Olive</td>
<td>None</td>
<td>2px</td>
</tr>
<tr>
<td>Last Name:</td>
<td>&lt;asp:textbox ID=&quot;Txt_lastname&quot; runat=&quot;server&quot; Width=&quot;270px&quot; MaxLength=&quot;100&quot;&gt;&lt;/asp:textbox&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Gender:    | <asp:radiobutton ID="RdBtn_gender_Male" runat="server" Checked Text="Male" />
<asp:radiobutton ID="RdBtn_gender_Female" runat="server" Text="Female" /> |
| Birthday:  | <asp:textbox ID="Txt_birthdate" runat="server" Width="270px"></asp:textbox> |
| Address:   | <asp:textbox ID="Txt_PostalCode" runat="server" Width="270px" MaxLength="200" TextMode="MultiLine"></asp:textbox> |
| Email:     | **Please Enter Email** |<asp:requiredfieldvalidator ID="EmailRequiredFieldValidator" runat="server" ControlToValidate="Txt_Email" ErrorMessage="Please Enter Email"/>
<asp:textbox ID="Txt_Email" runat="server" Width="270px" MaxLength="30"></asp:textbox> |
|           | &nbsp; |
Dear User,

Your registration is complete. This is the new method for graphical password authentication, proposed by UM University of Malaysia.

[Continue]
Registration.aspx.vb

'--------------------------------------------------------------------------------------------------------
'Project Name: Graphical User Authentication Algorisme (GUABRR)
'
'Author: Arash Habibi Lashkari
'
'Page Name: Registration.aspx
'
'Objective: Registering user information

'--------------------------------------------------------------------------------------------------------

Imports System.Data

Partial Class Registration
    Inherits System.Web.UI.Page
    Private Obj_ImageOriginal as New CLS_Image_Original
    Private Obj_user as New CLS_UserInfo
    Private Arr_ImagesID as integer() = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}
    Private count as Integer = 0
    Private ImgBtn_Sample as ImageButton
    Private Bln_Flag as Boolean
    Private Obj_Function as New CLS_Functions
    Private Str_Password as string
    Private Int_RandomNumber as integer()
    Private Int_counter as integer = 0

    Protected Sub Page_Load(ByVal sender As Object, ByVal e As System.EventArgs) Handles Me.Load
        '-----------------------------------------------------------------------------------------------
        'Objective: If the page load for the first time, create
        '25 random number for calling 25 random picture
        '
        'Input: All controls of the page
        '
        'Output: Set 25 images URL randomly
        '-----------------------------------------------------------------------------------------------

        if me.IsPostBack = False then
            Int_RandomNumber = obj_function.RandomNumberCreator (26)
            Do while bln_flag = False
                Set_ImagePassword_URL(page.Controls)
            Loop
            Session("Arr_Images_Random") = Arr_ImagesID
        end if

    End Sub

    Protected Sub Control_Reset()
        '-----------------------------------------------------------------------------------------------
        'Objective: Reseting Page
        '
        'Input: All text box of the page
        '
        '-----------------------------------------------------------------------------------------------

'Output: All Text box of the page which reset
---------------------------------------------
me.Txt_firstname.Text = ""
me.Txt_lastname.Text = ""
me.Txt_PostalCode.Text = ""
me.Txt_Username.Text = ""
me.Txt_Email.Text = ""
me.Txt_birthdate.Text = ""
me.Txt_Country.Text = ""
End Sub

Protected Sub ImgBtn_Submit_Click(ByVal sender As Object, ByVal e As System.Web.UI.ImageClickEventArgs) Handles ImgBtn_Submit.Click
','-------------------------------------

Objective: Submit Field to database

Input: All inputs of user

Output: One field in the database

Do while bln_flag = False
    Arr_ImagesID = Session("Arr_Images_Random")
    Password_Finder(page.Controls)
Loop
Obj_user.str_Password = Str_Password
Obj_user.str_Birthdate = me.Txt_birthdate.Text
obj_user.str_Email = me.Txt_Email.Text
Obj_user.str_Firstname = me.Txt_firstname.Text
if me.RdBtn_gender_Male.Checked = True
    Obj_user.str_Gender = "True"
else
    Obj_user.str_Gender = "False"
end if
Obj_user.str_Lastname = me.Txt_lastname.Text
Obj_user.str_Postalcode = me.Txt_PostalCode.Text
Obj_user.str_username = me.Txt_Username.Text

Obj_user.Insert_UserInfo()
response.Redirect ("Registration.aspx?ID=success")
End Sub

Private sub Password_Finder (Ctl_Parent as ControlCollection )
 ','-------------------------------------

Objective: Trace all pictures to find out which
Pictures are been clicked by the user (The ones
which have border is been clicked)

Input: All controls of hte page

Output: The string which contact all user password ID
 ','-------------------------------------

Dim Ctl_Child as control

For Each Ctl_Child In Ctl_Parent
    Password_Finder (Ctl_Child.Controls)
    If TypeOf Ctl_Child Is CheckBox and Ctl_Child.ID <> "RdBtn_gender_Male" and Ctl_Child.ID <> "RdBtn_gender_Female"
    Then
        if CType(Ctl_Child,CheckBox).Checked = True then
```

159
'As the border is double means the user click on it
'So we start fetch the picture ID from database
'And create string of password

'---------------------------------------------------
Dim ControlId as integer = Ctl_Child.ID.Substring(13, 
                     Ctl_Child.ID.Length - 13)
Str_Passwordd = Str_Passwordd + Arr_ImagesID(ControlId - 
                     1).ToString + "-"

End If
end if
if Ctl_Child.Controls.Count = 0 then Bln_Flag = true
Next
End Sub

Private sub Set_ImagePassword_URL (Ctl_Parent as 
ControlCollection )
'-----------------------------------------------------
'Objective: Set the image URL for 25 password image
'This is a recursive function to find the password
'image and then assign one random image from database
'to this picture

'Input: All controls of page

'Output: 25 images which their URL set from DB

'Need: One array of random numbers

'-----------------------------------------------------
Dim Ctl_Child as control
Dim str_Imagename as String
Dim Rst_ImagesOriginal as DataTable

For Each Ctl_Child In Ctl_Parent
  Set_ImagePassword_URL (Ctl_Child.Controls)
  '-----------------------
  'The Images password Find
  '-----------------------
  If TypeOf Ctl_Child Is ImageButton and (Ctl_Child.ID <> 
      "ImgBtn_Submit") and (Ctl_Child.ID <> "ImgBtn_Reset") Then
    '------------------------------------------
    'Find the picture from DB base on random ID
    '------------------------------------------
    Rst_ImagesOriginal = 
      Obj_ImageOriginal.Select_Image_ByRandID
        (Int_RandomNumber(Int_counter))
    str_Imagename = 
      Rst_ImagesOriginal.Rows(0)("IMG_ORG_UserName")
    Arr_ImagesID(Int_Counter) = 
      Rst_ImagesOriginal.Rows(0)("IMG_ORG_Rand")
    '---------------------
    'Set the URL of Image
    '---------------------
    CType(Ctl_Child,ImageButton).ImageUrl = "~/images/images/" + 
      str_Imagename
    Int_counter=Int_counter+1
  end if
if Ctl_Child.Controls.Count = 0 then Bln_Flag = true
Next
End Sub
Protected Sub ImgBtn_Reset_Click(ByVal sender As Object, ByVal e As System.Web.UI.ImageClickEventArgs) Handles ImgBtn_Reset.Click
    Control_Reset()
End Sub
End Class
Public Class CLS_UserInfo
    Private Int_Internal_ID As Integer
    Private str_Internal_username As String
    Private str_Internal_Password As String
    Private str_Internal_Firstname As String
    Private str_Internal_Lastname As String
    Private str_Internal_Gender As String
    Private str_Internal_Birthdate As String
    Private str_Internal_Country As String
    Private str_Internal_Postalcode As String
    Private str_Internal_Email As String

    Private StrSql as String
    Private objDLayer As New CLS_Dalayer

    Public Sub New()
    End Sub

    Public Property Int_ID()
        Get
            Return Int_Internal_ID
        End Get
        Set(ByVal value)
            Int_Internal_ID = value
        End Set
    End Property

    Public Property str_username()
        Get
            Return str_Internal_username
        End Get
        Set(ByVal value)
            str_Internal_username = value
        End Set
    End Property

    Public Property str_Password()
        Get
            Return str_Internal_Password
        End Get
        Set(ByVal value)
            str_Internal_Password = value
        End Set
    End Property
Public Property str_Firstname()
    Get
        Return str_Internal_Firstname
    End Get
    Set(ByVal value)
        str_Internal_Firstname = value
    End Set
End Property

Public Property str_Lastname()
    Get
        Return str_Internal_Lastname
    End Get
    Set(ByVal value)
        str_Internal_Lastname = value
    End Set
End Property

Public Property str_Gender()
    Get
        Return str_Internal_Gender
    End Get
    Set(ByVal value)
        str_Internal_Gender = value
    End Set
End Property

Public Property str_Birthdate()
    Get
        Return str_Internal_Birthdate
    End Get
    Set(ByVal value)
        str_Internal_Birthdate = value
    End Set
End Property

Public Property str_Postalcode()
    Get
        Return str_Internal_Postalcode
    End Get
    Set(ByVal value)
        str_Internal_Postalcode = value
    End Set
End Property

Public Property str_Email()
    Get
        Return str_Internal_Email
    End Get
    Set(ByVal value)
        str_Internal_Email = value
    End Set
End Property

Public Sub Insert_UserInfo ()
'-----------------------------------------------------
'Insert the user specification
'-----------------------------------------------------
StrSql = "insert into
    UsersInfo(UINFO_Username,UINFO_Password,UINFO_Firstname,UINFO_L
Public sub Select_User_ByUsername(ByVal Str_UserID As string)
'----------------------------------------
'Select the user by giving its username
'----------------------------------------
Dim Rst_User as datatable

StrSql = "select * from UsersInfo where UINFO_Username = " & Str_UserID & ""
Rst_User = objDLayer.RetrieveQuery(StrSql)

if Rst_User.Rows.Count > 0 then
    Me.Int_ID = Rst_User.Rows(0)("UINFO_ID")
    Me.str_username = Rst_User.Rows(0)("UINFO_Username")
    Me.str_Password = Rst_User.Rows(0)("UINFO_Password")
    Me.str_Firstname = Rst_User.Rows(0)("UINFO_Firstname")
    Me.str_Lastname = Rst_User.Rows(0)("UINFO_Lastname")
    Me.str_Gender = Rst_User.Rows(0)("UINFO_Gender")
    Me.str_Birthdate = Rst_User.Rows(0)("UINFO_BirthDate")
    Me.str_Postalcode = Rst_User.Rows(0)("UINFO_PostalCode")
    Me.str_Email = Rst_User.Rows(0)("UINFO_Email")
else
    Me.str_username = ""
end if

End sub

Public function Select_User_ByUserID(ByVal Str_UserID As string)
'----------------------------------------
'Select the user by giving its userID
'----------------------------------------

StrSql = "select * from UsersInfo where UINFO_ID = " & Str_UserID & ""
Select_User_ByUserID = objDLayer.RetrieveQuery(StrSql)

End function
End Class
CLS_Image_Rotation.vb

---
Project Name: Graphical User Authentication Algorisme

Author: Arash Habibi Lashkari

Class: CLS_Image_Rotation

Objective: All functions related to Rotated images
---

Imports Microsoft.VisualBasic

Public Class CLS_Image_Rotation
    Private strSql as String
    Private objDLayer As New CLS_Dalayer

    Public Function Select_ImageRotation_ByOriginalID_And_Rotation(ByVal Int_RandID As Integer, Int_Rotation as Integer)
        <![CDATA[
        StrSql = "SELECT *, Images_Rotation.*, Images_Original.* " 
            & "FROM Images_Original INNER JOIN " 
            & "Images_Rotation ON Images_Original.IMG_ORG_ID = Images_Rotation.IMG_ROT_OriginalID " 
            & "WHERE (IMG_ORG_Rand = " & Int_RandID  
            & ") AND " 
            & "(IMG_ROT_RotateDegree = " & Int_Rotation & 
            ")"
        Select_ImageRotation_ByOriginalID_And_Rotation = objDLayer.RetrieveQuery(StrSql)
        End Function
    End Class
]]>
Imports Microsoft.VisualBasic

Public Class CLS_Image_Original

    Private Int_Internal_ID As Integer
    Private str_Internal_ImageName As String
    Private StrSql As String
    Private objDLayer As New CLS_Dalayer

    Public Sub New()
    End Sub

    Public Property Int_ID()
        Get
            Return Int_Internal_ID
        End Get
        Set(ByVal value)
            Int_Internal_ID = value
        End Set
    End Property

    Public Property str_ImageName()
        Get
            Return str_Internal_ImageName
        End Get
        Set(ByVal value)
            str_Internal_ImageName = value
        End Set
    End Property

    Public Function Select_Image_ByRandID(ByVal Int_ID As Integer) As String
        StrSql = "select * from Images_Original where IMG_ORG_Rand = " & Int_ID
        Select_Image_ByRandID = objDLayer.RetrieveQuery(StrSql)
    End Function

    Public Function Select_Image_ByImagename(ByVal Str_Imagename As String) As String
        'Find original image by its imagename
        Select_Image_ByImagename = objDLayer.RetrieveQuery("select * from Images_Original where IMG_ORG_Imagename = "." & Str_Imagename
    End Function

End Class
StrSql = "select * from Images_Original where IMG_ORG_ImageName = '' & Str_Imagename & ''"
Select_Image_ByImagename = objDLayer.RetrieveQuery(StrSql)
End Function

End Class