Graphical Passwords Authentication System Resistant To Shoulder Surfing Attacks

By

Amna Jamal Abdulsalam Abraheem

Supervisor

Dr. kenz A. Bozed

This Thesis was submitted in Partial Fulfillment of the Requirements for Master's Degree of Computer Science

University of Benghazi

Faculty of Information Technology

March 2022

University of Benghazi

Faculty of Information Technology

Department of Computer Science

(Graphical Password Authentication System Resistant to Shoulder Surfing Attacks)

By

Amna Jamal Abdulsalam Abraheem

This Thesis was Successfully Defended and Approved on **17/ 3 /2022**

Supervisor

Dr. Kenz A.Bozed

……………………….……………………………..

Dr. Tarig Ali Elshheibia (**Internal examiner**)

Signature: ..…………………….…………………………..

Dr. Mussa Ahmed Mohammed (**External examiner**)

Signature: ………………………………..………………….

(Dean of Faculty) **(Director of Graduate studies and training)**

Dedication

I dedicated this dissertation to my beloved parents

My brothers and sisters

With thanks for all the years of love, caring, encouragement and endless support

Amna J. Al-Ojeli

Acknowledgments

First and foremost, I thank God who has inspired and blessed me to accomplish this research despite all the obstacles and delays I went through.

I extend many, many thanks to all the individuals who have contributed to the successful completion of my dissertation. My advisor, Dr. kenz A. Bozed, deserves my gratitude for giving me support and faithfulness in all guidance.

Thank you to my dad, **Jamal Al Ojeli**, and mom, **Naima bin Ghazi**, for their unwavering love, encouragement, and support.

Dad, the ways you have supported me are endless, you never fail to help me keep things in perspective.

Mom, I am grateful for the countless hours you spent teaching me belief that I would get this research done and how you have always been a true supporter of me.

Special thanks for Dr. Wafa El-Tarhouni who gave me all the necessary support needed for success from the start of my Masters Study journey. May God reward you all the relentless efforts to see through this academic pursuit.

I wish thank my all colleagues specially Amina Abdo, and others for their support and encouragement.

I also wish to express my sincere appreciation for my sisters and brothers who always encourage and give me full support to doing this work.

Last but not least, I would like to extend my thanks to the administration of the College of Information Technology - Ajdabiya University, especially Dr. Muhammad Buhalfaya and Mister Suleiman Kunduz, I am grateful to them for the support I received throughout my study and when I was work on this research.

Publications

ICEEIT2021 Paper: (Published)

Amna J. AL-Ojeli., Kenz A. Bozed., and Wafa I. Eltarhouni "Develop Graphical Passwords Authentication System Resistant To Shoulder Surfing Attacks". In International Conference on Electrical Engineering and Information Technology (ICEEIT2021). November 2021, Benghazi-Libya.

TABLE OF CONTENTS

Contents **Page No.**

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

Abbreviation	Meaning
PIN	**P**ersonal **I**D **N**umber
KBA	**K**nowledge **B**ased **A**uthentication
PDA	**P**ersonal **D**igital **A**ssistant
DAS	**D**raw **a** **S**ecret
QDAS	**Q**ualitative **D**raw **a** **S**ecret
CCP	**C**ued **C**lick **P**oint
PCCP	**P**ersuasive **C**ued **C**lick **P**oint
S3PAS	**S**calable **S**houlder **S**urfing Resistant Textual-Graphical **P**assword **A**uthentication **S**cheme
CAPTCHA	**C**ompleted **A**utomated **P**ublic training **T**uring tests to tell **C**omputer and **H**umans **A**part
SDLC	**S**ystems **D**evelopment **L**ife **C**ycle
GUI	**G**raphical **U**ser **I**nterface
ISO	**I**nternational **S**tandards **O**rganization

LIST OF APPENDIXES

Appendix **Page no.**

Graphical Passwords Authentication System Resistant To Shoulder Surfing Attacks

By

Amna Jamal Abdulsalam Ibrahim

Supervisor

Dr. kenz A. Bozed

Abstract

Passwords are widely used for authentication in information systems, and it is still the dominant method of authentication despite its weaknesses due to its simplicity. However, users have difficulty remembering long passwords that are restricted with high security policies. Thus, they make short password, which makes it insecure and vulnerable to hacking. To solve this problem the graphical password techniques was proposed, which is a technique based on the use of images and patterns instead of text. However, this technique has deficiencies and requires further research. As with current schemes of this technique, when increasing the ease of use, it will reducing the security defenses vice versa. The main goal of this research is combining usability features with providing secure defense mechanisms, without compromising the ease of use and memorization. Where this research focuses on verifying graphical password schemes and summarizing the most important solutions that can be offered in the field of graphical password techniques. To make sure that the main objective of the research is achieved, a new system has been built based on the comparison between graphical password technique and text password technique. The proposed system was also tested with a sample of users and the usability features offered were evaluated, with positive results. Most of the users preferred the graphical password over the text password in terms of ease of use and remembering. The security of the proposed system was also evaluated, and the results showed that the system provides a defense mechanism against common attacks exposed by graphical password techniques.

CHAPTER 1

INTRODUCTION

1.1 Overview

This chapter provides an introduction to text and graphical passwords techniques and clarifying major problems facing both techniques. Methodology followed in this study to reach required results has also been clarified. The scope of the study has been defined to provide a comprehensible vision of what this work is going to provide.

1.2 Background

Security is an important component of most computer systems, especially those, which are used over the internet. Universal access to information makes security a critical design issue in these systems and with the development of technology, more resources (i.e. information and services) are becoming available online.

In addition, with the increasing number of people using the World Wide Web for commercial, entertainment or personal purposes, the need for accurate and confidential information to be easily passed between parties is also increasing. Moreover, users often keep their communications, financial data, business documents and personal media safe by means of some software that provides information protection. Therefore, as reported by *Jali* (2011) and *Tiller* (2020), the need to control and protect users to access a particular resource is a critical issue.

Bianchi et al. (2016) reported that one of many steps to achieving this protection is known as authentication and authorization. Authentication is a central area in security research, where *Menezes et al.* (1996) defined the authentication as: "*it is the act of verifying that a user is who they claim to be, and it is a key topic in computer security*". While *Ariffin et al.* (2021) define the authentication as the process of determining whether a user should be allowed access to a particular system or resource.

Nowadays, the text passwords are the most popular authentication method for access control to protect computer systems, mobile phones, ATMs, etc. User may need passwords for many purposes such as computer login, accounts, e-mail, access to files, databases, networks and websites. *Dhiviyaa* et al. (2018) support this viewpoint when they stated that providing a person's identity to gain legitimate access to a service is increasingly necessary to prevent unauthorized users from stealing information, misusing the service, stealing identities, or damaging reputation.

Traditional text passwords are widely used for authentication, although other methods are available today, including biometrics and smart cards; however, these alternative techniques have some problems. Biometrics are raise privacy concerns and smart cards usually need a PIN because the cards can be lost. As a result, passwords are still prevalent and are expected to remain so for some time as an authentication process. However, text passwords also have drawbacks as mentioned by *Tiller* (2020) from a usability point of view, and these usability issues tend to translate directly into security issues.

For example, *Mali and Rattanafil* (2017) have presented that the user usually chooses a simple password that can be easily remembered. Therefore, it would be easy to guess and could also be an easy target to hack attacks and brute force. On the other hand, enforcing a strong password policy might have the opposite effect as well, because user can resort to typing hard-to-remember passwords on sticky notes, exposing them to outright theft. While the purpose of authentication is to provide security, usability cannot be ignored. However, if the system is not easy to use, users will avoid using it. Hence, it will lead to system failure.

To address these problems, many researches were conducted in the field of system security to develop new and more secure authentication methods. A new technique based on using images instead of text as a password was introduced, as the new technique tried to improve security and avoid the weakness of the traditional text password. This authentication method is named "Graphical Password".

Snodgrass et al. (1972) proposed psychological studies, which support the fact that humans can remember images better than text, which is cited in *Patra et al.* (2016), "*pictures are generally easier to be remembered or recognized than text*".

The first idea for graphical passwords was described by *Blonder* (1996), in which this method was to allow the user to click with a mouse or stylus, on a few selected areas in an image. If the correct areas are clicked, the user will be authenticated; otherwise, the user will be rejected. Subsequently, several researchers conducted search graphical passwords over time. According to *Jali* (2011), the graphical password is likely to be easier to remember and more secure compared to the text password because it takes advantage of humans' ability to better save and retrieve recalling images.

Graphical passwords are considered more secure and resistant to traditional attacks such as brute force and dictionary attacks as reported by *Sananse and Karwande* (2020). However, as cited by *Ologundudu and Sakpere* (2021) graphical passwords technique is a promising domain and requires more scientific researches and the use of case studies.

1.3 Problem Statement

Although some authentication methods such as biometrics and smart cards have proven effective, text passwords are still the most popular method of authentication as *Heera et al.* (2020) stated. This is because passwords have a number of useful properties that contribute to their persistence. Text passwords are easy to implement, do not involve any additional hardware and no additional cost is required. For the user, it is portable and convenient, as well as familiar and easy to understand.

However, *Abhijith et al.* (2021) discussed that text passwords are a major usability challenge for users, who are required to create secure and unique passwords for each account, remember each of these passwords for a long time, and remember which password corresponds to any account for multiple accounts. These security requirements impose requirements beyond human capabilities on users' memory and attention. In addition, it lead users to create passwords, which are easy to remember, at the same time, it might be easy for attackers to guess. However, *Fatima* (2020) reported that users tend to use the same password for all or most of their accounts to make it easier to remember. This makes their accounts vulnerable to hacking; therefore, if the attacker hacks the users' password, he/she might hack the accounts of all the users and access any information might be important and private.

Accordingly, the above-mentioned problem has led to innovation of the graphical password techniques. Where the graphical password authentication system should motivate the users to form strong and easy to remember passwords. Although graphical password is easier to remember to the users, as cited by *Ariffin et al*. (2021), most of its schemes are vulnerable to shoulder surfing attacks due to the lack of anti-shoulder surf mechanism. However, there are some graphical password schemes which attempt to offer anti-shoulder surfing mechanism such as the Triangle Scheme. However, these schemes are time consuming and inconvenient as the user will need to locate his\ her Pass-Object among many other objects.

Therefore, the essence of this research is to introduce and achieve a new scheme in the field of graphical password techniques, which will overcome authentication security issues.

1.4 Research Motivation

Some modern security systems use graphical password authentication methods in order to provide greater ease of use while providing the required security. This is because it has gained great popularity in the last decade such as the graphical pattern of unlocking the mobile phone screen, which is considered as a "doodle scroll scheme".

However, these methods still have some shortcomings, such as the aforementioned Pass-doodle scheme, which is a hand-drawn design usually drawn with a stylus on a touch-sensitive screen, although it is easy to use and remember , however, it is vulnerable to shoulder surfing attacks.

Therefore, the impetus for this research is to develop a new hybrid graphical password scheme based on the concepts of the two graphical password techniques. The main objective of this proposed scheme is to combine the features of high security, ease of use, and memorability. Moreover, a new graphical authentication system has been proposed as its features are based on analyzing various existing graphical password schemes and then using the best of these features.

The proposed graphical password scheme is intended to be more secure compared to previous systems, as it focuses on providing an anti- shoulder- surfing mechanism, which is one of the most common attacks against graphical password technique.

1.5 Research Aim and Objectives

The main aim of this study is to extend previous work in graphical password techniques and propose a new hybrid scheme that resists shoulder surfing attack, which is mainly based on recognition-based and cued recall-based techniques in order to increase the level of security.

The aims are supported by the following objectives:

1. To provide an updated survey of various graphical password schemes, in order to understand the mechanism of graphical authentication methods.
2. To develop security improvements to graphical password techniques based on the use of the advantages of previous research.
3. To create a new scheme and then evaluate its suitability as an alternative method of user authentication.
4. To evaluate the effectiveness of the proposed scheme by designing a reliable system, to ensure that it provides the optimum level of security and ease of use

1.6 Research Methodology

The research methodology has the following steps :

1. Investigating current graphical password schemes by studying research papers, journals, articles and websites. In addition, summarizing the authentication problems related to graphical password techniques in order to understand the concept of the process; and to identify the problem's background, objectives, and scope of the study.
2. Taking advantage of the existing graphical password schemes and combine their advantages to produce the proposed scheme (Image Grid Scheme) with the addition of improvements.
3. Designing graphical authentication system based on the proposed scheme.
4. Implementation of the proposed system of Visual Studio 2013 as a programming environment and Visual Basic as a programming language.
5. Evaluation of the proposed system based on security and usability metrics, where usability metrics were measured by conducting an experiment on a sample of users.
6. Analyzing and discussing the obtained results and comparing the proposed work with the previous research.

1.7 Scope and Limitations of the Study

The most common attack on graphical password technique is a shoulder surfing attack. Thus, the scope of this research is to provide a good defense mechanism against shoulder surfing attacks.

It is known that each study has its own limitations, which reflect the extent of accuracy and adherence to the study methodology in general. Therefore, the limits of this study are as follows:

1. The proposed scheme was applied on offline system.
2. The proposed system is designed and implemented by Visual Basic, that is, the system works only on computers and does not support mobile devices.
3. The questionnaire was mainly relied on with direct observation as tools for collecting results. Therefore, the results obtained from the questionnaire is a potential limitation since it is not possible to know whether the questionnaire is completely filled with honest answers.
4. The sample was limited to university places, as all sample members are educated and most of them have computer knowledge.

1.8 Significance of the Study

The main significance is to providing a balance between usability and security in this context, which is an open problem, given the tendency to design defenses that force users to perform complex password to be more secure which is complicated and hard to be remembered.

Thus, the significance of this study is to generate new insights into graphical password authentication methods by proposing a new scheme that makes passwords more secure and easy to use.

Moreover, while the proposed scheme focused on increasing the level of security, the proposed scheme was applied by implementing a system that provides a mechanism against guess and shoulder attacks.

1.9 Research Questions

- Are graphical passwords as secure as text passwords?
- How does a graphical password system measured?
- How far is the user's acceptance of the new technology?

1.10 Thesis Organization

This chapter provided an overview of the text and graphical password techniques, problem statement, research methodology and objective of the work, which led to the development and implementation of a new graphical password scheme and system. The following is the organization of the rest chapters:

- Chapter 2: Provides a literature review of graphical password schemes, discusses some previous work of graphical password techniques, and identifies the shortcomings of each scheme. In addition, it discusses common attacks against graphical password schemes.
- Chapter 3: Discuss and suggest a hybrid graphical password scheme in details, which is named Image Grid scheme. In addition, it provides a simplified description of the proposed system design.
- Chapter 4: Explains the process of implementing the proposed system. It also shows how the system works in the registration phase and the login phase by displaying some graphical user interfaces of the system.
- Chapter 5: Illustrates the experiment that was conducted, the results obtained from the experiment by using percentage diagrams, and it shows the evaluation of these results in terms of their usability and resistance to attacks.
- Chapter 6: Discusses the results presented in the previous chapter and compares them with previous schemes, presents the conclusion and some of forthcoming works.

Chapter 2

Literature Review

2.1 Overview

This chapter is to investigate and provide a survey of using and understanding the mechanism of the authentication methods, graphical password techniques and schemes including advantages and disadvantages.

2.2 Authentication Methods

Authentication as defined by *Ariffin et al* (2021) is the process of determining whether a user should be allowed access to a particular system or resource. While authentication is defined in computer security, it is the process of attempting to verify the digital identity of a communication sender such as a login request. In web authentication, "authentication" is defined as a method of ensuring that the user trying to perform functions in the system is in fact the authorized user.

As cited in *Mali and Rathanavel* (2017) the authentication method is divided into three main areas:

1. The authentication based on something the user knows (e.g., passwords, PINs), which known Knowledge-Based Authentication [KBA].
2. Something the user has (e.g., smartcards, password-generation tokens), which known Token-Based Authentication [TBA].
3. Something the user is (either physical or behavioral biometrics, e.g., fingerprints, retinal scans, typing patterns), which known Biometric Based Authentication [BBA].

Users are often not interested in following strict security guidelines when using KBA's authentication methods. Accordingly, this puts the system developer and users in a common evolutionary conflict, in which the security and usability of the authentication system are paradoxically increasing.

Although biometrics and token-based authentication promise high security for systems, biometrics have privacy concerns and usually require extra hardware and can be relatively expensive. Smart cards and authentication tokens are also very expensive, and they require that the user remember to hold the token around.

Graphical password authentication technique is a type of knowledge-based authentication. Where graphical passwords consist of images and visual representation, which attempt to solve the traditional password problems while preserving the properties of passwords, but do not follow the traditional text format. *Biddle et al.* (2012) defined the graphical password technique: "*it is knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity, with the shared secret being related to or composed of images or sketches*".

Blonder's first graphical password was patented in 1996 and a variety of schemes soon followed. Lots of research has been done on the graphical passwords area, and it is starting to get limited publication, particularly in Android unlock pattern and Windows 8 picture password.

The graphical passwords are based on the psychological discovery that humans are able to remember images better than text. Therefore, it was developed in response to the textual password problems, with the hope that image-based passwords could be both memorable and secure.

Recently, many computer systems, networks and the internet-based environment are attempting to use graphical authentication technique. Thus, as *Vorster et al.* (2016) and *Abhijith et al.* (2021) mentioned the foundation of an authentication system is to encourage users to choose better password, which consequently increases security and usability.

This study was utilized the knowledge-based authentication because it does not required any additional hardware, and it is easy to learn and use by the simple user.

2.3 Graphical Password Techniques and Schemes

Graphical password techniques are supported to be more secure and resilient against various attacks than text passwords. However, they are still vulnerable to some threats as cited by *Tahmina* et al. (2020). Where graphical password techniques can be further divided into three categories: recognition-based techniques, recall-based graphical techniques and hybrid techniques as shown at Figure 2.1.

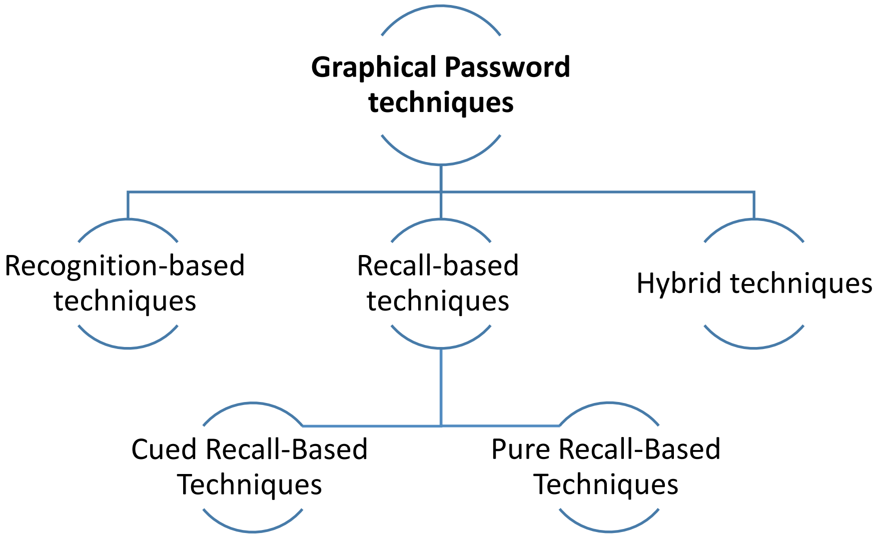

Graphical Password techniques
Recognition-based techniques
Recall-based techniques
Hybrid techniques
Cued Recall-Based Techniques
Pure Recall-Based Techniques

Fig. 2.1: Graphical password techniques.

2.3.1 Recognition-based Technique

In recognition technique, a set of images or figures is presented to the user during the registration phase, and the user passes authentication by recognizing and selecting his choices during the login phase. Where the user has to select a pre-selected image, icon or logo during the registration phase from a large selection of distraction images. There are several types of charts such as:

1. D'ej'a Vu scheme.
2. Pass-face scheme.
3. Triangle scheme.
4. Pass-objects scheme.
5. Thumbnail images scheme.
6. Theme scheme.
7. Story scheme.
8. Pass-Image scheme.

2.3.1.1 D'ej'a Vu Scheme

Dhamija and Perrig in 2000 proposed a new scheme known as D'ej'a Vu scheme. In their program, as shown in Figure 2.2, the user is asked to select certain number of images from a set of random images generated by the program. Later, user is required to identify the preselected images to be authorized user. The results that *Stobert* (2015) was presented in his study showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS.

The drawbacks with their program are that the server needs to store a large amount of images, which might have to be transferred over the network and delays the authentication process, which can be tedious and time consuming for the user. Moreover, the number of images to be stored in the database is too large, which slows down the authentication process and makes the program tedious and time-consuming from the user's point of view.

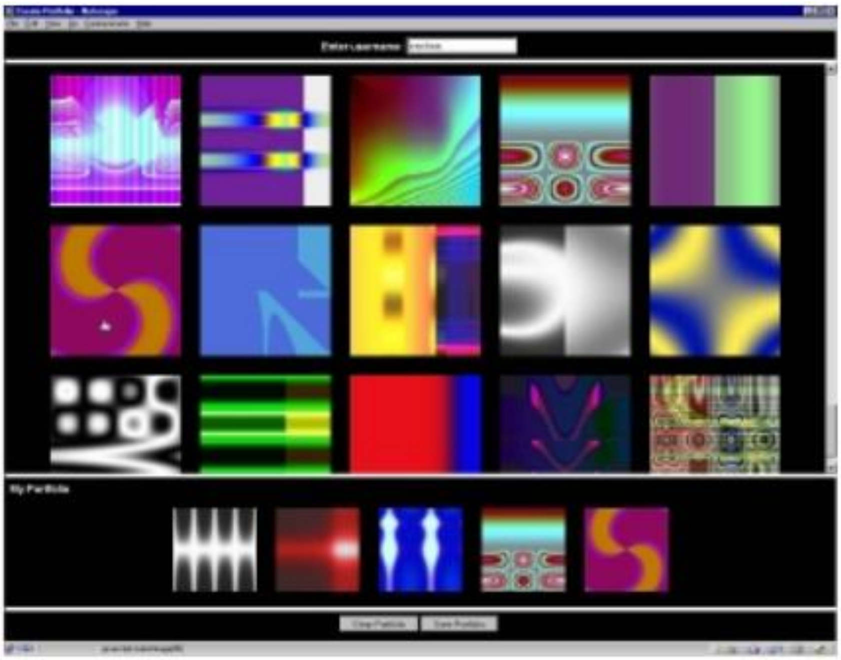


Fig. 2.2: D'ej'a Vu program.

Akula and Devisetty (2004) proposed an algorithm similar to the previous technique. The difference is that by using hash function SHA-1, which produces 20-byte output, the authentication is secure and require less memory. However, the image file still occupies more space than text even after hashing.

2.3.1.2 Pass-face Scheme

As cited by *Tahmina et al.* (2020) Pass-Faces scheme was proposed in 2000, which is an alternative scheme was developed by Real User Corporation and based on using facial images as shown in Figure 2.3.

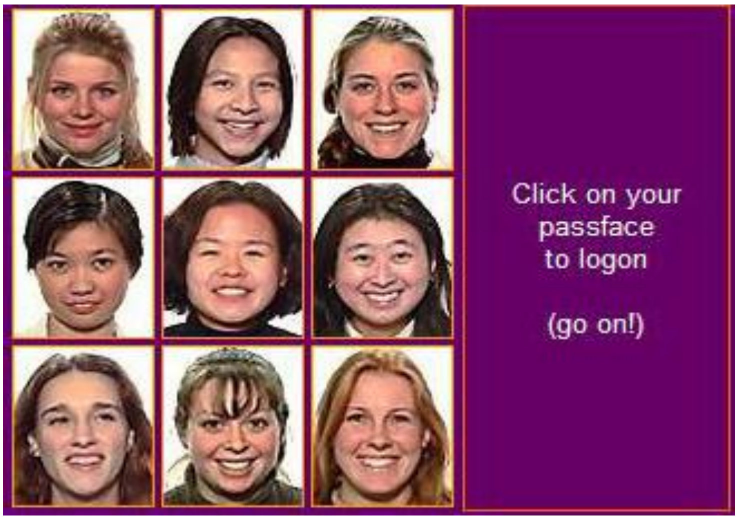


Fig. 2.3: Pass-Faces scheme.

In this scheme, the user registers by selecting a number of faces from a large database of faces. During authentication one of the registration images are shown together with eight other faces in a 3x3 grid. The user should go through a number of rounds and select the correct face from the nine options during each round.

However, the effectiveness of this method is still uncertain until *Davis et al.* (2004) studied the graphical passwords that using the Pass-faces scheme and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Pass-faces password somewhat predictable.

2.3.1.3 Triangle Scheme

As mentioned by *Xiaoyuan* (2006), the Triangle Scheme was developed by *Sobrado* and *Birget* in 2002. The triangle is a graphical password scheme that deals with shoulder-surfing problem. At registration phase, user is asked to choose a certain number of pass objects from 1000 proposed objects as shown in Figure 2.4. To authenticate, the system displays a variety of objects on the screen and the user is asked to click inside the area that the previously selected objects form. The action repeats for several times but every time the icons on the screen will shuffle and appear in different place.

The main drawback of this scheme is that the screen is very crowded which confuses the user when distinguishing objects on the screen. In addition, the average registration and login time is much longer than in a traditional text-based system. On the other hand, if fewer elements are used to reduce congestion, it will reduce the password space and become more vulnerable to hacking.

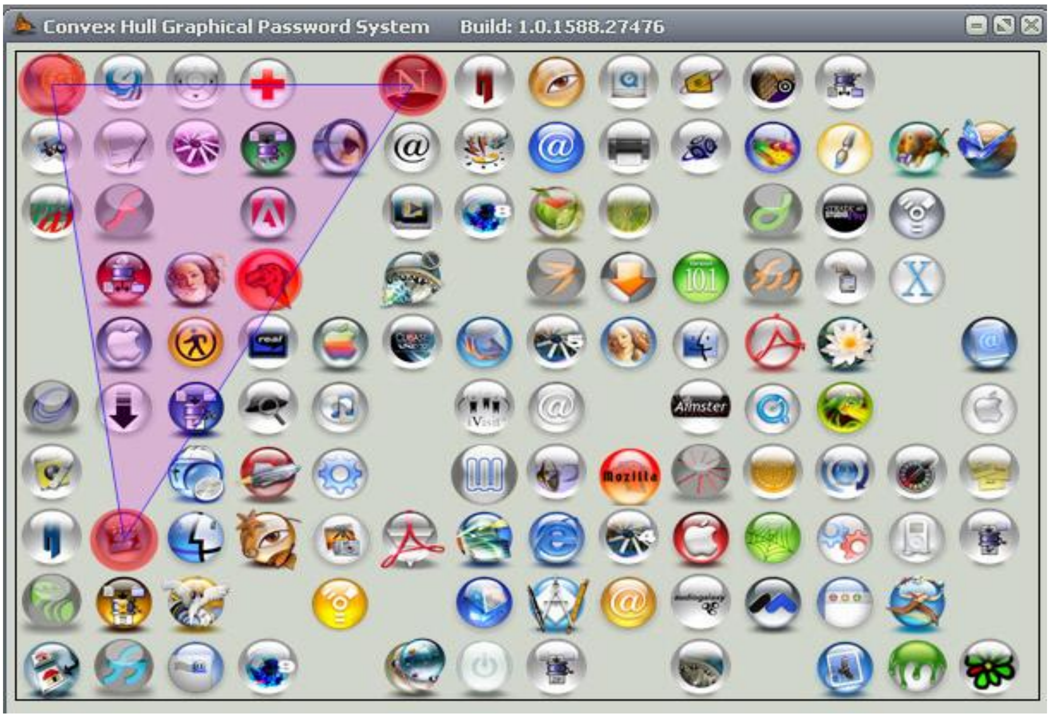


Fig. 2.4: Triangle scheme.

The authors attempted to improve their scheme as second algorithm in 2005, in which the user moves a frame (and the objects within it) until the pass-object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process several times to reduce the likelihood of logging in by clicking or rotating randomly. It did not solve the main drawback in the previous algorithm, as the login process was slow.

2.3.1.4 Pass-objects Scheme

Man et al. (2003) proposed shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of images as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects.

However, this method still requires users to memorize the alphanumeric code for each pass-object variant. For example, if there are four pictures each with four variants, then each user has to memorize 16 codes. Although the pass-objects provide some cues for recalling the codes, it is still quite inconvenient. Figure 2.5 shows the login screen of this graphical password scheme.

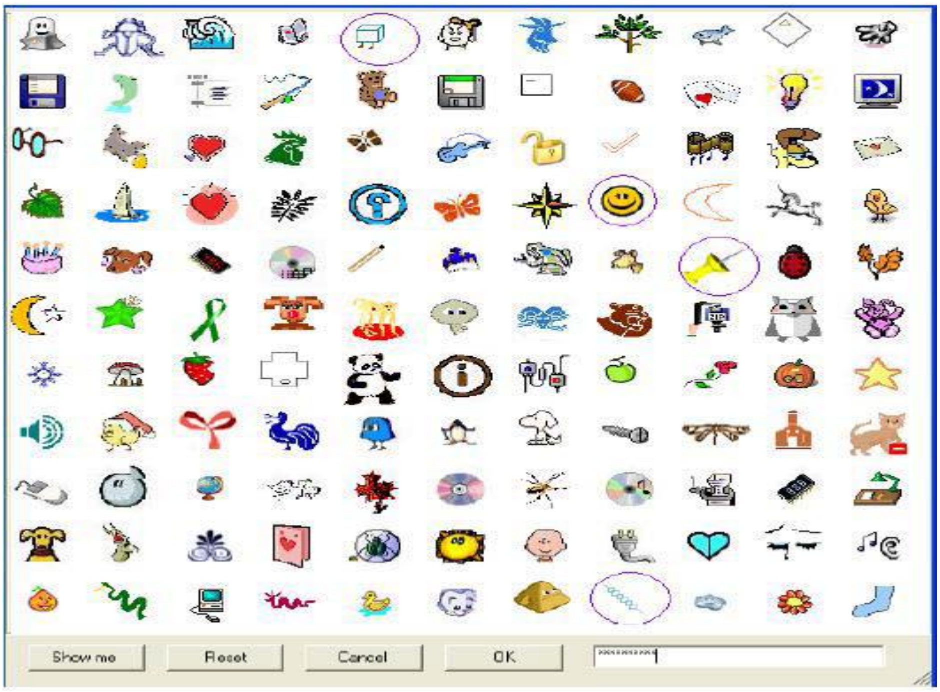


Fig. 2.5: Pass-objects scheme.

2.3.1.5 Thumbnail images Scheme

Wayne et al. (2003) developed graphical password scheme, which is designed especially for handheld device like Personal Digital Assistant (PDA). As it is shown in Figure 2.6, during registration, the user selects sequence of thumbnail images to be registrant. When the PDA is turn on, the user has to enter the registered image sequence for verification to gain access to the device. After a successful authentication, the user may change the password and selecting a new sequence or theme.

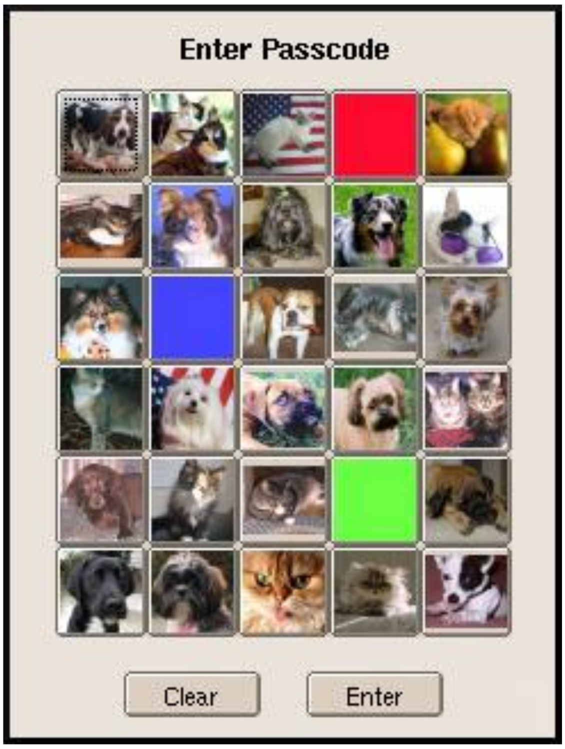


Fig. 2.6: Thumbnail images scheme.

Since the numbers of thumbnail images are limited to only 30, the size of the password space is considered small. Therefore, to ensure that the password space is comparable to text password, the designer added second method of selecting thumbnail element. Besides selecting individual thumbnail elements as before, one could select two thumbnail elements together to compose a new alphabetic element. This was done by using a shift key to select uppercase or special characters on a traditional keyboard. The drawback of this scheme is that the addition of shift key causes the algorithm complex and difficult.

2.3.1.6 Theme Scheme

Jansen et al. (2004) proposed a graphical password mechanism for mobile devices. During registration stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail images and then registers a sequence of images as a password, as shown in Figure 2.7.

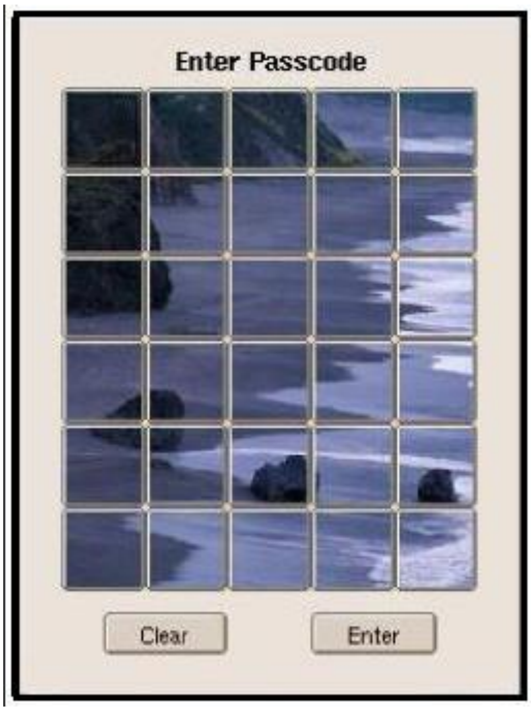


Fig. 2.7: Theme scheme.

During the authentication, the user has to enter the registered images in the correct sequence. After a successful authentication, the user may change the password, selecting a new sequence, or possibly change the theme.

Suo and Owen (2005) cited the disadvantage of this scheme is that while the amount of thumbnail image is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will essentially generate a numerical password. The result showed that the image sequence length was generally shorter than the length of textural password.

2.3.1.7 Story Scheme

As mentioned by *Christopher and Noordean* (2017), *Davis et al*. in 2004 was proposed story scheme by categorizing the available images to nine categories, which are animals, cars, women, food, children, men, objects, nature and sport. According to Figure 2.8, the users have to select their passwords from the mixed images of nine categories in order to make a story easily to remember.

Their studies showed there were some users who used this method without defining a story for themselves and these studies showed that the story scheme was harder to remember in compare to text passwords.

Fig. 2.8: Story scheme.

2.3.1.8 Pass-Image scheme

Takada and Koike (2003) discussed a graphical password technique for mobile devices. This technique allows users to use their favorite images for authentication. The users first register their favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification as shown at Figure 2.9. In each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful.

This method does not more secure authentication method than text-based password. As reported in studies by the *Davis et al.* (2004) users' choices of image passwords are often predictable. Allowing users to register their own images makes it easier for user to remember their pass-images, nevertheless make the password even more predictable, especially if the attacker is familiar with the user.

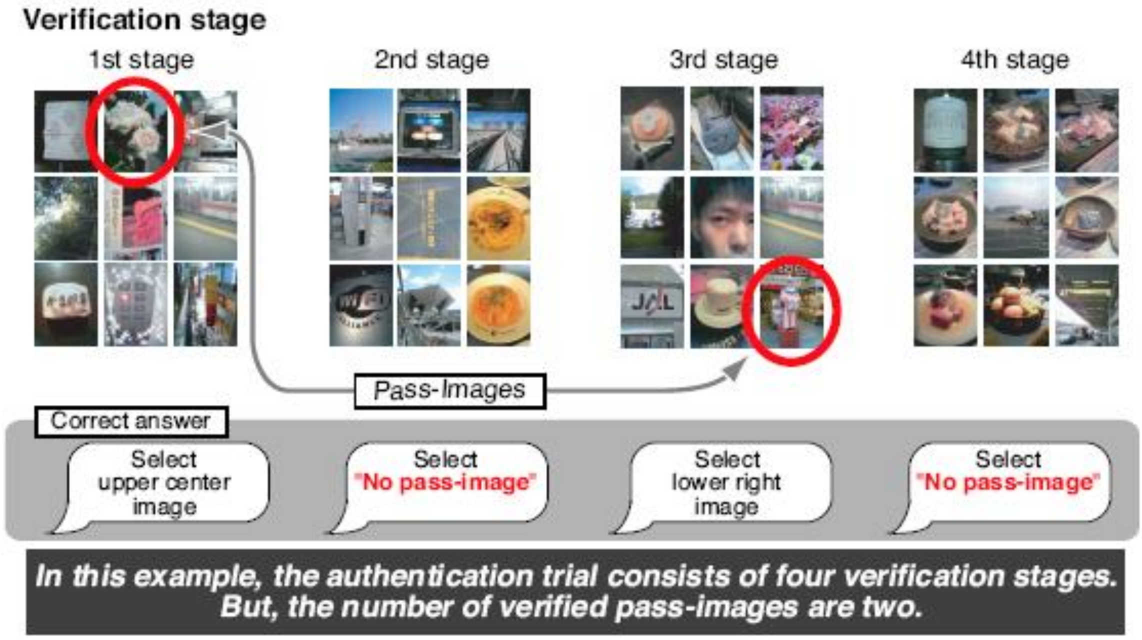

Verification stage
1st stage
2nd stage
3rd stage
4th stage
Pass-Images
Correct answer
Select upper center image
Select "No pass-image"
Select lower right image
Select "No pass-image"
In this example, the authentication trial consists of four verification stages. But, the number of verified pass-images are two.

Fig. 2.9: Pass-Image scheme.

2.3.2 Recall-based Techniques

In recall-based techniques, user is asked to reproduce something that he or she created or selected earlier during the registration stage as mentioned by *Ologundudu and Sakpere* (2021). In this section, two types of recall-based password techniques discusses:

1. Pure Recall-Based Technique.
2. Cued Recall-Based Technique.

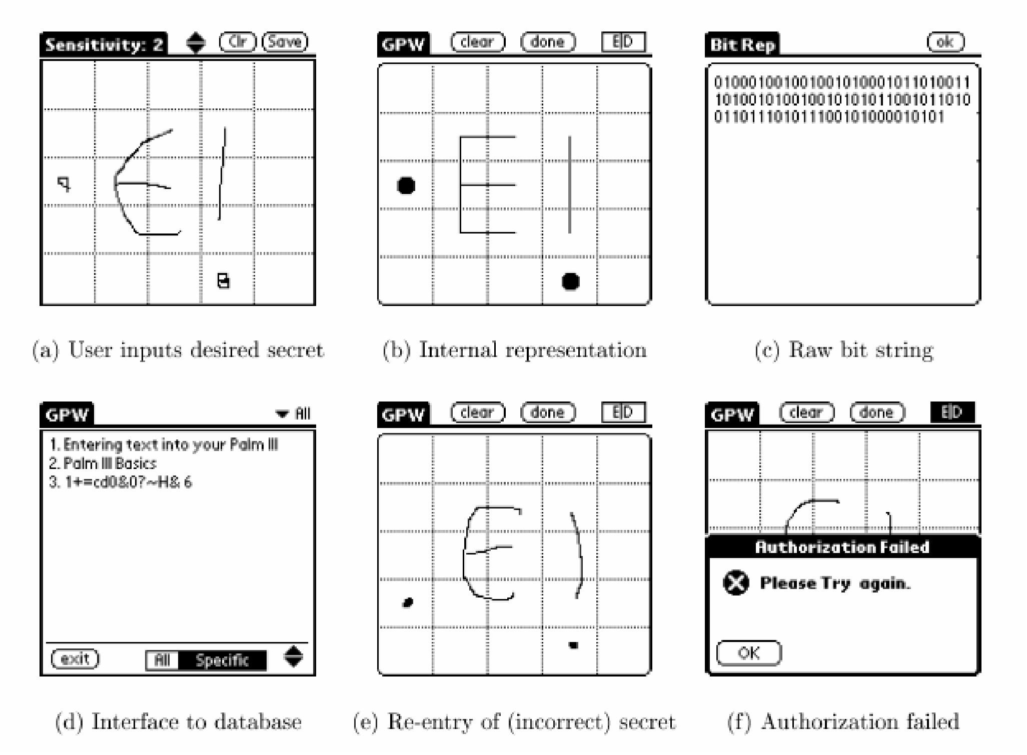
2.3.2.1 Pure recall-based Technique

It is also known as draw-metric technique, where the user is asked to reproduce something that he or she created or selected earlier during the registration stage without clues are given to remind the passwords. This technique is simple and easy, but the difficulty is that passwords are hard to remember. Where there several exist types of these schemes such as:

- DAS scheme.
- Pass-Doodle scheme.
- Signature scheme.

2.3.2.1.1 DAS scheme

As reported by *Fatemeh* (2020), a new scheme was proposed by *Jermyn et al*. in 1999 called "Draw-a-Secret" (DAS), which allows user to draw their unique password as show in Figure 2.10, where the user is asked to draw a simple image on a 2D grid. During authentication, the user is asked to redraw that image. If the drawing touches the same grids in the same sequence, then the user is authenticated. *Jermyn, et al.* suggested that given reasonable-length passwords in a 5X5 grid, the full password space of DAS is larger than that of the full text password space.



```
010001001001001010001011010011
101001010010010101011001011010
011011101011100101000010101
```

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H& 6

Please Try again.

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 2.10: DAS scheme.

Thorpe and Oorschot (2004) examined the effect of password length and number of strokes as a complexity characteristic of a DAS schema. Their study showed that the number of strokes has the largest effect on the DAS password space. The size of the DAS password space decreases significantly with fewer strokes along the static password. DAS password length also has a big impact but the effect is not as strong as the number of strokes.

To improve the security, *Thorpe and Oorschot* proposed a "Grid Selection" technique. The selection grid is initially a large fine-grained grid from which the user selects a drawing grid, a rectangular area to enlarge, where they can enter their password as shown in Fig. 2.11. This will greatly increase the DAS password space.

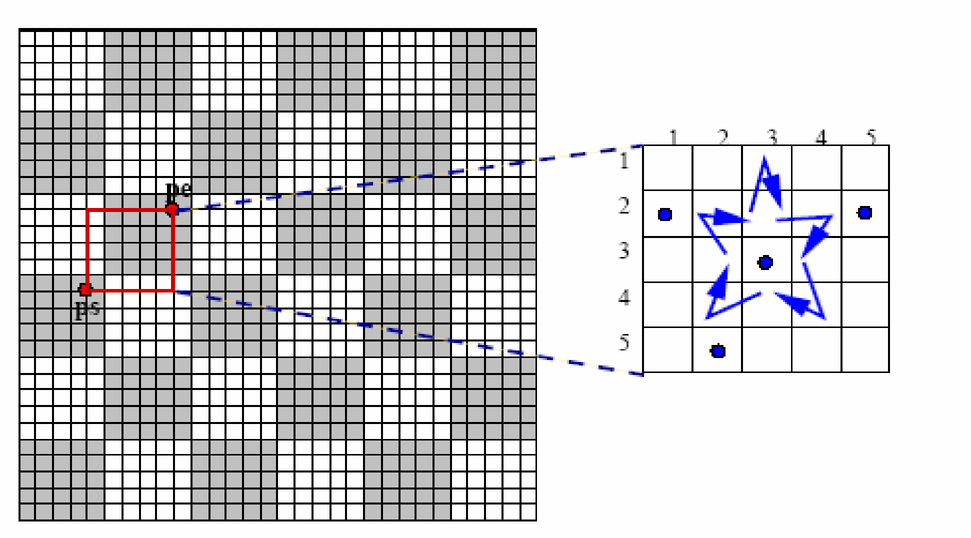


Fig. 2.11: Grid selection scheme.

Lin et al. (2007) presented an enhanced variation of the DAS Qualitative Draw-A-Secret (QDAS). In this scheme, a stroke is mapped to its starting cell and the sequence of qualitative direction changes including "up", "down", "left" and "right". Therefore, the user only needs to remember the starting cell index and the correct direction order of each stroke. QDAS uses qualitative spatial relations and dynamic grid transformations to reduce potential usability problems and shoulder surfing attacks. However, QDAS did not solve the issue of usability in DAS where the drawing cannot pass through a crossing point. It remains a concern whether the use of grid transformations will create new problems, such as cells decreased to a predefined minimum size, much smaller than the original. Figure 2.12 shows the QDAS scheme.

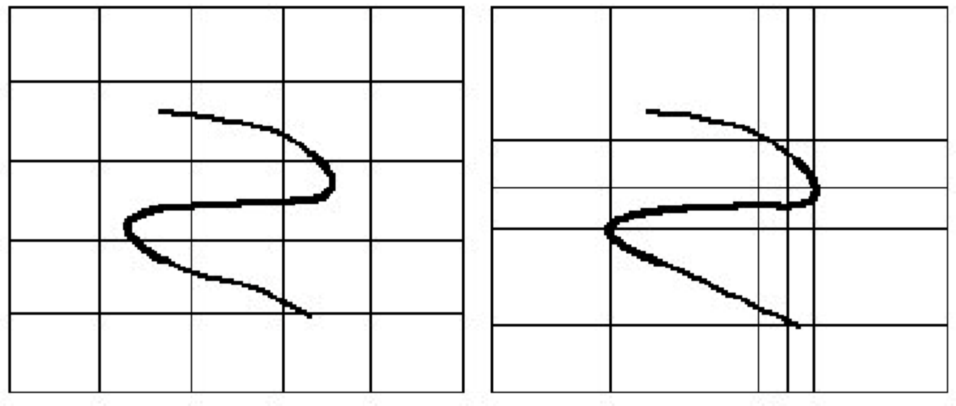


Fig. 2.12: Qualitative DAS (QDAS) scheme.

The drawback of DAS scheme is that the user is not familiar with drawing via mouse, so users attempt to draw something simple, which makes the number of strokes less. That leads to a small password space. There are some improvements have been suggested with the "Grid Selection" scheme and the "Qualitative Draw-A-Secret" scheme, nevertheless, these schemes still suffers from the problem that the user does not accept the use of the mouse as a drawing tool. In addition, when the user draws the shape entered in the registration stage, the user may not be able to choose accurately correct points, which leads the user to try again and that is considered as boring process for the user.

2.3.2.1.2 Pass-doodle Scheme

Varenhorst (2004) introduced the Pass-doodle scheme. This scheme allowing users to create a freehand drawing as a password without a visible grid, Figure 2.13 shows an example of a doodle draw. A doodle should consist of at least two pen-strokes placed anywhere on the program screen. After reading the mouse input, the system begins to scale and stretch the doodle to a grid, and then compares the stretched doodle with the stored user data.

In addition to the doodle drawn, the speed used in drawing the doodle is also calculated and saved. This graphical authentication scheme provides an easy way for users to remember the pass-doodle drawn but it was observed that sometimes the users forget the order in which they were drawn and it tends to be vulnerable to shoulder surfing.

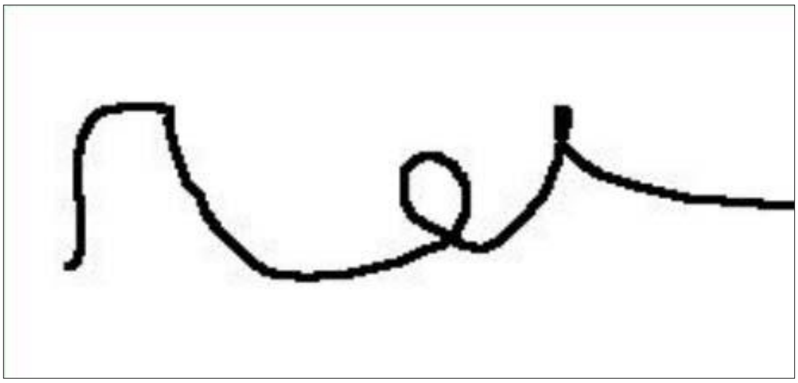
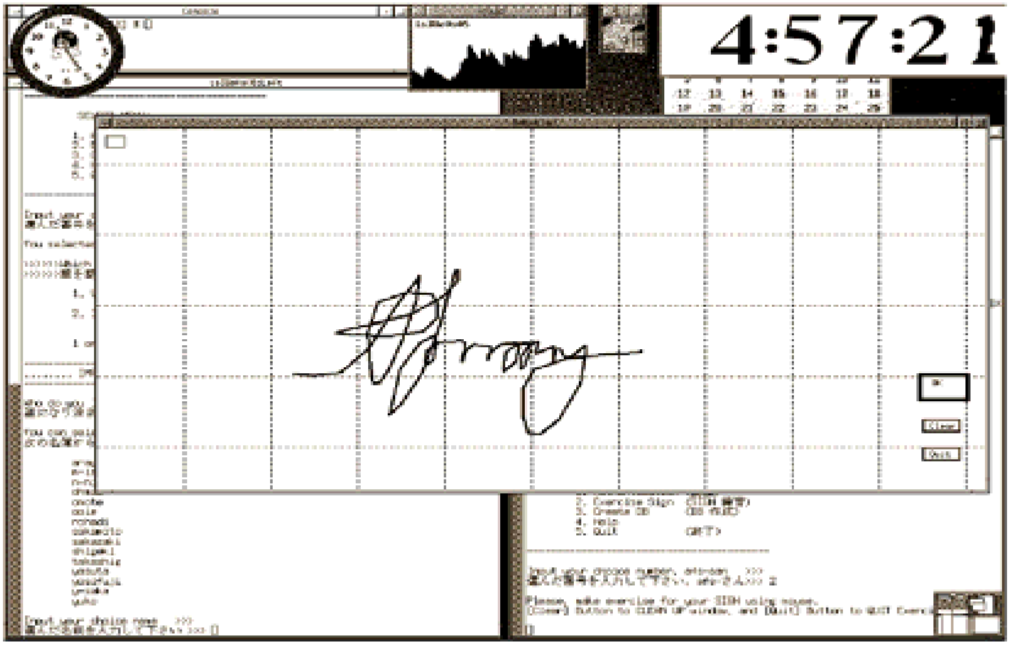


Fig. 2.13: Pass-doodle scheme.

2.3.2.1.3 Signature Scheme

Syukri et al. in 1998 proposed a system, where authentication is conducted by having user drawing their signature by using the mouse, which is shown in Figure 2.14.

During the registration stage, user first will asked to draw their signature with mouse, and then the system will extract the signature area and either enlarge or scale-down signatures, rotates if needed (also known as normalizing). The information will later saved into the database.



2. Exercise Sign
3. Create ID
4. Help
5. Quit

Please, make exercise for your SIGN using mouse.
[Clear] button to CLEAR UP window, and [Quit] button to QUIT Exercise

Fig. 2.14: Signature scheme.

The validation stage first takes user input, normalizes again, and then extracts signature parameters. Next, the system performs the verification using geometric averages and a dynamic update of the database. According to Sukri's algorithm, the successful validation rate was satisfactory. The biggest advantage of this scheme is that there is no need to memorize a person's signature and it is difficult to forge signatures.

However, not everybody is familiar with using mouse as a writing device; the signature can therefore be hard to drawn. One possible solution to this problem would be to use a pen-like input device, but such devices are not widely used, and adding new hardware can be expensive.

2.3.2.2 Cued recall-based Technique

In this authentication technique, a user is asked to repeat sequences of actions originally conducted by the user during the registration stage with providing some hints. There are exist schemes that fall under this type of techniques such as:

- Blonder scheme.
- Pass-Point scheme.
- Pass-Logix scheme.

2.3.2.2.1 Blonder Scheme

Initial graphical password research was performed by *Blonder* in 1996, who designed a graphical password system in which a password is generated by having the user click on several sites on an image. During the authentication, the user has to click on the approximate areas of those sites. The image can help the users to remember their passwords and thus this method is more convenient than unassisted invocation (as in text password) as shown in Figure 2.15.

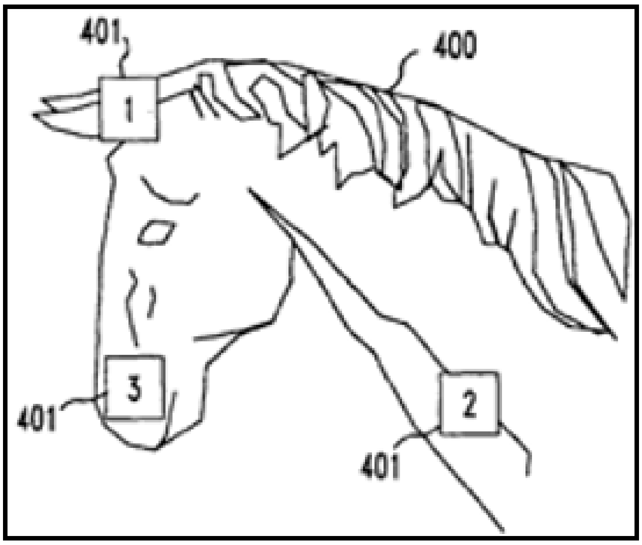


Fig. 2.15: Blonder scheme.

The disadvantage of this scheme is that the user cannot select the same point down to the pixel level, so the scheme must inherently have some margin of error. The size of the error area effectively sets a theoretical limit to the number of different passwords for each image.

2.3.2.2.2 Pass-Point Scheme

Wiedenbeck and others. (2005) proposed a scheme called Pass-Point similar to the Blonder scheme, in which the system would display an image to the user and then ask them to choose five distinct click points on that image. To log in, the user has to click on those same five dots in the same order. Since it will be difficult for users to click the exact pixel at each login, a tolerance zone is created around each point, and any click is accepted within the tolerance zone. Figure 2.16 shows the Pass-Points login screen.

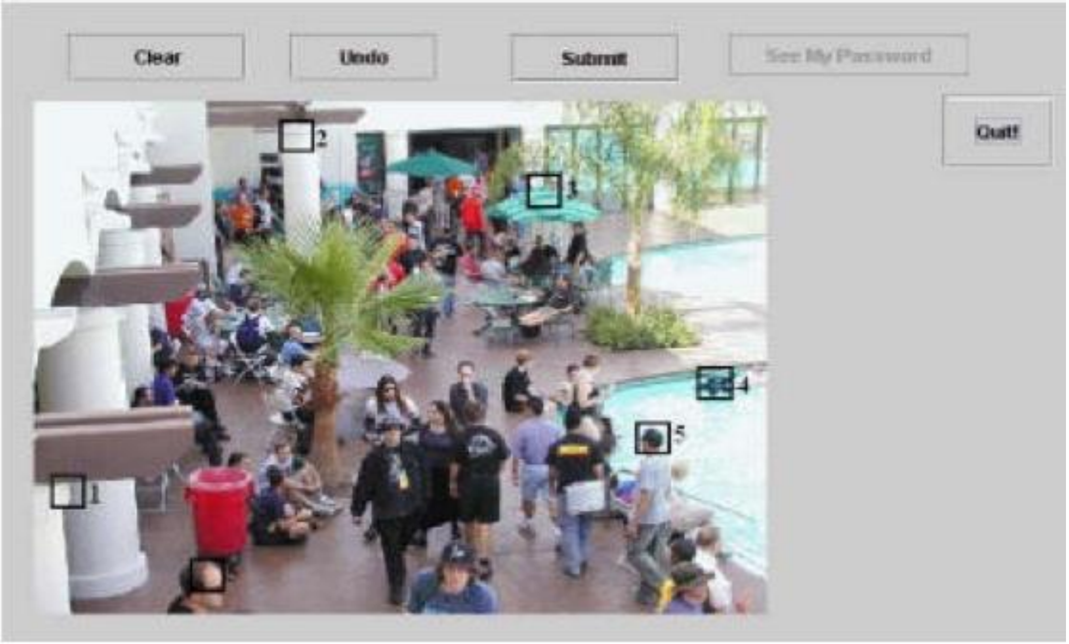


Fig. 2.16: Pass-points scheme.

A user study was conducted in which one group of participants was asked to use a text password and the other group was asked to use the graphical password. The results of this study showed that the graphical password took fewer user attempts than text passwords. However, graphical password users had greater difficulties learning the password and took longer to enter their passwords than textual users.

They conducted another user study to evaluate the effect of tolerance of clicking during the re-authenticating stage, and the effect of image choice in the system. The result showed that memory accuracy for the graphical password is strongly reduced after using smaller tolerance for the user-clicked points, but the choices of images do not make a significant difference.

Chiasson et al. (2007) proposed Cued Click Points (CCP) scheme, which is works similarly to Pass-Points, but instead of choosing five click points on one image, the user is asked to choose one click-point on each of five images. The way the next image will be displayed is determined by user's click point on the current image as shown in Figure 2.17.

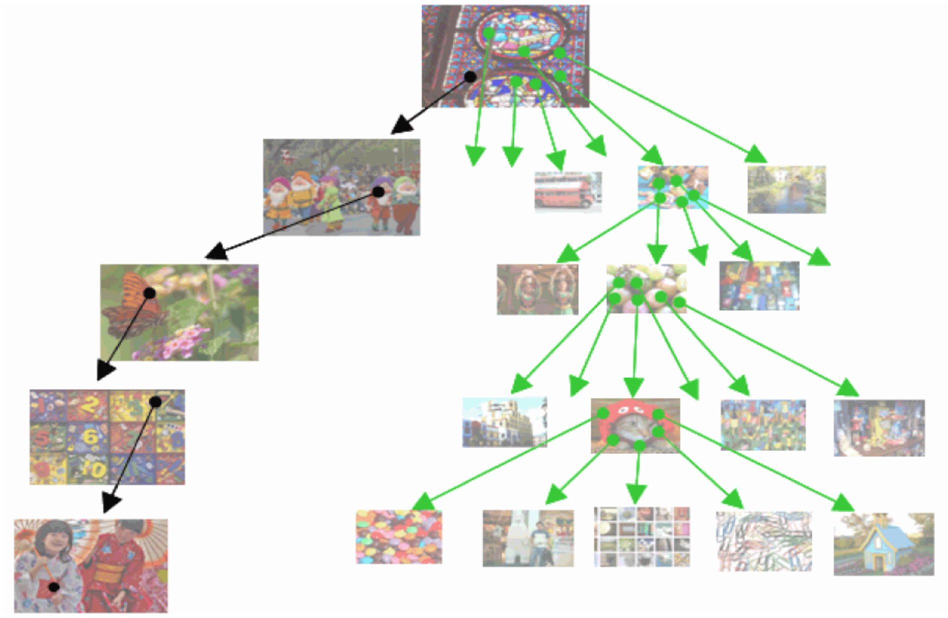
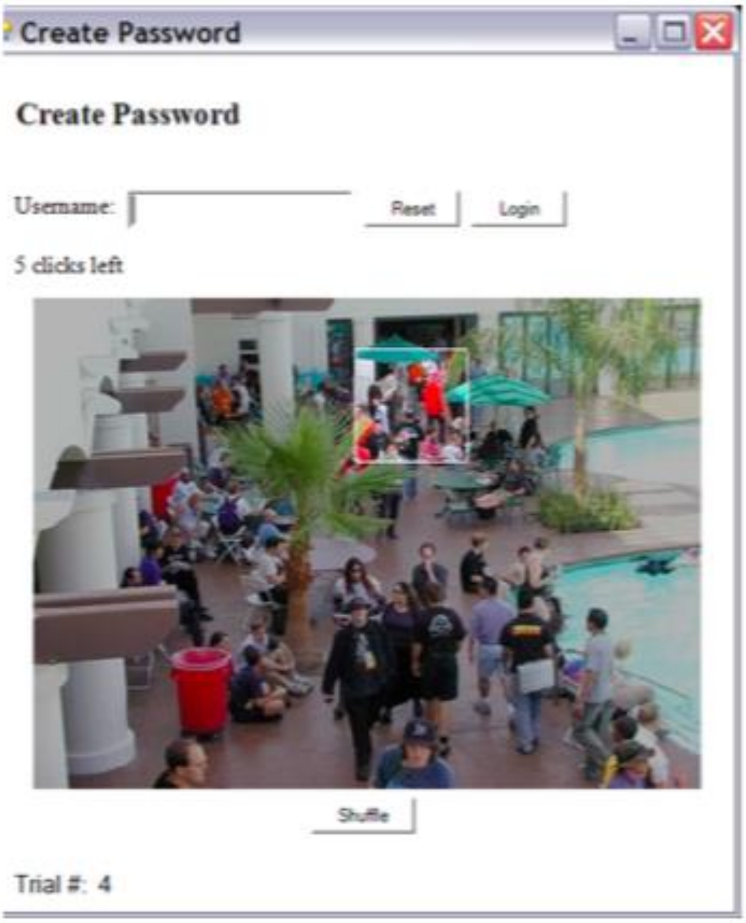


Fig. 2.17: Cued Click Points scheme.

In this scheme, they improved two aspects of usability; prevent users from clicking all passwords on one image (eliminate the problem of forgetting click points), and providing feedback at the early stage of login, rather than at the end of the login session. When logging in, the user has to click again on the correct point on each image. The images are presented in sequence and feedback is built into the system if the user clicks on an incorrect point, they see an incorrect subsequent image, immediately alerting the user to their error.

They improved the above scheme in 2008 as the Persuasive Cued Click-Points (PCCP) scheme. Where during password creation the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure 2.18. Users have to select image password (click point) within the current image. If they are unable or unwilling to select a point in the current image, they may use the Shuffle button to reposition the image randomly. A user who is determined to reach a certain click point may still Shuffle until the view port moves to the specific location, but this will take lot of time and make it more tedious process.



Create Password

Username:

5 clicks left

Trial #: 4

Fig. 2.18: Persuasive Cued Click-Points (PCCP) scheme.

2.3.2.2.3 Pass-Logix Scheme

In 2002, Pass-Logix Inc. Company developed a new graphical authentication scheme called Pass-Logix v-Go algorithm shown in Figure 2.19. At registration phase, the password is created by a chronological situation with repeating a sequence of actions. In this scheme user is asked to click on various items on the image in the correct sequence in order to be authenticated.

The main drawback of this scheme is provide only a limited password space, therefore causing the password to be kind of guessable or predictable.

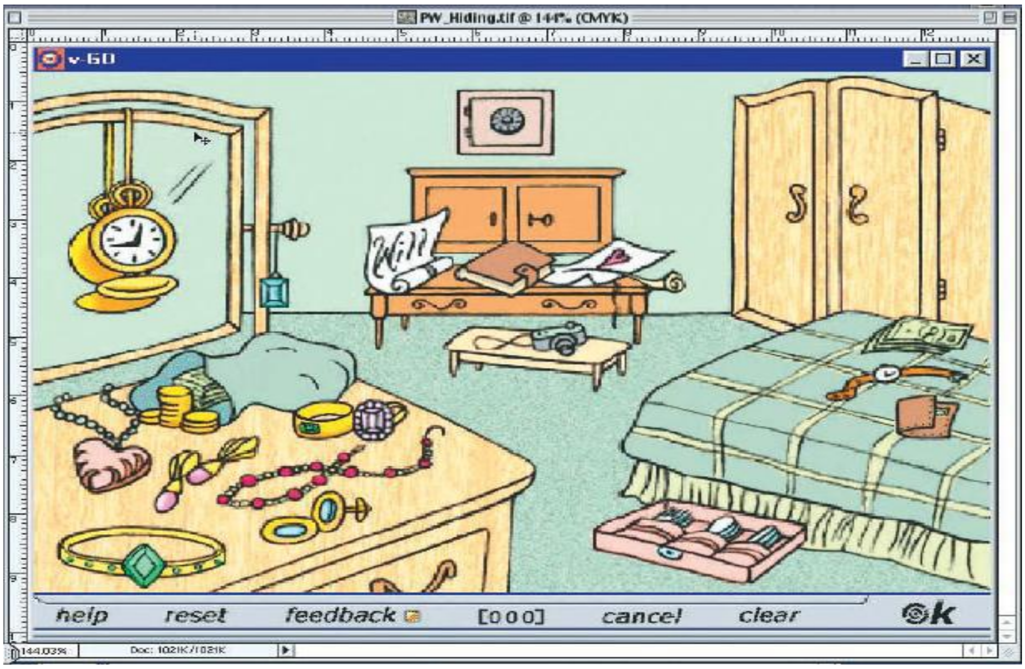


Fig. 2.19: A recall-based technique developed by Pass-logix.

2.3.3 Hybrid Techniques

Hybrid techniques is generally a fusion of two or more authentication techniques. The hybrid technique was used to overcome limitations of a single scheme such as spyware, shoulder surfing etc. There are some exist schemes such as:

- Shoulder surfing resistant authentication scheme.
- S3PAS scheme.
- CAPTCHA scheme.

2.3.3.1 Shoulder Surfing Resistant Authentication Scheme

This scheme was introduced by *Li et al.* in 2005 as a graphical password scheme as shown in Figure 2.20, which used three steps and claimed to reduce the problems of shoulder surfing, where the user is going through three main steps.

First, users need to choose one secret image as background image. Second, to choose their second secret image, users need to click on any area of their secret background, in which a series of images will later appear for them to choose. Finally, once finished selecting their second image, another set of images will appear and users need to choose their third secret image. The drawback of this scheme is that it is still vulnerable to shoulder surfing attack.

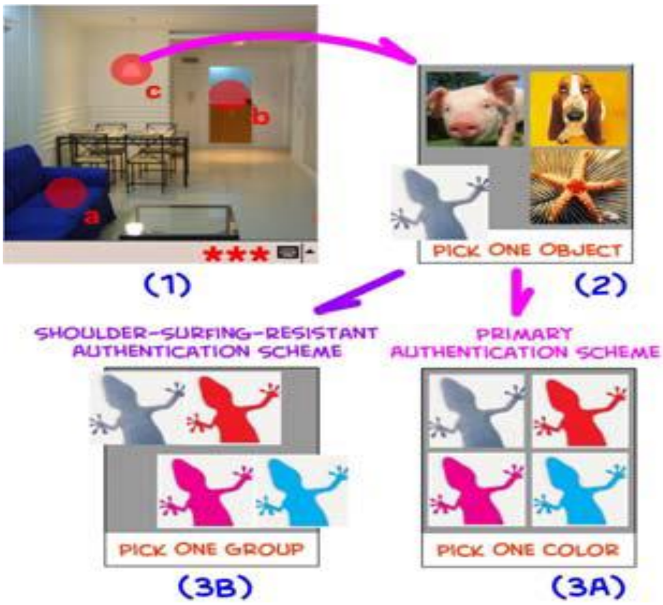

a
b
c
(1)
PICK ONE OBJECT
(2)
SHOULDER-SURFING-RESISTANT AUTHENTICATION SCHEME
PRIMARY AUTHENTICATION SCHEME
PICK ONE GROUP
(3B)
PICK ONE COLOR
(3A)

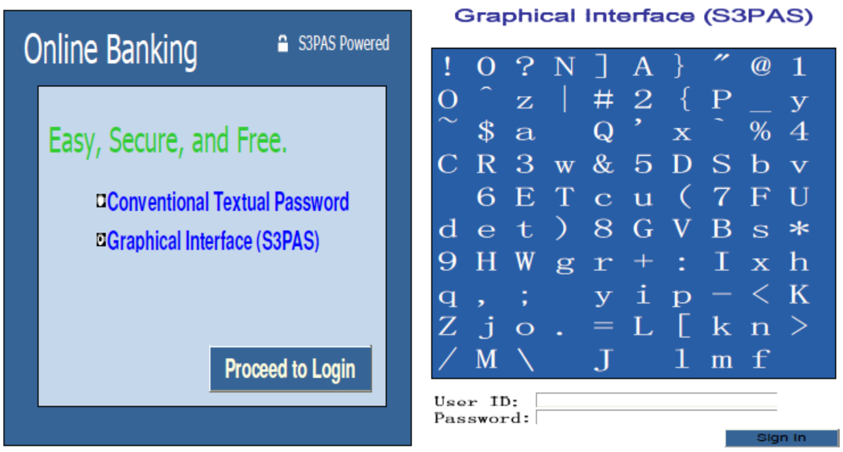
Fig. 2.20: Shoulder surfing resistant authentication scheme.

2.3.3.2 S3PAS Scheme

Zhao and Li (2007) proposed a textual and graphical password authentication scheme (Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS)) as shown in Figure 2.21, which combines features of both textual and graphical passwords. This scheme is resistant to attacks such as spyware, shoulder surfing etc. Users of this scheme have two types of passwords; one fixed password which only they know (e.g. Staff number, Library ID) and one random password which is created during the login.

To login, users will be displayed with the login interface, which consists of the image of characters displayed randomly for every round and two text boxes for inserting fixed and random password. First, users need to input the fixed passwords. To get the random password, they need to find their fixed textual passwords represented in a graphic. After identifying their random password, users have to insert it in the text box provided.

However, there are still some minor drawbacks in this scheme similar to other graphical password schemes. The major issues in S3PAS schemes include slightly more complicated and longer login processes.



Online Banking

S3PAS Powered

Easy, Secure, and Free.

□ Conventional Textual Password

☒ Graphical Interface (S3PAS)

Proceed to Login

Graphical Interface (S3PAS)

!	0	?	N	]	A	}	”	@	1
O	ˆ	z	|	#	2	{	P	_	y
~	$	a		Q	’	x	`	%	4
C	R	3	w	&	5	D	S	b	v
	6	E	T	c	u	(	7	F	U
d	e	t	)	8	G	V	B	s	*
9	H	W	g	r	+	:	I	x	h
q	,	;		y	i	p	–	<	K
Z	j	o	.	=	L	[	k	n	>
/	M	\		J		1	m	f	

User ID:

Password:

Sign In

(a) Login Screen (b) Login Image

Fig. 2.21: S3PAS scheme.

2.3.3.3 CAPTCHA Scheme

Gao et al. in 2009 inspired and proposed the CAPTCHA scheme, which is (Completed Automated Public training Turing tests to tell Computer and Humans Apart). It provides features of both graphical password scheme as well as CAPTCHA techniques. During registration, user selects the image as their password. At the authentication, user choose the password image from decoy of images and types the password CAPTCHA below every password image as shown in Figure 2.22. Where this scheme is complicated and requires memorizing a series of letters and numbers.

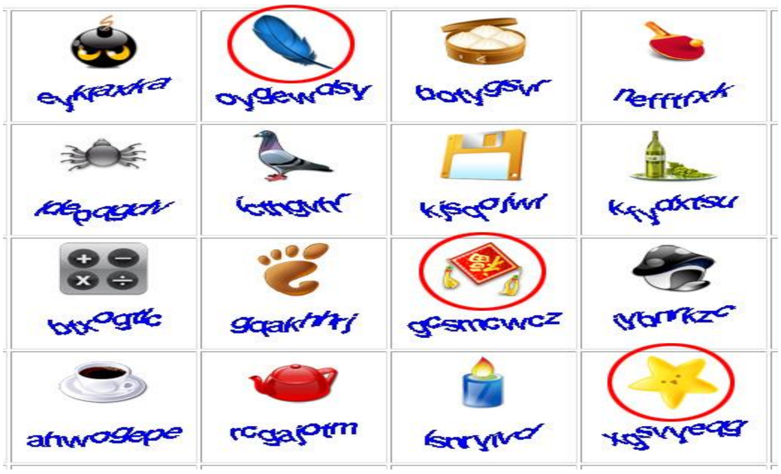


Fig. 2.22: CAPTCHA scheme.

2.4 Summing up of Graphical Password Schemes

The following Table 2.1 is summarizes the previous section.

Scheme / Attacks	Brute force	Shoulder surfing	Dictionary	Predictability	Spyware	Social Engineering	Storage Defect	Tedious Process
CAPTCHA	Yes	No	No	No	Yes	Yes	No	Yes
S3PAS	Yes	No	Yes	No	Yes	No	No	Yes
Shoulder surfing resistant authentication	Yes	No	No	No	Yes	No	Yes	Yes
Pass-Logix	Yes	Yes	No	No	Yes	Yes	No	No
PCCP	No	Yes	No	No	Yes	No	No	Yes
CCP	No	Yes	No	No	Yes	No	No	Yes
Pass-Point	No	Yes	No	No	Yes	No	No	Yes

Table 2.1. A: summarizing of graphical password schemes.

Scheme \ Attacks	Brute force	Shoulder surfing	Dictionary	Predictability	Spyware	Social Engineering	Storage Defect	Tedious Process
Blonder	Yes	Yes	No	No	Yes	No	No	Yes
Signature	Yes	Yes	No	Yes	Yes	No	No	No
Pass-Doodle	Yes	Yes	No	Yes	Yes	No	No	No
DAS	Yes	Yes	No	No	Yes	No	No	No
Pass-Image	Yes	Yes	No	Yes	Yes	Yes	No	No
Story	No	Yes	No	Yes	Yes	No	No	Yes
Theme	Yes	Yes	No	Yes	Yes	Yes	No	No
Thumbnail images	Yes	Yes	Yes	No	No	Yes	No	Yes
Pass-objects	Yes	No	Yes	No	Yes	No	No	Yes
Triangle	Yes	No	Yes	No	Yes	No	No	Yes
Pass-face	Yes	Yes	No	Yes	No	No	Yes	Yes
D'ej'a Vu	No	Yes	No	Yes	No	No	Yes	Yes

Table 2.1.B: summarizing of graphical password schemes.

2.5 Evaluation of Graphical Password Techniques

In this section, the most important factors that have been observed from the literature review that may affect the use of graphical password techniques as an alternative to text password techniques are addressed.

Several user studies had confirmed that people could recall graphical password more reliably than text-based password over a long period of time, which is supported by *Ariffin et al.* (2021). However, there is still no concrete evidence to prove whether graphical password in general is more or less secure and useable than text-based password. There are some factors used to evaluate the graphical passwords techniques, which are listed in the following sections:

2.5.1 Usability Factors

From the previous section, some factors affecting the usability of schemes are noted, which are summarized as follows:

2.5.1.1 Efficiency Factor

The time it takes for the user to login is used as a factor for measuring the efficiency of the scheme, while most of the recognition-based technique schemes are user-friendly, some of their schemes take time to login. As noted in a story scheme, the user has to go through three rounds to generating the graphical password, which will take additional time. While in the recall-based technique schemes, their schemes take longer time to login due to the presence of more than one round to finish the process of generating the graphical password. On the other hand, in the Pass-Point scheme, it has one round in which five points are selected in the same image, but the time taken for the users is long because it is difficult for the users to click the exact pixel when they choose the required points.

2.5.1.2 Effectiveness Factor

In this factor the number of attempts that user tries to login is counted. As in most of the recognition-based technique schemes, the user does not need to have many attempts, due to the ease of the login process. While in recall-based technique schemes, the user needs a number of attempts to be able to login successfully, due to the difficulty of the use and the imposition of strict policies to provide a mechanism to resist the attacks that may be exposed to the schemes of graphical password techniques.

2.5.1.3 Memorability Factor

The main reason for suggesting the graphical password technique is the previous psychological studies, which proved that the human brain is able to remember images more easily than texts. However, some users of some graphical password schemes find it difficult to remember their passwords as in the case of Pass-Object, S3PAS and CAPTCHA schemes.

2.5.1.4 Storage defects Factor

The usability feature that distinguishes graphical password techniques is an existing flaw. As the main complaint among users of graphical passwords is that the process of password registration and login takes a long time, especially in recognition-based techniques and is a weakness of graphical password schemes. Whereas, the delay in the system's response is due to storing a large number of images in the database, which causes slow response, whether in the process of entering the system or even when registering in it. This problem may direct the user to return to using the text password because waiting for the response will cause boredom.

2.5.2 Security Factors

Many attacks may face the graphical password techniques as mentioned by *Abdalkareem et al* (2021). As reported in *Harasimowicz* (2018), the identified potential attacks are based on three aspects of password security:

- Recordability relates to the ease with which the user can record the graphical password, making it easier for the attacker to capture and replay such as brute force attack, dictionary attack and spyware.

- Observability relates to the ease with which an attacker can view the graphical password as it is being entered such as shoulder surfing attack.
- Guessability relates to how easily the attacker can guess the graphical password such as predictability and social engineering.

2.5.2.1 Brute Force Attack

A brute force attack is a cryptographic hack data relies on guessing possible combinations of a targeted password until the correct password is discovered. The main defense against brute force search is to have a sufficiently large password space, whereas if the password is weak it could merely take seconds with hardly any effort to discovered the password.

Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding space button. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords such the Pass-doodles scheme which introduced by *Varenhorst* (2004).

It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to generate accurate mouse motion automatically to imitate human input, which is particularly difficult for recall-based graphical passwords.

2.5.2.2 Shoulder Surfing Attacks

Bianchi et al. (2016) defined in their research that the shoulder surfing attack is *"Sneaking and peek from behind the shoulder into a victim's computer to learn the whole password or part of password or some confidential information"*. Where most of the graphical password schemes are vulnerable to shoulder surfing attacks. Only a few recognition-based techniques are designed to resist shoulder surfing such the S3PAS scheme, which was designed by *Zhao and Li* (2007). None of the recall-based based techniques are considered should surfing resistant.

2.5.2.3 Dictionary Attack

A dictionary attack is a method of breaking into a password by systematically entering every word in a dictionary as a password. These attacks are usually unsuccessful against systems using multiple-word passwords and often unsuccessful against passwords made up of uppercase and lowercase letters and numbers in random combinations. Consequently, since recognition-based techniques involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords.

2.5.2.4 Spyware

Spyware is a malicious software designed to entering to your computer device, gather data about you, and forward it to a third party without your consent. Except for a few exceptions similar to the scheme that developed by *Man et al* (2003), keylogging or key listening spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords.

However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

There are some programs that help in hacking by recording browsers' data such as Key-logger, which is a program that runs in the background and recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords or possibly other useful information that could be used to compromise the system or be used in a social engineering attack.

2.5.2.5 Guessing or Predictability

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies conducted by *Brostoff and Sasse* (2004) on the Pass-face technique have shown that people often choose weak and predictable graphical passwords. *Thorpe and Nali's* study (2004) revealed similar predictability among the graphical passwords created with the DAS technique. This means that more research efforts and studies are needed to understand the nature of graphical passwords created by real world users.

2.5.2.6 Social Engineering

Social engineering is an attack that relies heavily on human interaction and often involves tricking people into breaking normal security measures. Hackers can attempt different tricks to break into the normal security measures, such as knowing the victim's password from his date of birth, a favorite animal, etc. Some graphical passwords are vulnerable to this type of attack, especially those that rely on selecting images or patterns.

2.6 The Relevance Works

To achieve the objectives of this work, the relevant literature was relied upon:

1. The proposed scheme is a hybrid technique scheme based on two graphical password techniques. Since the use of one technique will be weak, therefore two techniques were combined to obtain a high level of security and maintain the ease of use.
2. This work is utilized the Pass-Image scheme that proposed by *Takada and Koike* (2003) as a recognition-based technique, which is allowing the users to choose their favorite image as their graphical password.
3. The proposed scheme in this work is inspired an idea from Pass-Point scheme, which was proposed by *Wiedenbeck et.al.* (2005) as a cued recall-based technique. Where in the Pass-point scheme the user has to select 5 points in image, this scheme is difficult to implement due to the pixel resolution to be selected.
4. This work introduces a hybrid scheme where the user has to choose cells from the selected image after it is divided as grid instead of points. The advantage of this proposed scheme is that the selecting cells is easier than selecting points, because it does not need to select pixels precisely, as the case in Pass-Point scheme.

2.7 Summary

In this chapter, the most important authentication methods are discussed, and through one of these methods, graphical password techniques are discussed. The most important graphical password schemes are summarized, with illustrate how each scheme is work. Moreover, the graphical password schemes are summarized and illustrated in table showing each scheme vulnerable to which attack.

In addition, the most important factors that help in evaluating graphical password schemes were summarized, which are usability and security factors. The most important sub-factors that come under these two factors are also summarized, in order to focus on reaching the best of these factors and overcoming the problems of these factors while designing the proposed scheme.

Chapter 3

Design of Image Grid Scheme

3.1 Overview

In this chapter, the new scheme named Image Grid Scheme is presented in the graphical password techniques to increase the level of security while maintaining ease of use and ease of remembering. The system development methodology of the proposed scheme including the concept, design, and verification is introduced in details.

3.2 System Development Methodology

The Systems Development Life Cycle (SDLC) is a conceptual model used to describe the stages involved in development a project from the initial study up to the end. Various SDLC methodologies have been developed to guide the processes involved, including the Waterfall model (which was the original SDLC method); Rapid application development (RAD); Joint application development (JAD); the Fountain model and the Spiral model.

The waterfall model is suitable for systems whose requirements are clear and the expected changes to these requirements are limited during the design phase, this model is also used in projects related to large systems as reported by *Ribdawi* (2018). Therefore, because the requirements of this work are clear from the beginning and the goal is specific, the waterfall model was chosen for the proposed system development methodology as shown in Figure 3.1.

The following steps illustrate the stages that this research has gone through using the waterfall model:

1. The first stage of the image grid scheme is the planning process. Firstly, the work started with a plan to develop new prototype system based on the usability features of existing schemes, while not repeating the problems of the existing graphical password schemes.
2. The second stage was the requirements analysis process where usability and security features should be analyzed for consideration in the development process.

3. The third stage was the design of the system, and at this stage, the system requirements were summarize and ready for implementation. The process of implementing the system is very important, and the system framework should be ready for the implementation process.
4. The implementation process started, where in this stage, the design was translated into code, which is computer programs written using a conventional programming language or an application generator, also a revise of the system was done to avoid the implementation errors during this stage.
5. Testing, this stage is the final stage of the development process. Where the system as a whole was tested first by the researcher who created this system and then it was tested on a sample of the community. Testing the system on a sample of the community done through testing it in a laboratory environment and then using questionnaires, which given to the experimenters of the system to ensure the implementation of usability features and user satisfaction with the proposed system design.
6. The final stage in the whole work was the results analysis stage, which is the process of testing the results collected from the direct observation of the participants in the experiment as well as from the questionnaires they filled out.

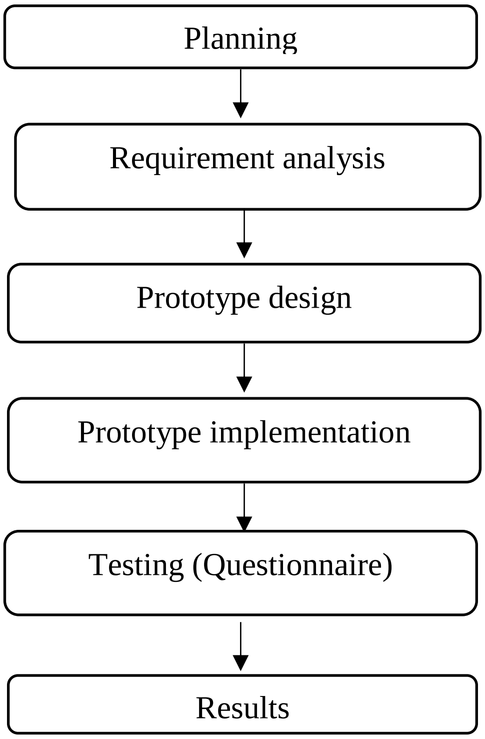


Fig 3.1: Prototype Development Life Cycles.

3.3 Concept of the Image Grid Scheme

This scheme is consider as a hybrid graphical password technique, where it depends on the recognition-based technique and cued recall-based technique. The idea for the image grid scheme is inspired from scheme discussed by *Takada and Koike* (2003), where their scheme allows users to use their favorite image for authentication. However, this method does not make it more secure authentication method than a text password. Nevertheless, the advantage of users using their favorite image as a password is weak feature, as indicated by *Davis et al* in their study (2004), as it is more vulnerable to hacking because it is considered easy to predict, especially if the hacker is close to the user.

To address these shortcomings, a new feature has been added based on recall-based technique, where the image after selection by the user will be display as 5x6 grid, meaning that the image will be divide into 30 cells. To complete the password selection, the user has to choose from 2 to 4 cells. This feature will help to solve a security issue that has exposed to the previous graphical password scheme based on the user's choice of their favorite image. So that, if the hacker is familiar to the user, this makes the password predictable and may know which image may choose from among a group of images. However, with adding the new feature the hacker will not be able to predict which cells the user may choose.

In addition, it addresses the shoulder surfing attack. Since the image grid scheme works on the desktop computer and is not on mobile devices, and since the screen is large, it is easy for anyone beside the user to know the chosen image, and this makes the password vulnerable to hacking. Wherefore, with adding the feature of selecting cells, anyone beside the user will not know what cells are selected.

Thus, this scheme tentatively has fulfilled the main usability requirement and provided a means of defense against prediction and shoulder surfing attack. Whereas, to ensure that the image grid scheme fulfills the conditions of these requirements, it will be tested using quantitative and qualitative approaches.

To test the image grid scheme and obtain realistic results a new system was developed based on using the image grid scheme, which proposed in this work. Moreover, case study was conducted to apply an experiment on the proposed system. Then the results were collected after the completion of the experiment process, where these results will be presented and discussed in Chapter 5.

3.4 Design of the Proposed System

The proposed hybrid authentication system is designed in this section, where all the problems and limitations of graphical based schemes is take into consideration. The proposed system is a scheme that offers more reliable, secure, user-friendly and robust authentication. The proposed system consists of two phases, as shown in Figure 3.2, which are as follows:

1. Registration phase.
2. Login phase.

3.4.1 Registration Phase

In this phase, what steps the user should follow to be registrant that will be displayed. However, how to implement these steps programmatically by the system will be discussed in Chapter 4.

Algorithm of the registration phase

Step 1: Request to registrant to the system.

Step 2: Enter the username, a new text password and some personal information.

Step 3: Select image.

Step 4: Select 2-4 cells from the 5X6 gird in sequential manner.

***Step 5**:* Click the Submit button.

The new user has to be registered in the system before starting the experiment, so the user is restricted to using the system window of the registration process. Where the user has to go through the following steps to be registered in the system:

1. The first step in the registration phase the user has to enter the username, the text password and other optional information. Whereas, the text password is restricted by some security conditions that were imposed in this research. The user is required to enter a new text password, which should be at least 8 characters and should contain at least one number. In addition, the user should not use a password that was previously used in one of the user's accounts; also, it should not be the name or date of birth of a close person to the user. These restrictions are imposed

to ascertain how well the user remembers a strong and unexpected password, and to compare it to how well they remember the suggested graphical password.

2. In the next step, the user has to choose image, where the user is completely free in choosing the image, so the user can choose his or her favorite image, an image of one of his or her family or even his or her personal image. After the user selects the image, the selected image will appear to the user in the form of a grid divided into 30 cells.
3. In the third step, the user has to select two to four cells from the image grid in a sequential manner, and the user has to focus on this sequence because he or she will need to remember it. Whereas, this step has been added to the image grid scheme to increase its defense against shoulder surfing attack, that is, if someone is next to the user and sees the selected image, they will not know which cells the user has selected. This is because when the user selects cells, their color will not change and no borders will be drawn on them, in other words, these selected cells will remain the same as displayed for the rest of the cells.
4. The last step, which is the user has to press the "Accept" button to migrate the entered data to the database, at this step it will be verified that the username which entered does not exist in the database. If the username already exists, the user will be alerted and the user will has to enter a new username. Otherwise, in case the entered username does not exist, the user will be notified that the registration has been completed successfully via a message.

After the user completes the process of selecting the image and cells, the system will save the image source address, its name, and the default name of the selected cells in the database as a text string. This means that the graphical password will be stored in the database as a text password without having the user to remember any text. Thus, the image grid scheme will provide another important advantage of graphical password schemes. As when storing images in the database, the size of the database becomes large, which slows down the process of storing and retrieval of data from it, which creates boredom for the user.

3.4.2 Login Phase

At this phase, the user should have a username, text password and graphical password to be able to access to the system.

Algorithm of the login phase

Step 1: Request to login the system.

Step 2*:* Enter username and text password that entered in the registration phase.

Step 3*:* Click the "Load Image" button to choose the chosen image.

Step 4: Select the chosen cells in the same sequence that selected in the registration phase.

Step 5: Press the "OK" button.

After the user registered in the system in the previous phase, now the user can login to the system. The user can login to the system through the following steps:

1. The first step in the login phase, the user has to enter his or her username and his or her text password, which has already been entered in the registration phase.
2. In the next step, the user has to select the same image that he or she chose in the registration phase. After the user chooses the image, it will appear divided into a grid containing 30 cells, as happened in the registration phase.
3. In the third step, the user has to select the previously selected cells from the image grid in the same sequence as before. Specifically, the user has to choose the same cells and in the same sequence that did in the registration phase.
4. The last step, the user has to press the "OK" button to migrate the entered data to the database, in this step the inserted data will be passed to the database for validation. If all the entered data is correct, the user will be notified that the login process has been successful. In other cases, the username entered by the user will first be checked if it exists. If there is no match, the system will send an error message to the user stating that the username is wrong and asking the user to try again. The next step, check the text password entered, if it is wrong, the system will send an error message to the user that the text password is wrong and ask the user to try again.

After checking the username and the text password, the database will check the validity of graphical password. If the graphical password does not match the username, an error message will sent to the user to enter the graphical password again and inform the user that he or she has only three attempts in order to be careful while choosing their password on the next attempts. Thus, if the three attempts fail, the account will be temporarily blocked for 24 hours for security reasons.

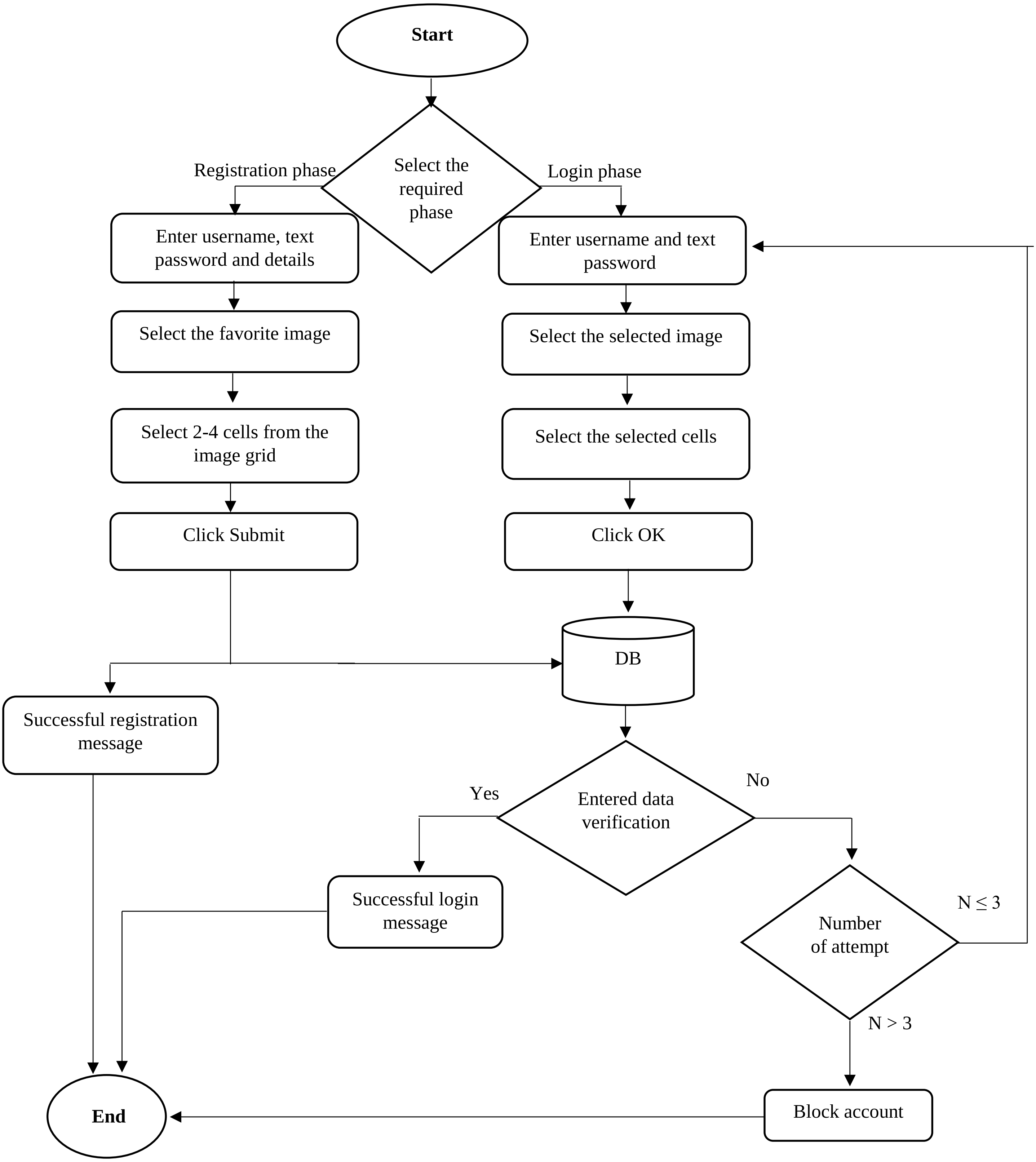

Start
Select the required phase
Registration phase
Login phase
Enter username, text password and details
Select the favorite image
Select 2-4 cells from the image grid
Click Submit
Enter username and text password
Select the selected image
Select the selected cells
Click OK
DB
Successful registration message
Entered data verification
Yes
No
Successful login message
Number of attempt
N ≤ 3
N > 3
Block account
End

Fig. 3.2: Flow chart of the proposed system.

3.5 Verification of the Image Grid Scheme

This section will focus on usability and security analysis. For usability, will focus on the easiness of registration and login, and will focus on the memorability of the user. For security, will focus on password space and the extent to which the image grid scheme provides a defense mechanism against shoulder surfing attacks.

3.5.1 Usability Verification

Akula and Devisetty (2004) stated that the important factors that influence of usability are the content (images), the spatial layout of the content, and input devices. Whereas, the use of recognition techniques are considered as the easiest technique to the users to remember their password as discussed by *Tiller* (2020). Therefore, this research is based on the recognition-based technique.

In most of the recognition-based schemes that deal with images, the user takes a lot of time when waiting to load a group of images. Then the user should recognize the image that he or she had chosen in the registration phase to be the password from a group of images that are displayed in the random order in each entry. As a result, the process takes time to wait for the download and then take time to recognizing, and this is one of the disadvantages of existing graphical password schemes. In addition, too many distraction images tend to slow down the authentication process, and if the authentication process is too tedious, it may create memorization difficulties and annoy users.

Accordingly, the image grid scheme is utilized an existing scheme, pass-image scheme, in order to allows users to use own favorite image to be their password and that saves a lot of user's time. Since the user selected the image, the user will not find it difficult to remember it. Although the pass-image scheme was used, it suffers from security issues that are resolved and discussed in the next section.

Thus, the image grid scheme will not make the user waits for the download process that is because the image will load it from user's computer and the user will not take time to recognize it. Therefore, it is easy to conclude that the login time can reduced greatly. Moreover, in the login phase, the user will not have to pass through many steps to enter the graphical password and will not have to do a lot of effort to remember that password.

3.5.2 Security Verification

Security can be judged based on several important areas; they are brute force search, dictionary attacks, guessing and shoulder surfing. As discussed in chapter 2, one of the common weaknesses of graphical passwords is susceptibility to a shoulder surfing attacks, which is the core of the image grid scheme to provide a defense mechanism against this attack. In the image grid scheme, the image will be divided to grid consist of group of cells then the user has to select cells. ***With this new feature***, it will be difficult for someone standing near or behind the user to notice which cells have been selected. Thus, the image grid scheme will be resistant to shoulder surfing attack. Moreover, this step makes the password more secure to guessing attack, where the attacker will not be able to predict the number of cells that the user had selected, and it is difficult to predict which of the 30 cells were selected. This feature is

3.6 Summary

In this chapter, the steps of the methodology for the image grid scheme was proposed and explained, where the Waterfall Model was selected for the image grid scheme as a guideline for the research. In addition, the steps of development the image grid scheme was explained as hybrid scheme based on recognition technique and recall technique.

The design of the system and its phases, the registration phase and the login phase, were clarified and explained, also the algorithm of each phase was explained, where the proposed system provide ease of use in the registration and login phases.

Moreover, this chapter discussed that the image grid scheme prevent the attacks that graphical passwords may exposed to, while some previously proposed work failed to provide it.

Another issue not addressed in this chapter is the extremely large storage requirements, which is an important issue for recognition-based technique schemes. Although the image grid scheme is based on recognition-based technique and while the size of typical image is much larger than text, the image grid scheme does not suffer from storage defects due to the addition of another new feature to the image grid scheme. As the system will store the image in the database as a string of letters and numbers, the database will not deal with any image. That is, it will not overload the database, and therefore will not cause the registration and login phases to be impaired.

Chapter 4
Implementation of Image Grid Scheme

4.1 Overview

This chapter presents the implementation of the system based on the image grid scheme, which was explained in Chapter 3, where this system was proposed based on solving the problems that faced the graphical passwords schemes in terms of usability and security. Also, some of the system interfaces were shown and how to use these interfaces.

4.2 Important Elements of Implement Image Grid System

In this section, the most important elements of usability and security that were focused on during implement the system will be presented. After investigated the previously existing schemes, it was noted that the graphical password techniques suffers from a problem that when the security increases, the usability decreases. Consequently, this research is focus on the most important elements that the users may request them in the system to make it easier for them to accept and use the proposed technique as an alternative to the text password, which they are accustomed to using, and the most important usability elements are as follows:

- Easy to use: use the mouse (that is, the user can use the system without any complexity, as the system allows the user to use the mouse to enter the password, where this is not an additional hardware or the user does not know).
- Easy to create: choosing image and cells are simple process (that is, the user can easily create the graphical password by ease to choose the image and select cells).
- Easy to memorize: choosing favorite image (that is, that the users can easily remember their favorite image that used as a password because the human beings can remember images easily).
- Easy to learn: simple terminology and windows layout, and ease interface understanding (where these features helps the user to use the system easily and without complicated problems).

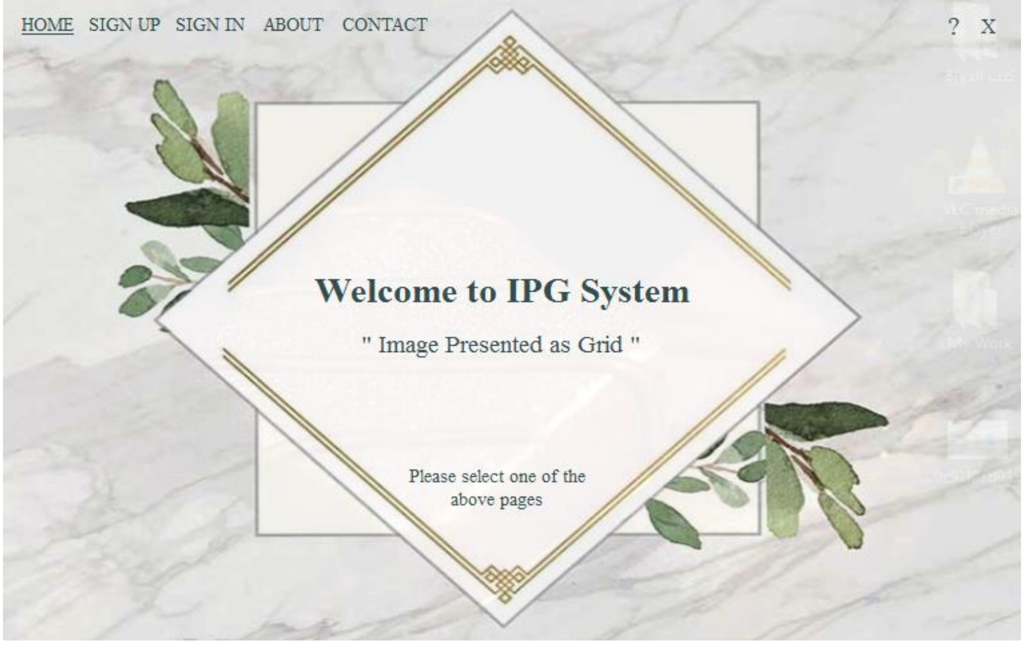
The important security elements that focus on in this research are following:

- Predictable attack: Allowing the user to choose their favorite image makes it an easy target for guessing attack, especially if the attacker is a friend of the user. Thus, the feature of splitting the image into a group of cells has been added, this feature will reduce the possibility of guessing the user's graphical password.
- Shoulder surfing attack: when the user chooses the image, if there is a person sitting next or behind to the user, this person will be able to know the chosen image and thus this person can know the user's graphical password. Therefore, in this research, the focus was on adding a new feature with allowing the user to choose an image as a password while maintaining confidentiality. Where the feature of selecting cells that has been added provides a defense mechanism against this type of attack, so that if the person next to the user knows the selected image, he or she will not know the selected cells.

4.3 Graphical User Interfaces (GUI) of Image Grid Scheme

The proposed system implemented via using Visual Studio 2013 as the developing environment and Visual Basic.net as a programming language. It is important to notice that in the design phase the size of cells has a strong impact on the usability of system, where if the cell is too small, the user has to slow down the speed of choosing the cells. On the other hand, if it is too big, then the user's password will be vulnerable to shoulder surfing attack.

For the database, MySQL Server database was used for storing the username and some information about the users, also the graphical passwords of the users will be stored as a text in the database, where MySQL Server database is a programming language for databases that is close to human language. Figure 4.1 shows the window of the system.



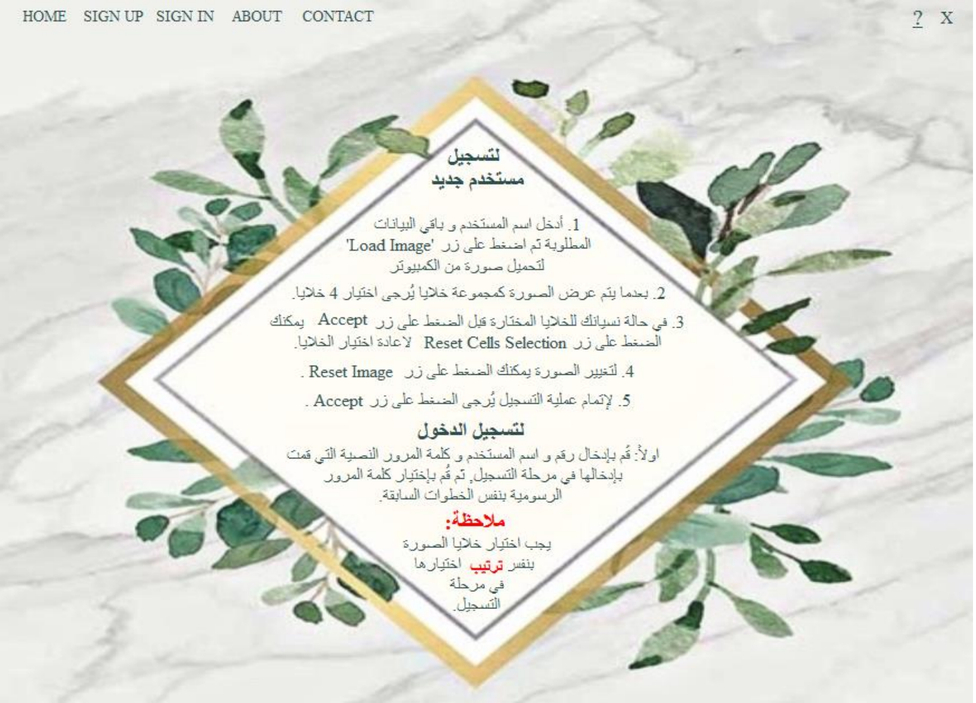
Welcome to IPG System

" Image Presented as Grid "

Please select one of the above pages

Fig. 4.1: Main window of the system.

As shown in the above Figure, the window contains welcome message and contains a set of menus at the top of the window that facilitate access to the system windows. Also this window contains (?) button at the top right of the window, when the user press this button, an window will appear on how to register in the system proposed as shown at Figure 4.2.



لتسجيل
مستخدم جديد

1. أدخل اسم المستخدم و باقي البيانات
المطلوبة ثم اضغط على زر 'Load Image'
لتحميل صورة من الكمبيوتر

2. بعدما يتم عرض الصورة كمجموعة خلايا يُرجى اختيار 4 خلايا.

3. في حالة نسيانك للخلايا المختارة قبل الضغط على زر Accept يمكنك
الضغط على زر Reset Cells Selection لاعادة اختيار الخلايا.

4. لتغيير الصورة يمكنك الضغط على زر Reset Image .

5. لإتمام عملية التسجيل يُرجى الضغط على زر Accept .

لتسجيل الدخول

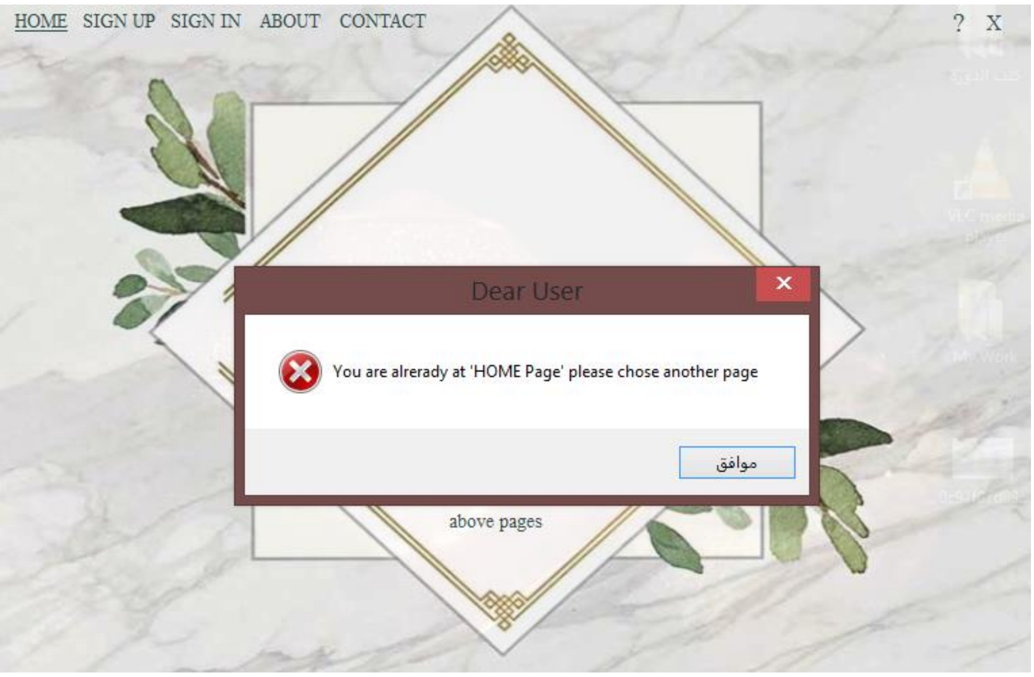
اولاً: قم بإدخال رقم و اسم المستخدم و كلمة المرور النصية التي قمت
بإدخالها في مرحلة التسجيل, ثم قُم بإختيار كلمة المرور
الرسومية بنفس الخطوات السابقة.

ملاحظة:

يجب اختيار خلايا الصورة
بنفس ترتيب اختيارها
في مرحلة
التسجيل.

Fig. 4.2: Information window.

Will notice that the first menu is named "Home" in the menus bar, which refers to the current window, the start window. If the user is in the main window and presses this menu, the user will be notified that he or she is on the main window as shown in Figure 4.3.



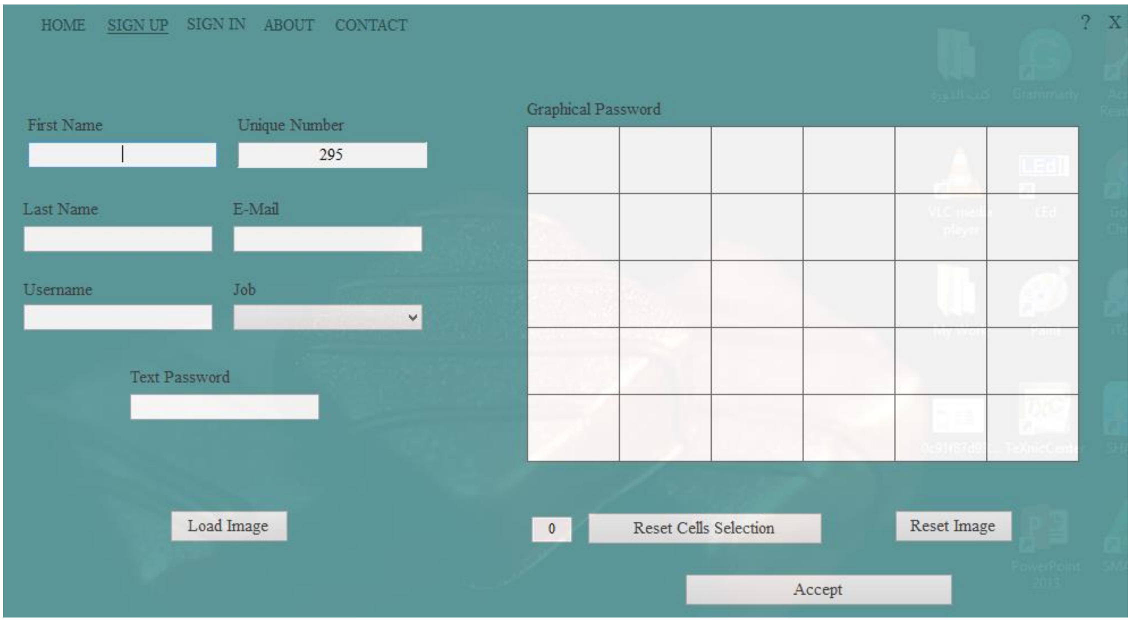
You are alrerady at 'HOME Page' please chose another page

Fig. 4.3: Notify message.

Where the "Home" menu is followed by a set of menus, including the “About” menu, when clicking on it, the user will be directed to an window containing some details about the proposed system. There is also a “Contact” menu, which an window containing the researcher’s accounts in case the user needs to communicate with the researcher. These windows will be shown in Appendix B.

4.3.1 Registration User Window

The menu that follows is the "Sign up" menu for the new user who does not have an account on this system, where when pressing this menu button, the user will be directed to the registration window shown in Figure 4.4.



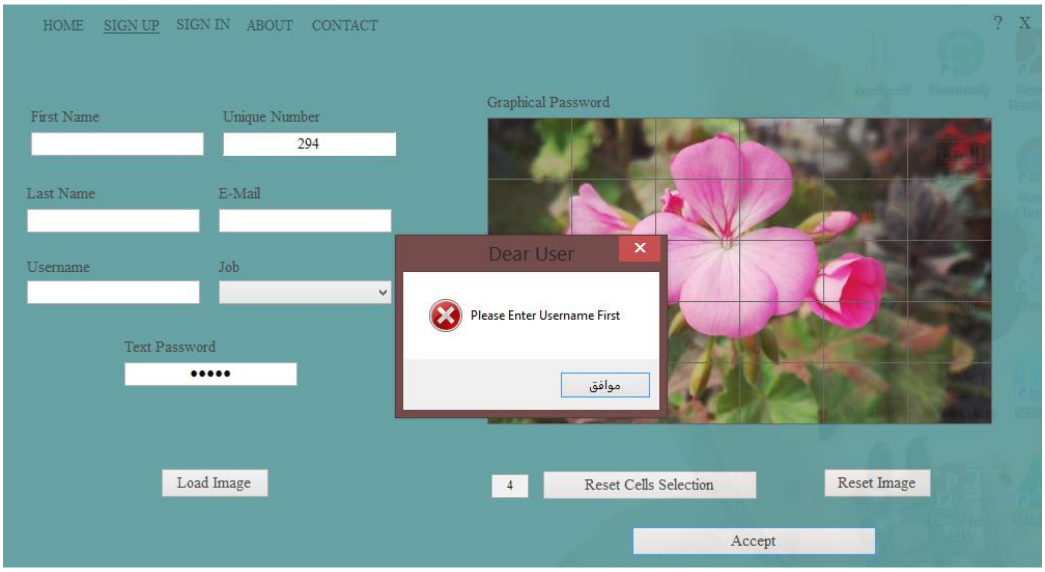
Unique Number: 295

0

Fig. 4.4: Sign up window.

This window contains some information that the user has to enter, some of them are optional and others are obligatory to enter. The system gives a unique serial number for every new user, but the user should not have to remember it or enter it at the login phase. Will notice that, there is a text box for entering the user First Name and Last Name in order to identify him or her, and a text box for the E-mail to communicate with the user in the experiment phase. Also, note that there is a “Job” option, this option has been added to help the researcher know the extent of the diversity of the sample taken from the community, as there are three options: student, employee or other.

One of the information that the user has to enter is the "Username", as the function of the system in the verification step is to ensure that there is no such username entered in the database, if there duplicate, the user will be notified to entered another username. Moreover, because this information is important and the user is required to enter it, in the event that the "username" is not entered, the system will send an error message to the user for asking to enter another "username" as shown in Figure 4.5.



First Name

Unique Number 294

Last Name

E-Mail

Username

Job

Text Password •••••

Dear User

Please Enter Username First

Fig. 4.5: Asking the user to enter a username message.

In order for the user to be registered in the system, the user has to enter a text password and it should be restricted by the conditions mentioned in Section 3.4.1, in the Algorithm of the registration phase section. If the user does not enter the "text password", the system will send an error message to the user for asking to enter "text password" first. Will be shown in Appendix B.

After entering the text password, the user has to choose the graphical password to complete the registration phase in the system by pressing the “Load Image” button shown on the window, where will appear to the user a window through which he or she can choose the wanted image. Consequently, after the selection process, the image will appear to the user in the form of 5×6 grid divided into 30 cells as shown in Figure 4.6. To finish the process of choosing the graphical password, the user has to choose from 2 to 4 cells to be his or her password, as notice the presence of a small box below the image shows to the user the number of cells that has been selected. Below the image, there are two buttons: “Reset Image” button to reselect the image in case the user’s opinion changes, and the “Reset cells selection” button to reselect the cells.

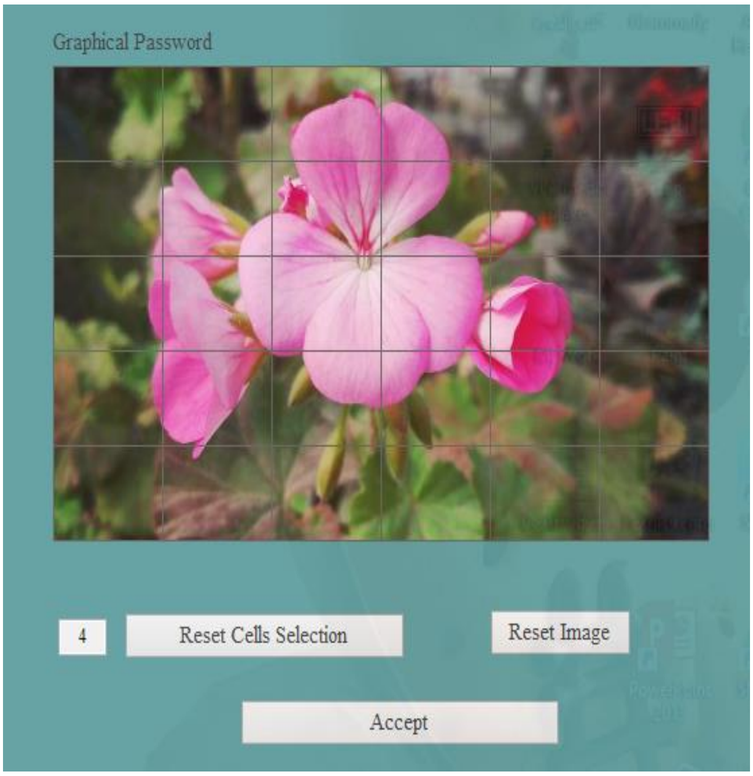


Fig. 4.6: Image displayed as a grid.

At the end of the process, the user has to press the “Accept” button to confirm the registration process. If all the entered data comply with the conditions, the user will be registered in the system and the data will be stored in the database then notified the user that the registration process was completed successfully with a message. In the event of any error or failure to entering any of the required data the user will be notified with a message.

4.3.2 Login User Window

After the user has registered in the system, the user can login while participating in the experiment phase by clicking on the "Sign In" menu to show the login window as shown in Figure 4.7.

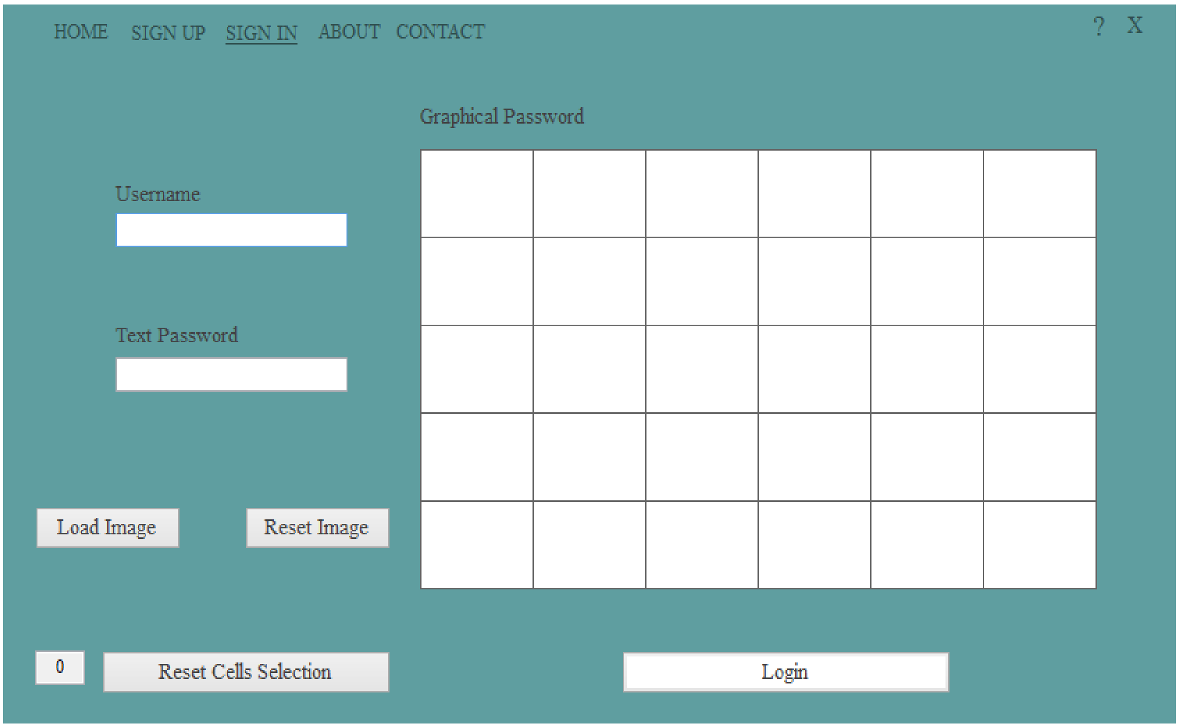


Fig. 4.7: Login window.

On this window, the user is asked to enter the username that entered at the registration phase and the text password that the user was created. Also, note that there is "Load Image" button whose task is the same as the "Load Image" button on the sign up window, where the user has to reselect the image and the selected cells at the registration phase and then press the "Login" button.

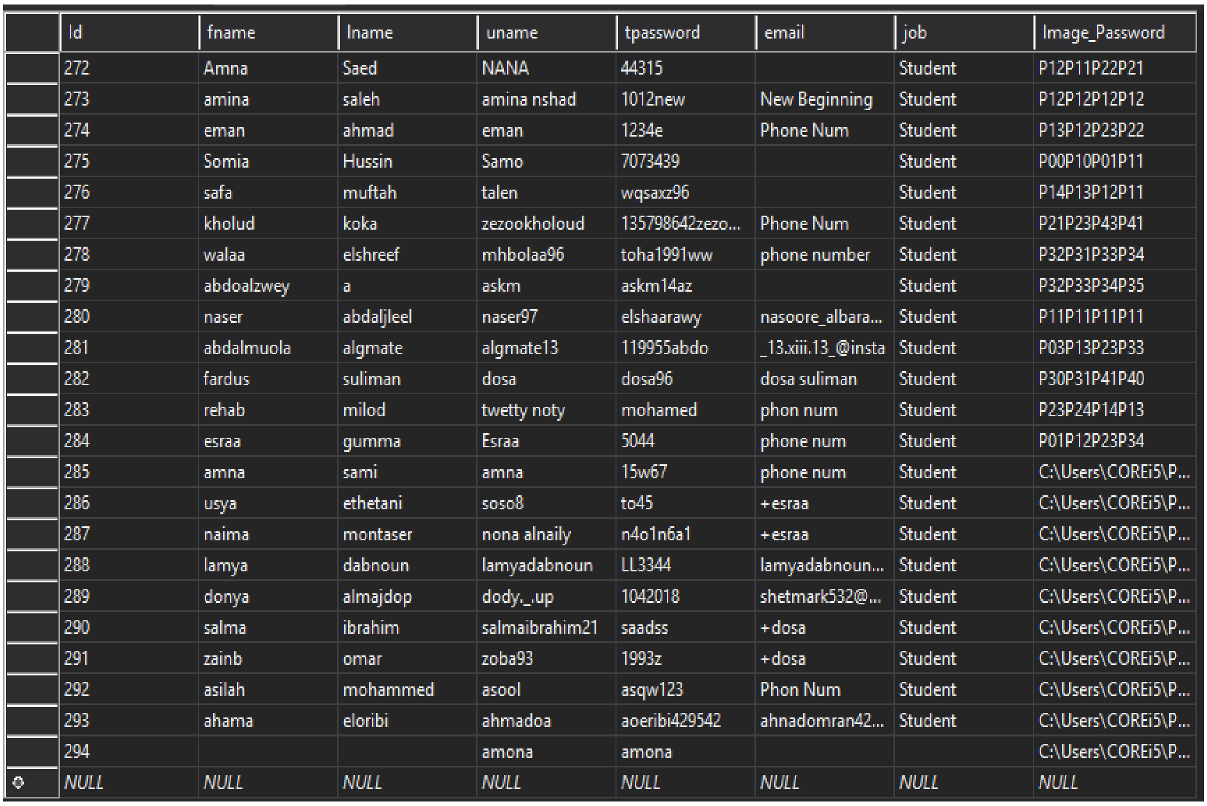
At this step begins the process of validating the data entered in the database, in the event of an error, the user will be notified about the error that entered. If all the data that entered are correct, the user will be notified that the login process was completed successfully through a message.

The purpose of the login phase is to obtain the results required in order to evaluate the image grid scheme that proposed in previous chapter based on usability and security terms as mentioned in Sections (2.5, 3.5).

4.4 Overview of the Database

As mentioned earlier MySQL database was used for storing the username and the graphical passwords of the users. Where MySQL database systems was chosen to use in this work because it is characterized by ease of use, stability and speed. It is also characterized by security, as MySQL system provides this feature with a complex system to access to the database, and a system to prevent any user from accessing the database Zaki, E. (2020)

One table just was created named 'users' with eight columns namely id, fname, lname, username, tpassword, email, job and image_Password. These stores the username, some optional information, the text password and the graphical password in separate columns. Where the graphical passwords will be stored as a combination of the image source with the name, and the name of selected cells. Figure 4.8 shows a screenshot of the database table.



Id	fname	lname	uname	tpassword	email	job	Image_Password
272	Amna	Saed	NANA	44315		Student	P12P11P22P21
273	amina	saleh	amina nshad	1012new	New Beginning	Student	P12P12P12P12
274	eman	ahmad	eman	1234e	Phone Num	Student	P13P12P23P22
275	Somia	Hussin	Samo	7073439		Student	P00P10P01P11
276	safa	muftah	talen	wqsaxz96		Student	P14P13P12P11
277	kholud	koka	zezookholoud	135798642zezo...	Phone Num	Student	P21P23P43P41
278	walaa	elshreef	mhbolaa96	toha1991ww	phone number	Student	P32P31P33P34
279	abdoalzwey	a	askm	askm14az		Student	P32P33P34P35
280	naser	abdaljleel	naser97	elshaarawy	nasoore_albara...	Student	P11P11P11P11
281	abdalmuola	algmate	algmate13	119955abdo	_13.xiii.13_@insta	Student	P03P13P23P33
282	fardus	suliman	dosa	dosa96	dosa suliman	Student	P30P31P41P40
283	rehab	milod	twetty noty	mohamed	phon num	Student	P23P24P14P13
284	esraa	gumma	Esraa	5044	phone num	Student	P01P12P23P34
285	amna	sami	amna	15w67	phone num	Student	C:\Users\COREi5\P...
286	usya	ethetani	soso8	to45	+esraa	Student	C:\Users\COREi5\P...
287	naima	montaser	nona alnaily	n4o1n6a1	+esraa	Student	C:\Users\COREi5\P...
288	lamya	dabnoun	lamyadabnoun	LL3344	lamyadabnoun...	Student	C:\Users\COREi5\P...
289	donya	almajdop	dody._.up	1042018	shetmark532@...	Student	C:\Users\COREi5\P...
290	salma	ibrahim	salmaibrahim21	saadss	+dosa	Student	C:\Users\COREi5\P...
291	zainb	omar	zoba93	1993z	+dosa	Student	C:\Users\COREi5\P...
292	asilah	mohammed	asool	asqw123	Phon Num	Student	C:\Users\COREi5\P...
293	ahama	eloribi	ahmadoa	aoeribi429542	ahnadomran42...	Student	C:\Users\COREi5\P...
294			amona	amona			C:\Users\COREi5\P...
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Fig. 4.8: Screenshot from the database.

4.5 Summary

This chapter presented the implementation of GUI_ image grid scheme, user registration window, login user window and the used database.

Chapter 5

Experiment and Results

5.1 Overview

This chapter discusses the experiment conducted to test the proposed system that based on the image grid scheme. The experiment was conducted on a random sample of the community, and the details of the case study conducted on this sample are mentioned in this chapter. The results were also analyzed in terms of usability and security, and compared with previous research. The system was implemented and ran on SAMSUNG laptop with 2.50 GHz Intel Core i5 CPU, hosted 4.0 GB of RAM and 14-Inch high-resolution screen.

5.2 Case Study

An experimental study was conducted to explore whether users would be satisfy about the use of the graphical password as an alternative to the text password, and whether it is more memorable of the text password. The results obtained from this experimental study helped in knowing whether the image grid scheme had fulfilled the requirements for which it was proposed; also, it helped in answering the research questions.

5.2.1 Participants of the Experiment

The total number of participants who were recruited is 293 participants, but only 225 participants completed the experiment to the end. The sample was from three different places: University of Benghazi - Faculty of Information Technology, University of Benghazi - Medical Faculties and Ajdabiya University - Faculty of Science. Table 5.1 list the number of participants with their categories, which was obtained through the first category in the questionnaire.

Category	Information classification	No. of participants
Age	Less than 18	3
	18 – 44	208
	45 – 64	14
Gender	Male	72
	Female	153
Education	High school graduate	38
	Undergraduate student	122
	College graduate	41
	Postgraduate student	13
	Master's/PhD degree	11

Table 5.1: Number of participants of the experiment.

5.2.2 Pre-stage of the experiment

1. The first step taken by the researcher in this experiment was to introduce the graphical password techniques, then explain the program and its purpose before starting the experiment for each group.
2. Some basic concepts, such as text password length, cells selections at creation the graphical password and the importance of memorizing the order of selection of these cells were clarified, in order for them to understand the policies they were going to face.
3. The participants were informed that the steps on how to use the program are available and can be accessed by simply clicking on the (?) sign on the top right of the system window in case they need help.
4. The participants were not given suggestions about how to choose a secure password or any mnemonic strategy. In addition, in the process of registering participants, they were allowed to choose their favorite image, as some of them sent the image to the used computer in the experiment.

5.3 Experiment

The participants were selected randomly, as they in the experiment were divided into 10 groups. Each group went through three sessions in order to evaluate the usability and the security. The user study was started with the first session for each group, where the sessions was in a laboratory environment.

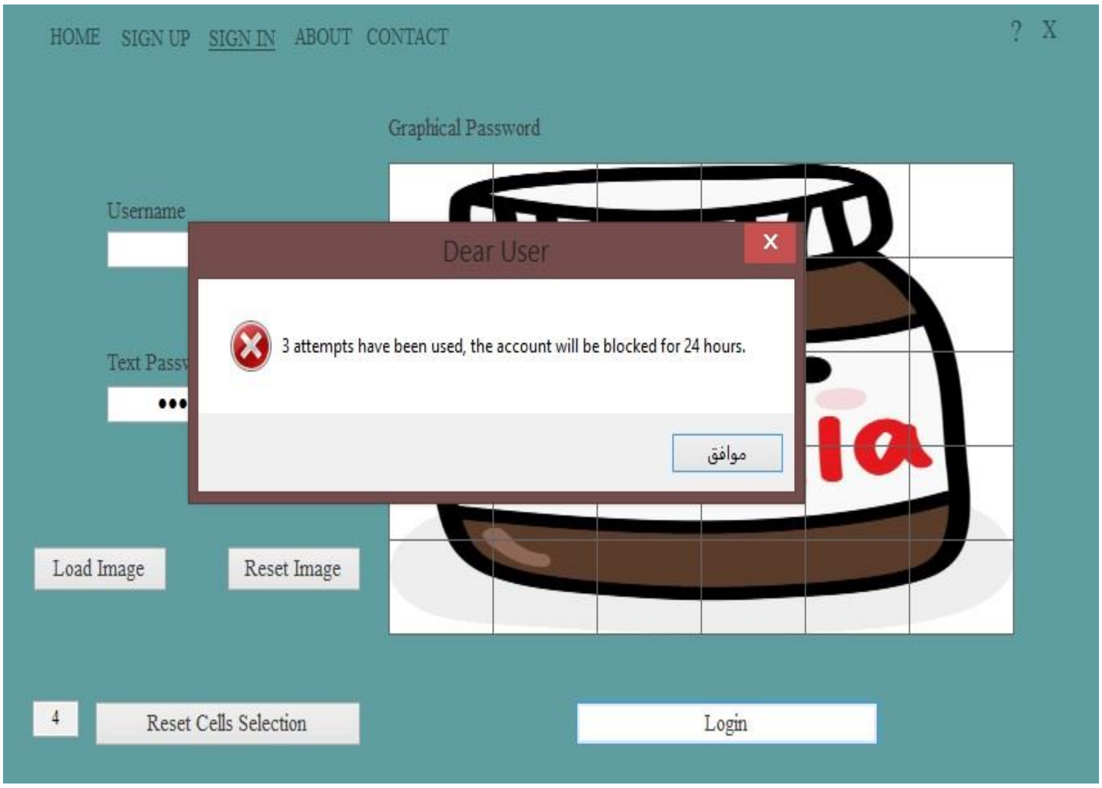
5.3.1 Session 1: Registration Stage

1. This session took about a month to gather enough participants, an explanation of how the program works was presented. In addition, participants were introduced to the purposes and procedures of the experiment by watching a 5-minute presentation using PowerPoint program.
2. Based on Section 4.3.1 and Figure 4.4 the participants create a graphical password and a text password.
3. In creating the graphical password, users had to select a distinct image, and they were allowed to use an image sent from their phones to the device that used in the experiment.
    a. To finish the process of creating the graphical password, the participants had to select cells from the image displayed as a grid.
    b. When the participant chose the image, it is divided into 5x6 grid and each cell in the image was given a default name.
4. To create a text password, users were required to enter at least eight characters with one number at least, as per the security requirements of the image grid scheme system on text passwords mentioned in Section 3.4.1. They were also asked not to choose password they had previously used.
5. When the participant clicks the OK button, the system will provide feedback on whether the username, the graphical password and the text password are valid or not.
    a. If the data entered is valid and correct, the user will be registered in the system.
    b. If one of the entered data is invalid, the user will be notified of the entered error with a message.

6. During this session, the time it took for each participant to create the text password and graphical password was recorded, as these results will be explained in results section.

5.3.2 Session 2: Login Stage

1. This session was started two weeks after the registration session for each group separately.
2. At the login session, the participants were asked to login, where they has to enter the username that was entered in the first session at the registration phase in the system.
3. Then enter the text password and the graphical password that they created previously.
4. Each user had three opportunities to enter the both passwords correctly. If the user filed the system will block the account for 24 hours as shown in Figure 5.1.



3 attempts have been used, the account will be blocked for 24 hours.

Fig. 5.1: Block account message window.

5.3.3 Session 3: Re-login and Filling Out the Questionnaire

1. The last session was two weeks after the second session, where participants were asked to enter their username, the graphical and the text password, which they generated in the first session and tested in the second session.
2. In this session, the time that took by each participant to remember the text password and the graphical password, and the number of attempts for each participant to login to his or her account were recorded.
3. The number of participants who forgot their text password and the number of participants who forgot their graphical password were recorded, as the participants who forgot their graphical password were not forgetting the image that they used, but rather forgetting the sequence of selecting the selected cells. These results are described in the Section 5.5.
4. After each group completed the third session, the participants were given a questionnaire to collect the results obtained from the experiment, and complete transparency and credibility was requested from the participants while filling out the questionnaire, also writing any notes that the researcher could use to develop the system.

5.4 Questionnaire Construction

The questions of the questionnaire were developed in a scientific way with the help of *Dr. Salem Al-Azraq* (2018), a doctor in the Department of Sociology - Faculty of Arts at Ajdabiya University. The questionnaire consists of twenty-two questions divided into four main categories as follows. The questionnaire will be attached to Appendix A.

1. General information: This is the first category of the questionnaire that includes general information about the participants from the point of view of age, gender and education. This information was presented at Table 5.1 in Section 5.2.1.
2. General Perspective towards password: This is the second category of the questionnaire and it consists of three questions, as it gives a clear view on how the participants deal with the password. The participant has to choose one of the following answers: Strongly disagree, Disagree, Not sure, Agree or strongly agree.
3. Evaluation towards the complete system of the graphical password system: In this category, evaluation of the complete system of the graphical password system is

also important in this questionnaire. Where it helps to know the participants' comments about the graphical password system in terms of the system's performance to know how they feel about the proposed system and whether they are satisfied with it or no. The answers range from completely dissatisfied, Dissatisfied, Not sure, Satisfied Completely to satisfied.

4. Evaluation towards the features of use within the graphical password system: This category consists of eleven questions, which generally include the user's acceptance of the proposed system and how easy it is to use and create the graphical password; it also includes easy learning and remembering questions. Each question has five answers describing the ease or difficulty of using the prototype ranging from very difficult, difficult, uncertain, somewhat easy, and very easy.

5.4.1 Data Collection

Data was collected from participants who answered the questionnaire regarding ease of password generation and recall-ability after a certain period of time, and compared with ease of remembering the text password. Whereas, data was collected immediately after participants completed the test task in Session 3. Where the users were required to use five-point scale ratings as shown in Table 5.2.

Completely Dissatisfied	Dissatisfied	Not Sure	Satisfied	Completely Satisfied
Very Difficult	Difficult	Not Sure	Not difficult	Very Easy
Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
1	2	3	4	5

Table 5.2: Five-point scale ratings.

5.5 Evaluation of the Results

The results are reported below by experimental phases: registration phase and login phase. The relevant questionnaire results are also reported for each phase.

5.5.1 Registration Phase Evaluation

In the registration phase, the participants generated two passwords, which are text password and graphical password. The time required to generate both passwords was measured, where the graphical password technique is a new technique to the participants. Table 5.3 and Figure 5.2 in respectively shows average time spent to generate text password and graphical password, and number of participants per category of average time taken. Which calculated for 200 out of 225 participants, as the participants did not take much time to generate the graphical password, while when creating the text password they took more time in thinking to try to fulfill the required security conditions.

Graphical password	1.15 Sec	1.30 Sec	2 Minutes	2.30 Sec
	87	73	32	8
Text password	46	65	58	31

Table 5.3: Average time to generate a password.

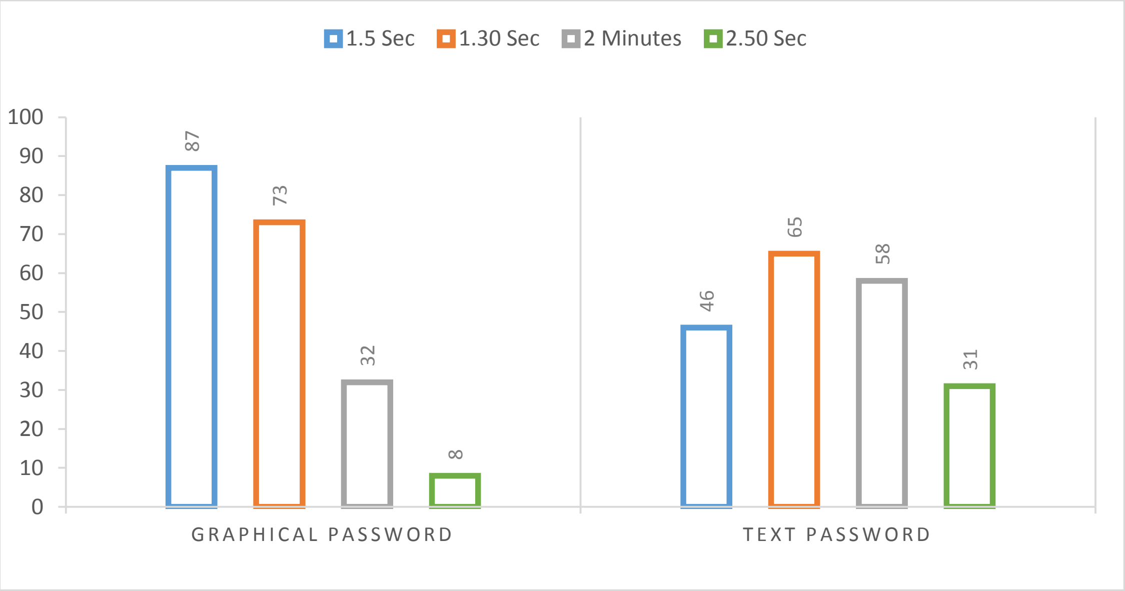


Fig. 5.2: Average time to generate a password.

5.5.1.1 Evolution the Simplicity of the System

Regarding to the simplicity of the prototype system, 89% of the participants indicated that they directly understood the program clearly, while the researcher repeated the explanation for 11% of the participants and used some examples. In addition, 30% of the participants were trained because they did not have a clear background on the use of computer programs because they were not specialized in information technology.

5.5.1.2 Evolution the Simplicity of the Graphical Password

In the questionnaire in Section III, the participants were asked a question about the ease of creating graphical password; the answers of the participants are as shown in Figure 5.3.

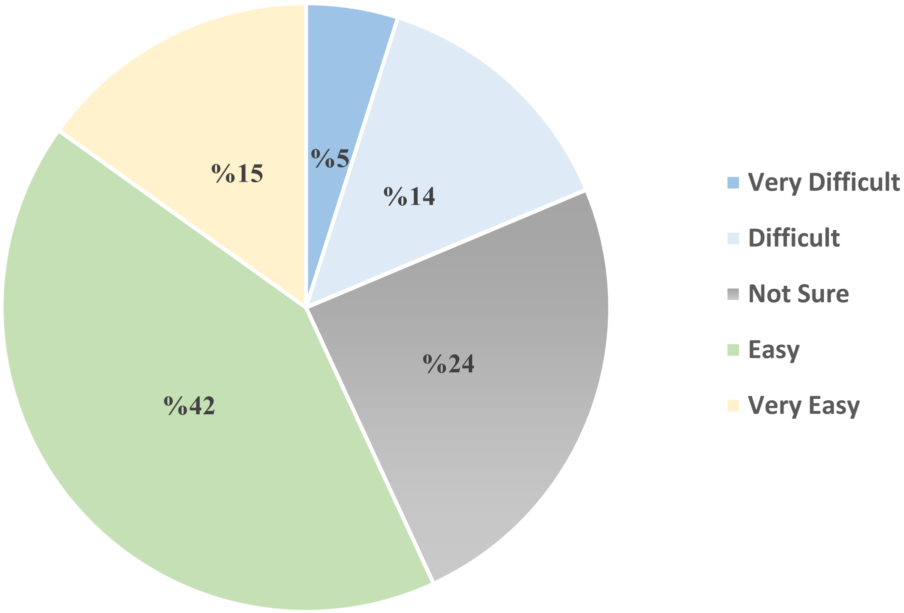


Fig. 5.3: Difficulty rate of graphical password generation.

Regarding the previous figure, 94 of the participants agreed that the creating of a new graphical password is easy process, and 34 participants answered that creating the graphical password is a very easy process, while the rest of the answers varied between difficult and neutral in creating the graphical password. Only 11 participants answered that it was a very difficult process.

5.5.2 Evaluating the Usability of the System

Usability relates to the "ease of use" of a product or system. Whereas, (International Standards Organization) ISO 9241-11 provides guidance on usability and defines it as follows:

“The extent to which the product can be used by specific users to achieve specific goals effectively, efficiently and with satisfaction in specific use contents” (ISO, 2021). Based on the ISO rating, usability revolves around three criteria by which the usability of a software can be measured , which are as follows:

- Efficiency: how much effort (time) does it require?
- Effectiveness: users can achieve what they need to do by using the product.
- Satisfaction: how do they feel about their interaction with the product?

In addition, usability can be assessed by quantitatively or qualitatively methods. Where quantitative metrics are particularly useful in evaluating the impact of design features on usability. While qualitative metrics provide insights into user satisfaction. In the next section, the ISO 9241-11 standards for software measurement are combined with the standards of quantitative and qualitative methods in order to obtain clearer and more accurate results.

5.5.3 Quantitative Metrics

Quantitative metrics are used to **evaluate the login phase** in order to measure the user's usability of the system. After linking metrics that commonly used in quantitative metrics with standards that developed by ISO 9241-11 standards, the proposed system was measured as the following:

5.5.3.1 Efficiency

In this research, password effectiveness was measured as the proportion of participants who logged into the proposed system in a given time period. Whereas, at the time of login to the image grid system, the number of participants who requested instructions on how to use the registration window and the login window was counted. Also, the number of their attempts to login to the system in the login session and re-login session that mentioned in Section 5.3 were counted. Where these data were illustrated in Table 5.4.

	Login			**Instruction**
	Attempt1	**Attempt2**	**Attempt3**	
Session 1: Registration stage	No need to login			69
Session 2: Login stage	187	36	2	34
Session 3: Re-login and filling out the questionnaire	150	48	27	2

Table 5.4: Participants who required instruction and their attempts.

Figure 5.4 shows the average login time in the third session, which is the re-login session. Where notice that the average login time fluctuates between good and weak, and noting that a few participants were unable to login because they forgot their password, which was the text password, and this is due to the difficulty of remembering texts and numbers for human memory compared to remembering images.

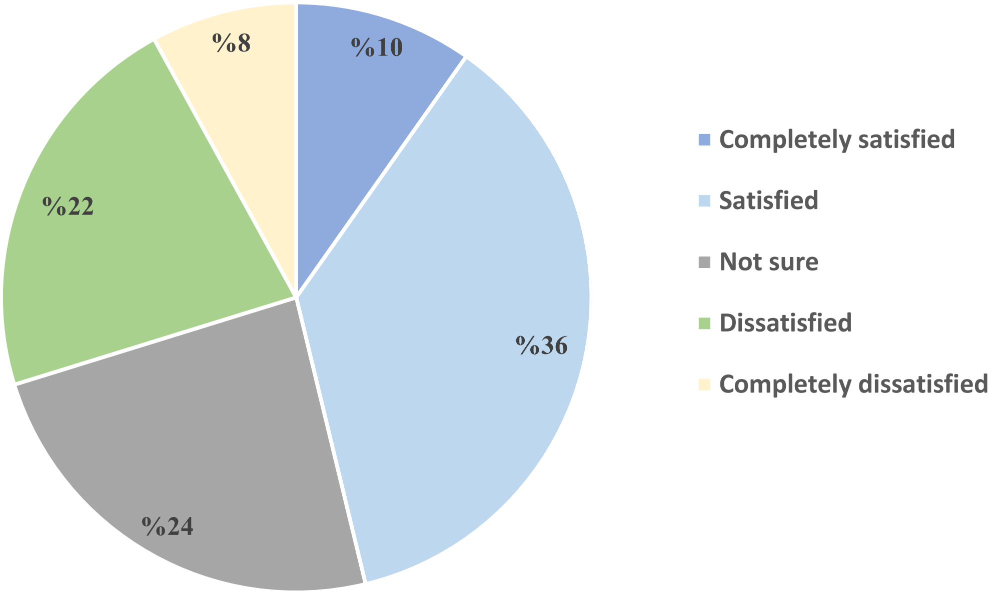


Fig. 5.4: The average of login time.

The data shown in the previous figure was obtained from the questionnaire in appendix A, from a question was asked to the participants in the third category about the time of login.

- ✓ Where 22 participants reported that they were being completely satisfied with the login time.
- ✓ 82 participants reported that they were being satisfied

- ✓ 54 participants whose answers were neutral with not sure.
- ✓ As 49, 18 are the rest of the participants and their answers were between dissatisfied and completely dissatisfied in respectively.

5.5.3.2 Effectiveness

The success rate for entering a password correctly is a common metric for effectiveness. Figure 5.5 shows participants' attempts to login to their accounts by the graphical password on the second and third sessions, which illustrating how well users remembered their password.

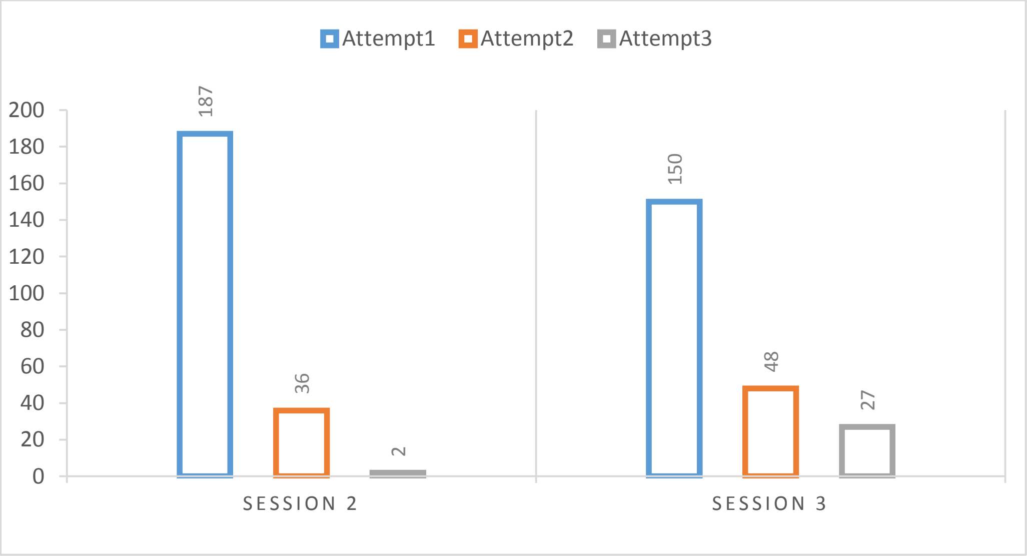


Fig 5.5: Participants' attempts to login.

From the previous figure, note that in the second session:

- ✓ 187 participants successfully enter to the system from the first attempt.
- ✓ 36 of the participants success from the second attempt
- ✓ Just two participants success in the third attempt.

In the third session:

- ✓ 150 participants successfully enter to the system from the first attempt.
- ✓ 48 of the participants success from the second attempt.
- ✓ 27 the participants success in the third attempt.

From these results, it is noted that the number of participants trying for second and third attempt in the third session has increased than in the second session, where the difficulty was in remembering the order of the selected cells. Some participants did not focus on the order of the selected cells in the registration phase in the first session, which led to confusion remembering their arrangement.

5.5.3.3 Memorability

The ability to remember can be supported by making use of a user's pre-existing knowledge rather than requiring users to memorize new or random information. As this image grid scheme was created based on the idea of the users using their favorite image, and therefore the user will not need to search an image from a group of images.

Figure 5.6 shows the results obtained from asking question in the section iv in the questionnaire, which shows that the rate of participants who were able to remember the graphical password is better than the rate that they remember the text password. Where this result boost the previous research that demonstrated that a person can remember images more easily than alphanumeric strings, which making the proposed technique in this research a good alternative to text password in terms of usability.

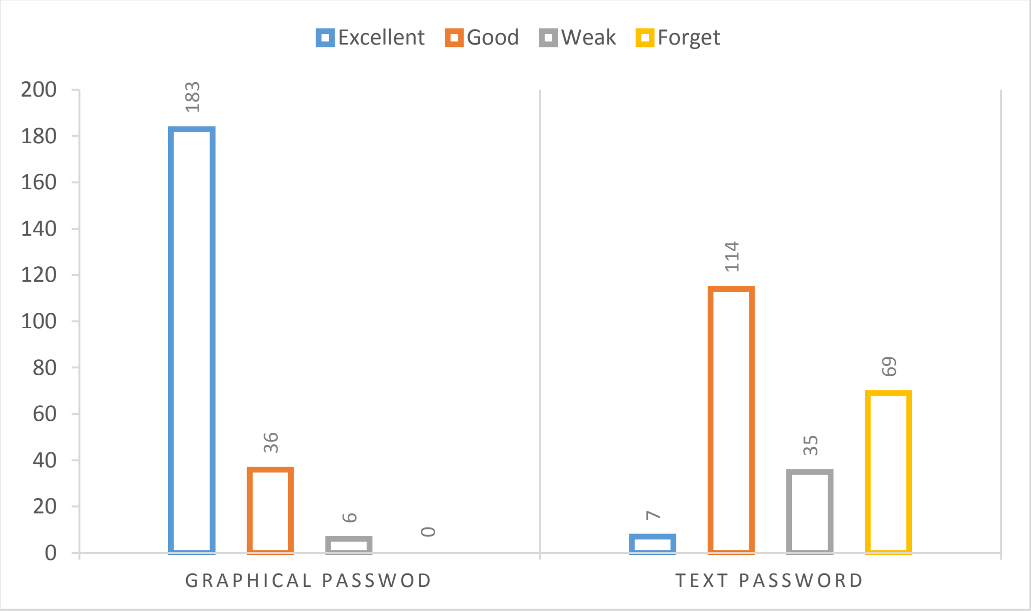


Fig. 5.6: Comparison of text and graphical password memorability.

5.5.4 Qualitative Metrics

Regarding qualitative methods, insights on user satisfaction were collected and determined in Section iv of the questionnaire. Where the results were as follows:

Overall program quality assessment	Repetition of answer
Very easy	80
Easy	108
Not sure	34
Difficult	2
Very difficult	1

Table 5.5: User satisfaction.

From Table 5.5 can notice that most of the users choose satisfied answer, which means that the majority are satisfied with the system. Figure 5.7 shows the percentage of all system evaluation answers to the user perspective question of the graphical password system. It notes that the participants are 48% satisfied with the graphical password system and 36% very satisfied and that means 84% of the users are satisfied with the proposed system.

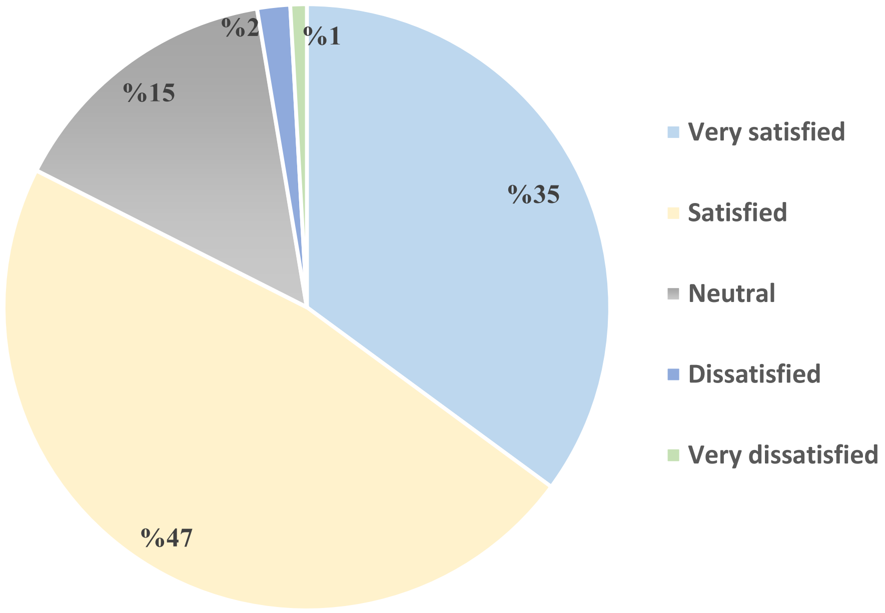


Fig. 5.7: Percentage of user satisfaction of software quality.

5.5.4.1 Solution of Storage Defects in Image Grid Scheme

As mentioned in Section 2.5.1.4, usability issue facing the graphical password techniques is the storage defects. Whereas, most of the existing schemes have storage defects; where when storing images in the database, the size of the database becomes large, resulting in slow storage and data retrieval from it, which generates boredom to the user and making the user to returns to traditional authentication processes (text passwords). In the proposed scheme (image grid scheme), will not be stored images in the database as previously mentioned, as the graphical password will be stored as a string of letters and numbers, so the proposed scheme will not be exposed to storage defects.

5.5.5 Security Issues

This section discusses the results of the Image Grid scheme's resistance to the most important attacks to which graphical password techniques can be exposed, which were mentioned in Section 2.5.2.

5.5.5.1 Brute Force Attack

The main defense against brute force attacks is to have a large enough password space. Throughout this work, the term password space will be used to describe the strength of passwords. The password space of recognition-based techniques largely depends on the size of the content. The password space of recognition-based techniques, as cited by *Xiaoyuan* (2006), is a function of the total number of images:

Password _ space = f (s x n)

Where S stands for the number of views/validation rounds while N stands for the number of images per page.

However, in the image grid scheme the password space will not depend on the image or the image content. Because, as indicated earlier, the password will not be stored in the database as an image, it will be stored as a text string. Where the password will consist of two segmentation, the first segment is the source and label of the chosen image and the second is the default label of the chosen cells that the system will assign to them.

In this research, the graphical password space will be computed as computing the text password space, which is mentioned in the chapter 2. The text-based passwords have a password space of 94^N, where N is the length of the password and 94 is the number of printable characters excluding SPACE button. Where the system will require the user to choose an image where its label consists of a number of characters not less than 25 characters. The system will then create a default label for each chosen cell, which will consist of two number and one letter.

Thus, for example, assume that the user chooses only two cells to complete the password, the number of passwords will be as follows:

Password space = number of characters of the chosen image's label + number of characters of the chosen cell's label.

Password space= 25+ 3+ 3= 31

Therefore, if there are 94 alphanumeric and type-able symbols excluding SPACE on the standard keyboard the password space for the previous example will be $94^{31} = 1.47\times10^{61}$.

Consequently, due to the large password space, it is hard to carry out brute force and dictionary attacks for this proposed scheme.

5.5.5.2 Shoulder Surfing Attacks

Most of the graphical password schemes are vulnerable to shoulder surfing attacks. In the image grid scheme, a feature has been added to the image, which is divide the image as a grid consisting of 30 cells, and the user has to choose 4 cells to complete the process of generating the graphical password, so if the attacker knows the chosen image, it is difficult to know the four selected cells.

5.5.5.3 Dictionary Attack

Dictionary attack is a method of breaking into a password by systematically entering every word in a dictionary as a password. Thus, since the image grid scheme is based on recognition-based techniques where it only involves mouse input rather than keyboard input, dictionary attacks against this type of graphical password are difficult to implement.

Moreover, in the event that the attacker has discovered that the graphical password is stored in the database as a text string and tried to systematically enter each word in the dictionary, the attacker will not be able to hack the password easily because it have a large password space.

5.5.5.4 Spyware

Spyware is malware designed to get into your computer to track the movement of the mouse to find out the password. Mouse movement alone is not enough to crack graphical passwords, as this information should be related to application information, such as window position and size, as well as timing information. Also, the image grid system is an offline system, as a result it is difficult to be exposed to such type of attacks.

5.5.5.5 Predictability

The chances of creating weak password are high in recognition-based password. Some studies by *Davis* (2004) showed that the user's choices of graphical passwords are often predictable. Such as the pass-image scheme, which allows users to use their own images would make the password even more predictable, especially if the attacker is familiar with the user. Where the image grid scheme is based on that existing scheme (Pass-Image scheme).

Therefore, while allowing the users to select their own images makes the password an easy target, in the image grid scheme there is another step should the user followed it, which is the choosing of a group of cells to complete the creation of the password, this step makes the password more secure. Consequently, if the attacker knows the image, it is difficult to discover the selected cells and the order in which the user selects these cells, thus the guessing will be very difficult in this case. Therefore, this system has the property of defending against this type of attack.

5.5.5.6 Social Engineering

While social engineering attacks rely on human interaction and are very similar to guessing attacks, this image grid scheme can be difficult to crack with this type of attack. Since no matter how the attacker is familiar with the user, he will never guess the order of the user selection of cells, and even if the user shares his chosen cells with someone, it is difficult to share the order.

5.6 Comparison of Various Schemes

Based on Table 2.1 which mentioned in Section 2.4 , the proposed image grid scheme can be compared with the existing schemes that it was derived as follows:

Scheme / Attacks	Image Grid Scheme	Pass-Image Scheme	Pass-Point Scheme
Brute force	No	Yes	No
Shoulder surfing	No	Yes	Yes
Dictionary	No	No	No
Predictability	No	Yes	No
Spyware	Yes	Yes	Yes
Social Engineering	No	Yes	No
Storage Defect	No	No	No
Tedious Process	No	No	Yes

Table 5.6: Comparison of various schemes.

5.7 Summary

This chapter presented experiment for 225 participants and verify that the users were satisfied with the use of the graphical password as an alternative to the text password, where the proposed image grid system was more user-friendly and memorable.

In addition, the three sessions that the participants went through in the experiment were illustrated.

The data that obtained from the questionnaires were explained and clarified with the help of a set of figures, tables and charts.

At the end of the chapter, the system was evaluated and assessed whether it met usability metrics. Also, evaluated security metrics and verifying that the image grid scheme it provided defense mechanisms against common attacks against graphical password techniques.

Chapter 6

Conclusion and future work

6.1 Overview

This chapter summaries the advantages provided by the Image Grid Scheme, review the principal contributions, the conclusion of the research and presents recommendations for the future works.

6.2 Contributions of this Research

This work has contributed to introduce solutions in the area of graphical password techniques by conducting thorough review and comparison of existing schemes. New scheme then developed to allow the stated aims and objectives to be achieved.

Specifically, this research has introduced three questions in Chapter 1, which have facilitated the creation of the proposed scheme (image grid scheme), which were answered as follows:

Are graphical passwords as secure as text passwords?

Many research and schemes have been presented in the field of graphical passwords to prove that they are more secure than text passwords, but in each scheme that provides high security compared to text passwords, there are shortcomings in terms of ease of use.

Therefore, this study was to investigate and solve the security deficiencies in the previous schemes then presented solutions to these deficiencies, where the image grid scheme did not focus on these security shortcomings and excluded the importance of ease of use, as it balance between providing high security with providing ease of use. After the obtained results discussed in Chapter 5 Section 5.5, the system that based on the new proposed graphical password scheme (image grid scheme) is considered to be as secure as the text password.

How does a graphical password system measured?

The most common metrics for measuring passwords were discussed in the previous chapter, as password systems can be measured in two respects: usability and security.

Under each item are the most important metrics that can be used to measure graphical password systems. These metrics is discussed in Chapter 5 Section 5.5, where the usability metrics are:

- ✓ Efficiency.
- ✓ Effectiveness.
- ✓ Memorability.
- ✓ User's satisfaction.
- ✓ Storage defects.

The security metrics are:

- ✓ Brute force.
- ✓ Shoulder surfing.
- ✓ Dictionary.
- ✓ Predictability.
- ✓ Spyware.
- ✓ Social Engineering.

How far is the user’s acceptance to the new technology?

The results that obtained and discussed in Chapter 5 in Section 5.5.4 show that most users have been satisfied and accepted the using of the graphical passwords instated of text passwords, because it is an easy-to-use and memorable technique especially for people who have many accounts.

6.3 Conclusion

This research included a review on the authentication methods that exist in information security systems, where the research focused on two authentication techniques under the item of knowledge-based authentication techniques (text password techniques - graphical password techniques).

1. A comprehensive study of the current graphical password schemes, especially those that depend on recognition techniques, was conducted.

   a. The usability features of specially those of recognition-based technique schemes were studied in order to obtain the best usability features, which assisted in creation the image grid scheme.
   b. The comprehensive study also focused on the most important weaknesses in the existing schemes on graphical password technique, and the shortcomings of these schemes were address.

2. This work aim to introducing a new graphical password scheme that utilizes the usability features that obtained from the comprehensive study, which gained from Pass-Image Scheme that depends on users choosing their favorite image as a password, while increasing defense mechanisms against the attacks that can be this scheme exposed to it.
3. The Pass-Image scheme has been improved by adding new feature, which is divided the chosen image to 5x6 grid.
   a. The new feature depends on the user's selection of a group of cells from the chosen image. This feature is considered as a cued recall-based technique in graphical password techniques, whereby when the selected image by the user is displayed as a grid it will be easier for the user to remember the selected cells.
4. The image grid scheme is presented as a hybrid scheme, which combines the recognition-based technique and the recall-based technique.
5. An experimental system was designed based on the image grid scheme by Visual Basic 2013 as a development environment, Visual Basic.net as a programming language and My SQL Server as a database.
6. An experiment was conducted using the image grid system on a random sample of the community, where the experiment was conducted in its three sessions by 225 participants out of 294 people who applied for the experiment.
   a. The participants were divided into 10 groups, each according to the place and the time in which each participant was chosen to be a participant in the experiment.
   b. The sample was from three different places: Faculty of Information Technology - University of Benghazi, Medical Colleges - University of Benghazi and Faculty of Science - University of Ajdabiya.
   c. Direct observation, test and questionnaires were used as study tools in this scientific research to evaluate usability and security metrics of the image

grid system, where the questionnaire focuses on evaluating the entire system and usability metrics.

7. By analyzing the questionnaire results that were measured by quantitative and qualitative methods, the image grid system bears the usability metrics that were identified as the objective of this work.
    a. Where 183 participants answered in the questionnaire questions that the graphical password is better to remember than the text password, while only 6 participants answered that it is difficult to remember compared to the text password.
    b. In section iv of the questionnaire, participants were asked to evaluate the image grid system from several aspects and the results were: 80 participants answered that the system is very easy, 108 participants answered that the system is easy, 34 participants answered with a neutral answer, two participants answered that the system is difficult, and one participant answered that the system very difficult.
8. Previous results showed that the graphical password is an easy-to-learn and easy-to-use technique whether the user knows how to use the computer or not, and the majority of participants preferred it as an alternative to the text passwords.
9. Form Section 5.6, the results also showed that the proposed system that based on the image grid scheme provides a good defense mechanism against the attacks those graphical password techniques exposed to it and provides better security than that provided with using text passwords.
10. The results of evaluating usability and security metrics that mentioned in Section 5.5 and 5.6 respectively, which showed that the proposed Image Grid scheme has obtained the objective of this work, which is the balance between the usability and the security.

6.4 Future works

There are several extensions could improve the performance of this work:

- Improvement the system to be an online system as well as a mobile application with more security against the spyware.

- Storing the chosen images by the users on the server, so that when the user opens the system from anywhere and from any device, the users will find their chosen image.

REFERENCES

Abdalkareem, Z, A., Akif, O, Z. and Abdulatif, F, A. (2021) "Graphical password based mouse behavior technique" *Journal of Physics: Conference Series,* 5th International Conference on Electronic Design (ICED).

Abhijith, S., Soja, S., Sreelekshmi, K,. Samjeevan and Sneha, M. (2021) "Web based Graphical Password Authentication System" *International Journal of Engineering Research & Technology (IJERT),* Vol. 9, no.7. pp 29.

Akula, S. and Devisetty, V. (2004) "Image based registration and authentication system" in Proceedings of Midwest Instruction and Computing Symposium.

Ariffin. N, A. Abdulhalem, A, A and Husin, N, A (2021) " Text and Image: A new hybrid authentication Scheme" *Journal of Physics: Conference Series*.

Bianchi, A., Oakley, I. and Kim, H. (2016) "Pass-BYOP: Bring Your Own Picture for Securing Graphical Passwords" *IEEE Transactions on Human-Machine Systems*, Vol. 46, no. 3.

Biddle, R., Chiasson, S. and Van Oorschot, P. (2012) "Graphical passwords: Learning from the first twelve years" *ACM Compute Surveys,* vol. 44, no. 4.

Bicakci, K., Atalay, N.B., Yuceel, M., Gurbaslar, H. and Erdeniz, B. (2009) "Towards Usable Solutions to Graphical Password Hotspot Problem", *IEEE International Computer Software and Application Conference*.

Blonder, G. E. (1996) "Graphical passwords" in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States.

Bonneau, J. and Shutova, E. (2012) "Linguistic Properties of Multi-word Passphrases" In Financial Cryptography and Data Security, Springer.

Brostoff, S and Sasse, M. A. (2004) "Are Pass-faces more usable than passwords: a field trial investigation" in People and Computers XIV- Usability, UK: Springer-Verlag.

Chiasson, S., Biddle, R. and Van Oorschot, P.C. (2007) "Graphical Password Authentication Using Cued Click Points" In European Symposium on Research in Computer Security (ESORICS).

Chiasson, S., Forget, A., Biddle, R. and Van Oorschot, P. C. (2008) "Influencing Users towards Better Passwords: Persuasive Clicked Points" *In 8th proceedings of the 22nd*

British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, vol.1.

Christopher, R, C. and Noordean, H (2017) "A Survey on Graphical Password Authentication System and their Security Issues" *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET),* Vol. 6, no. 6.

Davis, D., Monrose, F. and Reiter, M. (2004) "On user choice in graphical password schemes" In Proceedings of the 13th Usenix Security Symposium. San Diego, CA.

Dhamija, R. and Perrig, A. (2000) "Deja Vu: A User Study Using Images for Authentication" In Proceedings of 9th USENIX Security Symposium.

Dhiviyaa, S., Rakshitha, K. R and Vijayabharathi, R (2018) " Authentication System– Overview of Graphical Password" *International Research Journal of Engineering and Technology (IRJET),* vol.5, no. 2, pp 449-455.

Dunphy. P. (2012) "Usable, Secure and Deployable Graphical Passwords" Ph. D. thesis, School of Computing Science, Newcastle University, United Kingdom.

Elaurd, M. Maetz, Y. and Alessio, D. (2011) "Action-Based Graphical Password: Click-A-Secret" *IEEE International Conference on Consumer Electronics*.

Fatemeh, G (2020) "Secure graphical password based on cued click points using fuzzy logic" wileyonlinelibrary.com/journal/spy2.

Gao, H. C., Ma, L. C., Qiu, J. H. and Liu, X. Y. (2011) "Exploration of hand based Graphical Password Scheme" *Proceedings of the 4th International Conference on Security of Information*.

Gao, H.C., Liu, X.Y., Wang, S. and Dai, R (2009) "A New Graphical Password Scheme Against Spyware by Using CAPTCHA*" In Proceedings of the Symposium on Usable Privacy and Security*.

Gasser, M. (1975) "A Random Word Generator for Pronounceable Passwords" Technical Report.

Harasimowicz, H, R. (2018) "ACRAS- A hybrid graphical user- authentication system" Master degree thesis, cyber security engineering, University of Washington.

Herley, C. and Van Oorschot, P. C. (2012) "A Research Agenda Acknowledging the Persistence of Passwords" *IEEE Security & Privacy*, vol. 10, no.1.

Heera, K., Anusuya, M., Kaviyaa, V., Lavanya A, K, and Shanthi, R. (2020) "GRAPHICAL PASSWORD AUTHENTICATION FOR BANKING SYSTEM"

International Research Journal of Engineering and Technology (IRJET), Vol. 07, no.02. pp: 3228- 3231.

Jali, M. Z. (2011) "A Study of graphical alternatives for users' authentication" Ph.D. thesis, School of Computing and Mathematics Faculty of Science and Technology.

Jansen, W. (2004) "Authenticating Mobile Device Users through Image Selection" The National Institute of Standards and Technology.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. and Rubin, A (1999) "The Design and Analysis of Graphical Passwords" *In Proceedings of the 8th USENIX Security Symposium*.

Kausar, T., Pathan, N. and Dubey, S (2018) " Review of Multimedia Graphical Grid Based Text Password Authentication for Advanced User" *International Journal of Scientific Research in Science and Technology*, vol. 4, no.5, pp 1824-1830.

Komanduri, S., Shay, R., Cranor, L. F., Herley, C. and Schechter, S. (2014) "Telepath-words: Preventing weak passwords by reading users' minds" In Proceedings of the 23rd USENIX Security Symposium. USENIX Association.

ISO 9241-11 (2018)"Ergonomics of human-system interaction- Part 11: Usability Definitions and concepts" last access: 19.8.2021 – URL: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en.

Lau, S., Siena, S., Pandey, A., Sosothikul, S., Cranor, L. F. and Shay, R. (2014) "Exploring the Usability of Pronounceable Passwords" (Poster). In Proceedings of the 10th Symposium on Usable Privacy and Security.

Li, Z., Sun, Q., Lian, Y. and Giusto, D. D. (2005) "An association-based graphical password design resistant to shoulder-surfing attack" *IEEE International Conference on Multimedia and Expo*.

Lin, D., Dunphy, P., Olivier, P. and Yan, J. (2007) "Graphical passwords & qualitative spatial relations" *in Proceedings of the 3rd Symposium on Usable Privacy and Security,* Vol. 229.

Liu, X. Y., Qiu, J. H., Ma, L. C. and Gao, H. C. (2011) "A Novel Cued-Recall Graphical Password Scheme" *International Conference on Image and graphics(ICIG).* Vol. 6.

Mali, S. and Rathanavel, V. (2017) "Graphical Password as an OTP" *International Journal of Engineering and Computer Science ISSN*, vol. 6, no. 1.

Man, S., Hong, D. and Mathews, M (2003) "A shoulder-surfing resistant graphical password scheme" in Proceedings of International conference on security and management. Las Vegas, NV.

Menezes, A. J., VanOorschot, P. C. and Vanstone, S. A. (1996) " Handbook of Applied Cryptography" Webster Professor of Electrical Engineering and Computer Science Massachusetts Institute of Technology.

Nelson, D., Reed, V. and Walling, J. (1976) "Pictorial superiority effect" *J.Exp. Psychol.: Human Learning Memory*, vol. 2, no. 5.

Notoatmodjo, G. (2007) "Exploring the 'Weakest Link': A Study of Personal Password Security" Master’s thesis, The University of Auckland, New Zealand.

Ologundudu, B, T. and Sakpere B, A. (2021) "USABILITY STUDY ON TEXTUAL AND GRAPHICAL PASSWORDS" *The Proceedings of the Nigerian Academy of Science*, Vol 14, no 1, pp 82- 100.

Patra, K., Nemade, B., Mishra, D, P. and Satapathy, P, P (2016) "Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features" Procedia Computer Science, open access article under the CC BY-NC-ND license.

Pass-faces "Two Factor Authentication for the Enterprise" last access: 15 June 2021, URL: http://www.realuser.com .

Passlogix, last accessed: 17 June 2021, URL: www.passlogix.com .

Ribdawi, G (2018) "Software Engineering" publication of the Syrian Virtual University.

Sananse, S. S and Karwande V. S. (2020) "Graphical Systems Authentication Using ASCII" *International Journal of Advanced Scientific Research and Engineering Trends ISSN*, vol. 4, no. 6, pp. 24-30.

Snodgrass, J., Volvovitz, R. and WALFISH, E. (1972) 'Recognition memory for words, pictures, and words + pictures' *Journal of Psychological Science*, vol. 27, no. 6.

Sobrado, L and Birget, J, G (2005) "Shoulder-surfing resistant graphical passwords".

Stobert, E. A. (2015) "Graphical passwords and practical password management" Ph. D. thesis, Carleton University Ottawa, Ottawa.

Suo, X., Zhu, Y. and Owen, G. (2005) "Graphical Passwords: A Survey" Department of Computer Science, Georgia State University.

Syukri, A, F., Okamoto, E. and Mambo, M. (1998) "A User Identification System Using Signature Written with Mouse " *in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438)*, pp. 403-441.

Tahmina, I, S., Taslima, A., Muthmainna, M., Farida, C. and Md, S, F. (2020) "A Systematic Literature Review of Graphical Password Schemes" *Journal of Computing Science and Engineering,* Vol. 14, No. 4, pp. 167.

Takada, T. and Koike, H. (2003) "Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images" *In Human-Computer Interaction with Mobile Devices and Services.* Vol. 2795. Springer, Verlag, GmbH.

Thorpe, J and Nali, D. (2004) "Analyzing User Choice in Graphical Passwords" Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada.

Thorpe, J. and Oorschot, V. P. C. (2004) "Towards Secure Design Choices for Implementing Graphical Passwords" in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona.

Tiller, L. N. (2020) " Account Recovery Methods for Two-Factor Authentication (2FA): An Exploratory Study" A Thesis Submitted to the Faculty of Old Dominion University in Partial Fulfillment of the Requirements for the Degree of Master of Science.

Yan, J., Blackwell, A. F., Anderson, R. and Grant, A. (2004) "Password memorability and security: Empirical results" *IEEE Security and Privacy,* vol. 2, no. 5.

Varenhorst, C. (2004) "Pass-doodles: A lightweight authentication method". MIT Research Science Institute.

Vorster, J. S., Van Heerden, R. P. and Irwin, B. (2016) "The Pattern-richness of Graphical Passwords" Proceedings of the 15th International Information Security South Africa Conference (ISSA).

Wash, R., Rader, E., Berman, R. and Wellmer, Z. (2016) "Understanding Password Choices: How Frequently Entered Passwords are Re-used across Websites" Symposium on Usable Privacy and Security (SOUPS).

Wayne, J., Serban, G., Vlad, K., Rick, A. and Ryan, S., (2003) "Picture password: a visual login technique for mobile devices" NIST NISTIR 7030.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. and Memon, N. (2005) "Authentication using graphical passwords: Effects of Tolerance and Image Choice" In Proceedings SOUPS '05 symposium on Usable privacy and security.

Wiedenbeck., S., Waters, J., Birget, J. C., Brodskiy, A. and Memon, N. (2005) "Pass-Points: Design and Longitudinal Evaluation of a Graphical Password System" *International Journal of Human-Computer Studies*, vol. 63, no. 1-2.

Xiaoyuan, S. (2006) "A Design and Analysis of Graphical Password." Thesis, Georgia State University. Last access 2020: URL: http://scholarworks.gsu.edu/cs_theses/27 .

Zaki, E. (2020) "What is MYSQL and what are its uses, disadvantages and advantages" last access 4 August 2021 – URL: https://www.techno-4u.com/.

Zhao, H. and Li, X. (2007) "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme" 21st International Conference on Advance Information Networking and Application Workshops. IEEE Computer Society.

Appendix A

System Evaluation Questionnaire

APPENDIX A: SYSTEM EVALUATION QUESTIONNAIRE

Questionnaire of User Satisfaction

Dear user…

Thank you very much for completing this survey. Your response will be highly appreciated and it will help us greatly to evaluate and to improve our system.

Section I

General information about users

Please tell me just a bit about yourself

Your Age

□ Under 18 □ 18 - 44 □ 45 – 64

□ 65 or over □ I prefer not to respond

Your Gender

□ Female □ Male

Your Education Level

□ High school graduate □ Some coursework □ Undergraduate student

□ College graduate □ Postgraduate student □ I prefer not to respond

Section II

General Perspective towards password

	Strongly disagree	Disagree	Not sure	Agree	Strongly agree
I prefer to use easy password	□	□	□	□	□
I prefer to use text password in my applications	□	□	□	□	□
I prefer to use graphical password	□	□	□	□	□

Section III

Evaluation towards the whole system of the Graphical password system

How satisfied you are with the Graphical password system as general in terms of:

(For each of the following questions, please tick the answer that best expresses your opinion)

	Completely dissatisfied	Dissatisfied	Not sure	Satisfied	Completely satisfied
Login time	□	□	□	□	□
System response time	□	□	□	□	□
Clarity	□	□	□	□	□
Ease of use	□	□	□	□	□
Overall performance	□	□	□	□	□

Section IV

Evaluation towards the usability features inside the Graphical password system

Ease of use, ease of learn and ease of memorizing the password of the graphical password system

Please rate the "usability" of each part of the system based on how easy or difficult it was to perform, and tick the appropriate box:

	Very difficult	Difficult	Not sure	Easy	Very easy
Using the mouse	□	□	□	□	□
Using the keyboard	□	□	□	□	□
Ease to creation of graphical password	□	□	□	□	□
Ease to choose the images	□	□	□	□	□
Limited number of images	□	□	□	□	□
Ease to memorize	□	□	□	□	□
The system is ease to learn	□	□	□	□	□
The system is simple terminology	□	□	□	□	□
The window layout is well designed	□	□	□	□	□
The window is properly formatted and understandable	□	□	□	□	□
The system has improved my understanding of the graphical password	□	□	□	□	□

In your own words, what are the things that you would most like to improve in the program?

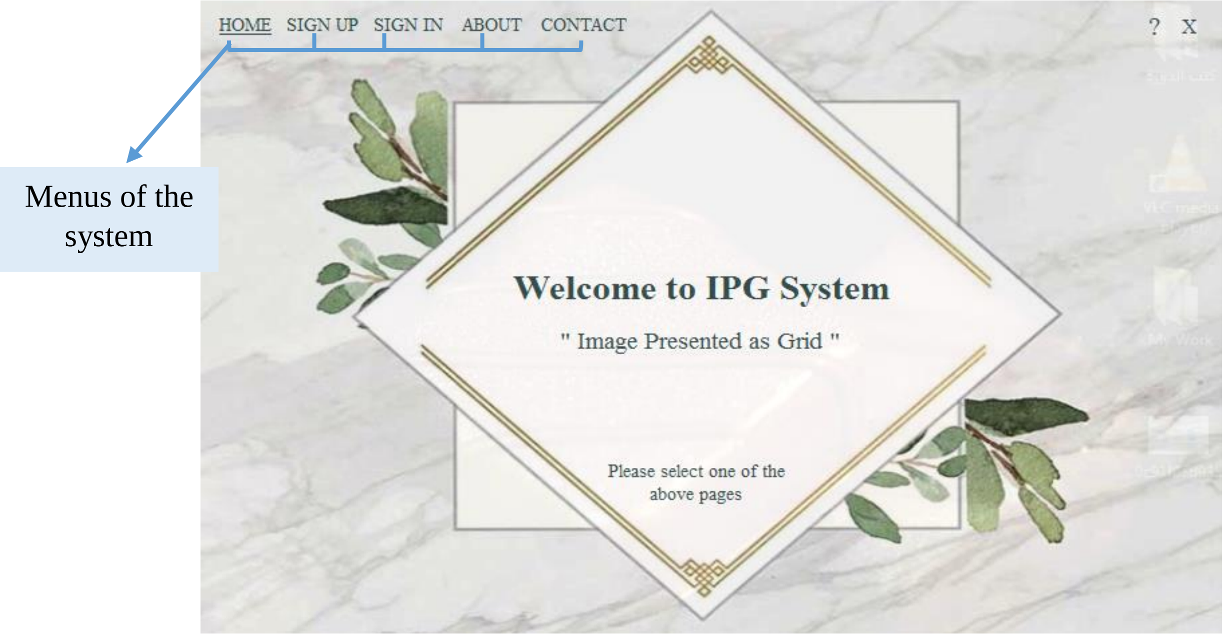
Thank you for your feedback it is highly appreciated

Appendix B

System's Interfaces

System's Interfaces

When the user enters the system, the following window will appear:



Menus of the system

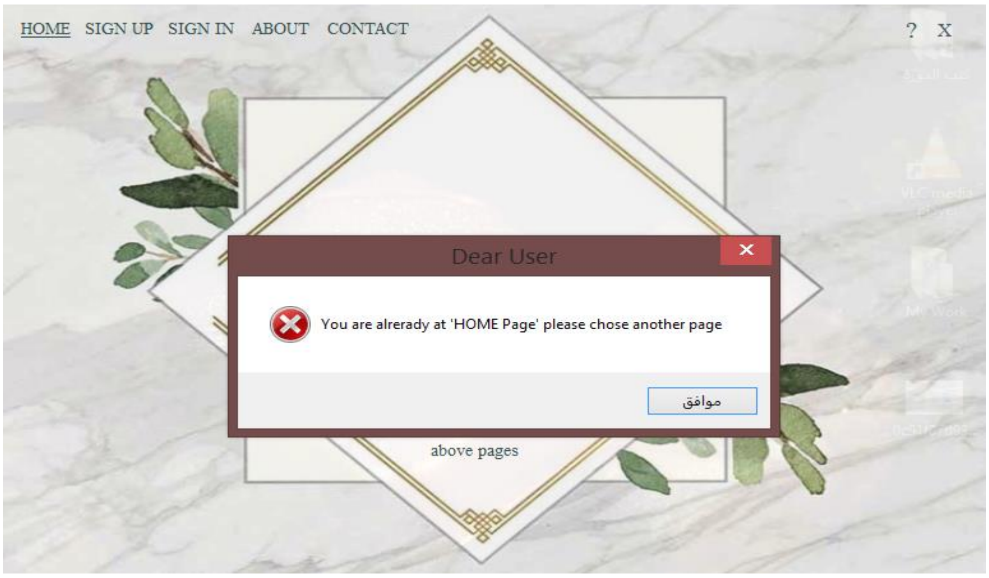
Welcome to IPG System

" Image Presented as Grid "

Please select one of the above pages

Main window.

If the user is in the "HOME" window and press "HOME" button, the system will notify the user by message shown in the following window.



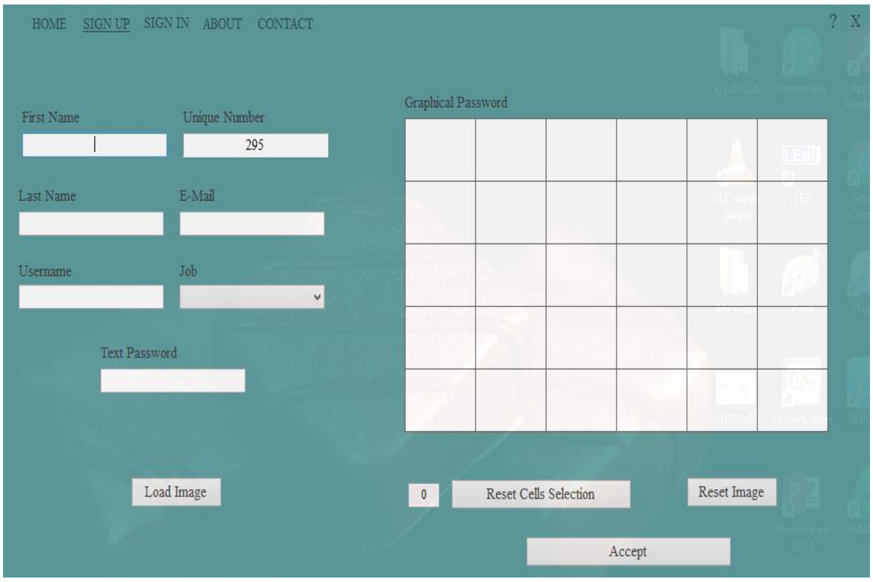
Dear User

You are alrerady at 'HOME Page' please chose another page

above pages

Warning message.

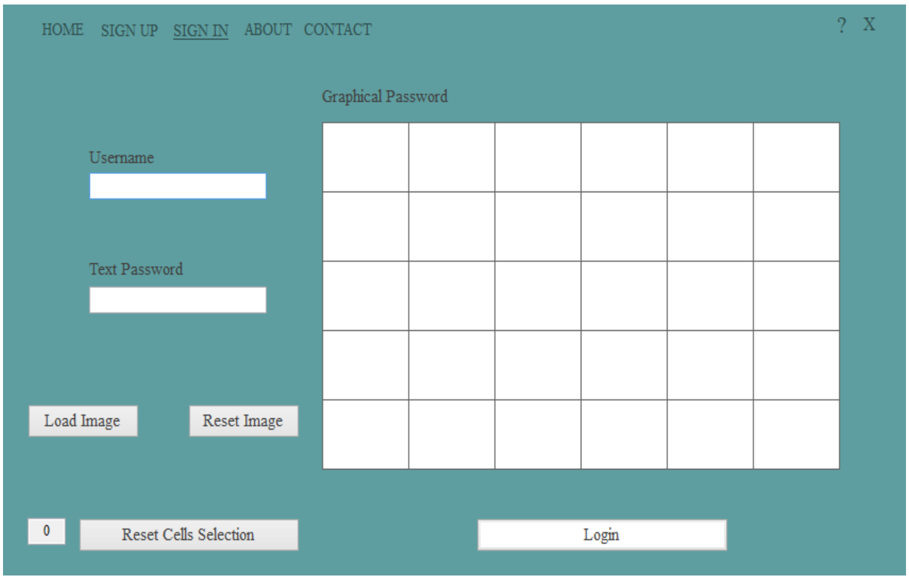
The second option in the menu bar is "Sign up" which is the registration window in the system as shown in the following window.



Unique Number 295

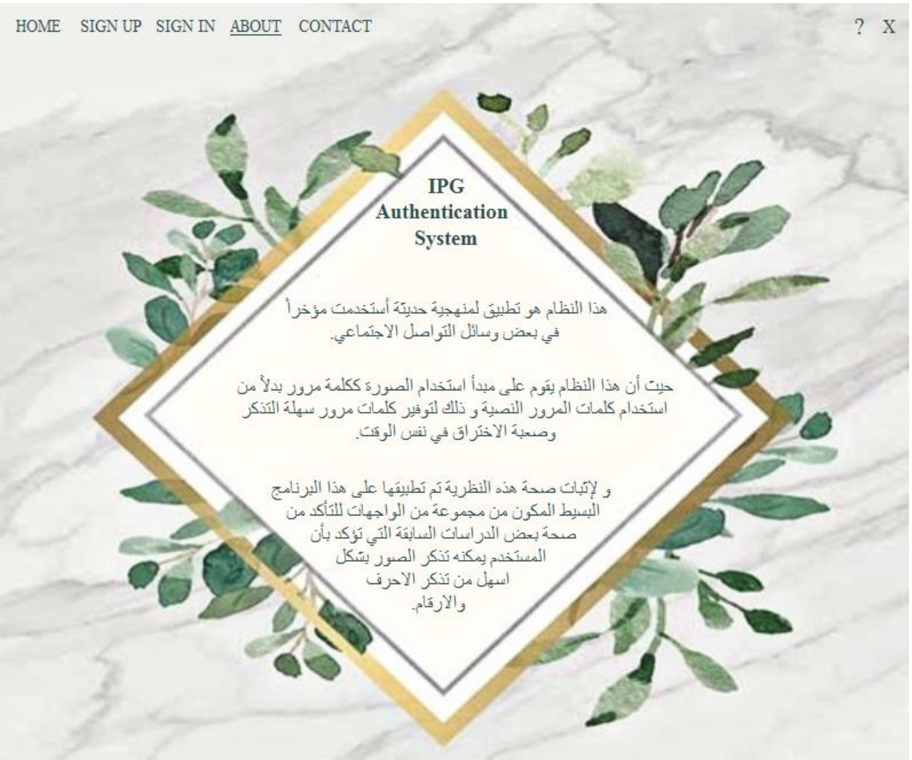
Registration window.

The option that follows this menu in the menu bar is the option for the login window in the system. When you press this option, the following window appears:



Login window.

If the user needs to get to know the system, he can click on the "About" menu in the menu bar at the top of the window, as this information was written in Arabic, because the participants' mother tongue is Arabic. The following window will appear:



IPG
Authentication
System

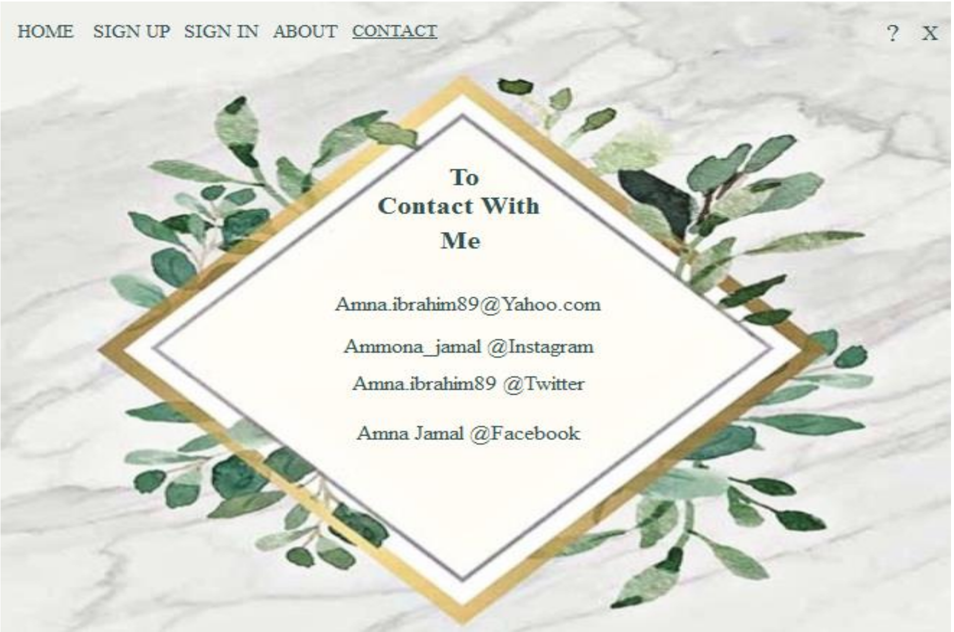
هذا النظام هو تطبيق لمنهجية حديثة أستخدمت مؤخراً
في بعض وسائل التواصل الاجتماعي.

حيث أن هذا النظام يقوم على مبدأ استخدام الصورة ككلمة مرور بدلاً من
استخدام كلمات المرور النصية و ذلك لتوفير كلمات مرور سهلة التذكر
وصعبة الاختراق في نفس الوقت.

و لإثبات صحة هذه النظرية تم تطبيقها على هذا البرنامج
البسيط المكون من مجموعة من الواجهات للتأكد من
صحة بعض الدراسات السابقة التي تؤكد بأن
المستخدم يمكنه تذكر الصور بشكل
اسهل من تذكر الاحرف
والارقام.

About the system.

The last option in the menu bar is the “Contact” option, as when clicking on this option, the user will be directed to an window containing the researcher’s accounts, displayed on the next window, in the event that one of the participants needs to communicate with her to learn more about the system.



To
Contact With
Me

Amna.ibrahim89@Yahoo.com

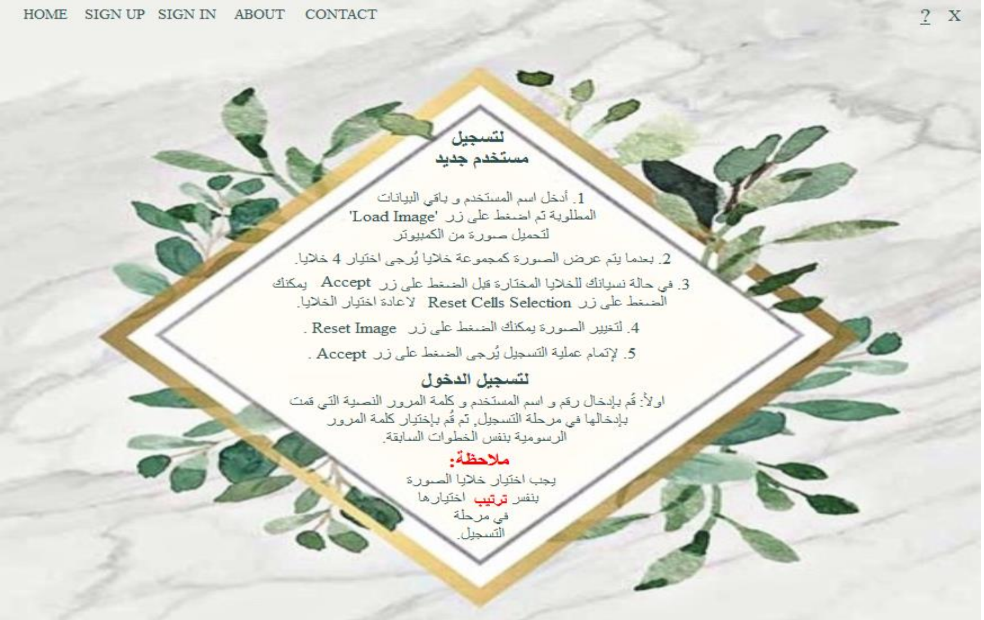
Ammona_jamal @Instagram

Amna.ibrahim89 @Twitter

Amna Jamal @Facebook

Contact window.

At the top right of the window you can notice the "?" When pressed, the user will see the following window, which contains briefly how to use the system.



لتسجيل
مستخدم جديد

1. أدخل اسم المستخدم و باقي البيانات
المطلوبة ثم اضغط على زر 'Load Image'
لتحميل صورة من الكمبيوتر

2. بعدما يتم عرض الصورة كمجموعة خلايا يُرجى اختيار 4 خلايا.

3. في حالة نسيانك للخلايا المختارة قبل الضغط على زر **Accept** يمكنك
الضغط على زر **Reset Cells Selection** لاعادة اختيار الخلايا.

4. لتغيير الصورة يمكنك الضغط على زر **Reset Image** .

5. لإتمام عملية التسجيل يُرجى الضغط على زر **Accept** .

لتسجيل الدخول

اولاً: قُم بإدخال رقم و اسم المستخدم و كلمة المرور النصية التي قمت
بإدخالها في مرحلة التسجيل. ثم قُم بإختيار كلمة المرور
الرسومية بنفس الخطوات السابقة.

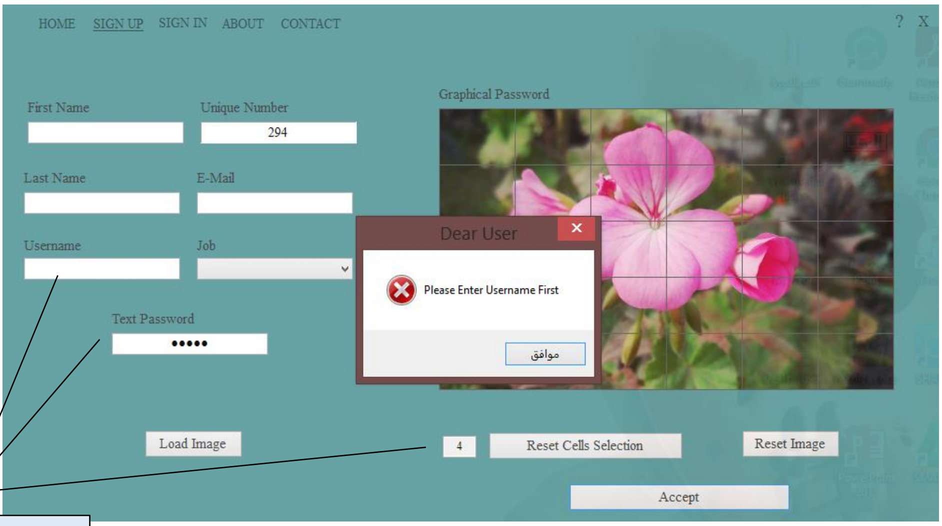
ملاحظة:

يجب اختيار خلايا الصورة
بنفس **ترتيب** اختيارها
في مرحلة
التسجيل.

Use's information window.

When the user presses on one of the previous menus, which are located in the menu bar at the top of the window, you can notice a line below the selected menu in order to increase the clarity to the user that he has chosen this menu.

The user may make some mistakes while registering in the system, such as pressing the registration button without entering the information that he is obliged to entered. Therefore, if the user falls into one of these errors, the user will be notified with an error message to be alerted. These messages will be explained in the following windows:



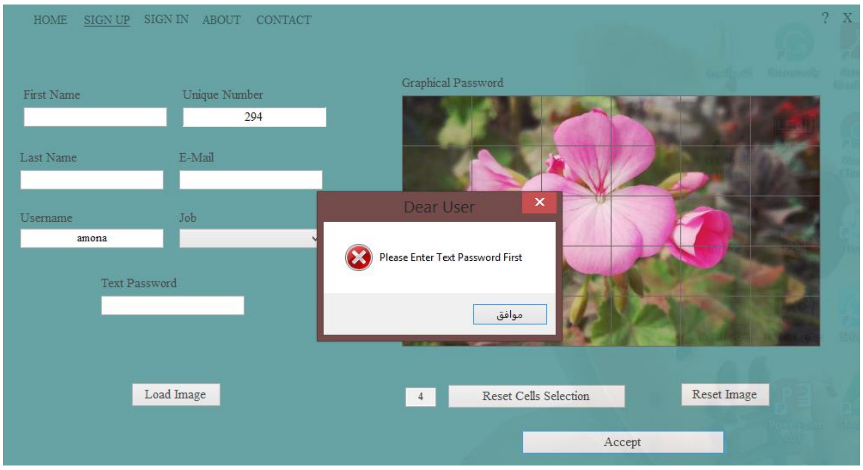
First Name:
Unique Number: 294
Last Name:
E-Mail:
Username:
Job:
Text Password: •••••
Graphical Password
4

Dear User

Please Enter Username First

Information should be entered

User do not enter username.



Unique Number: 294

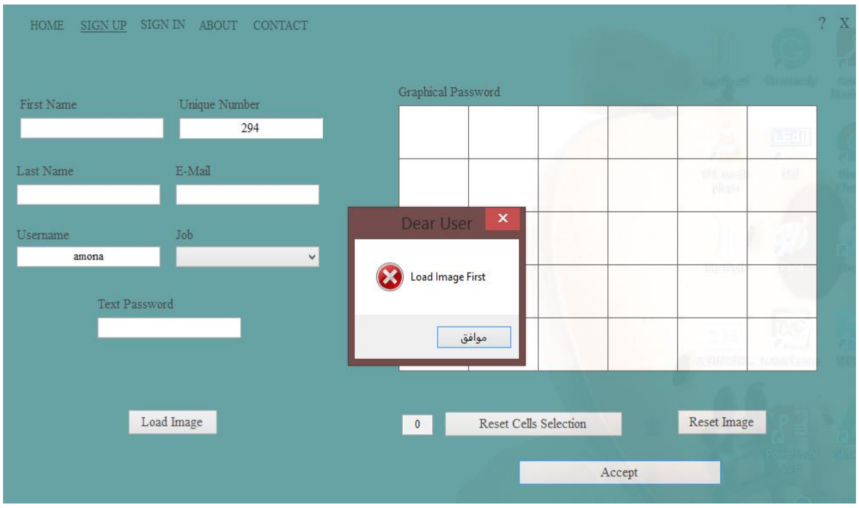
Username: amona

Dear User

Please Enter Text Password First

4

User do not enter the text password.



Unique Number: 294

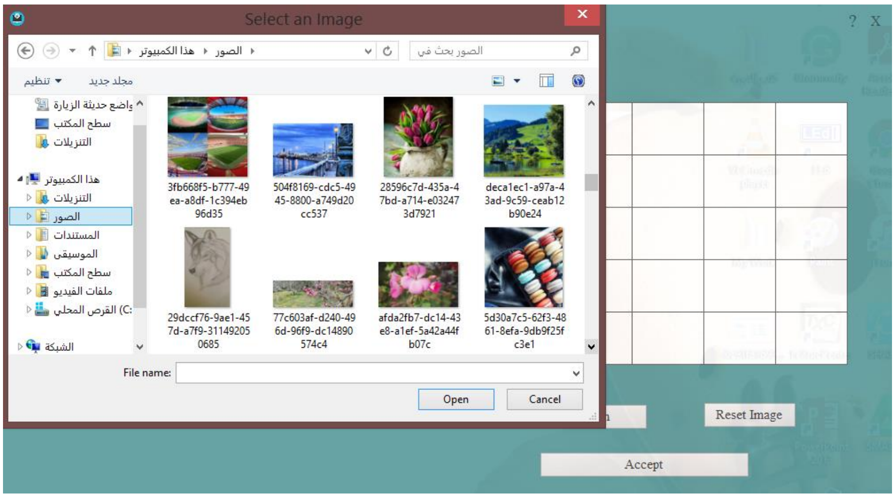
Username: amona

Dear User

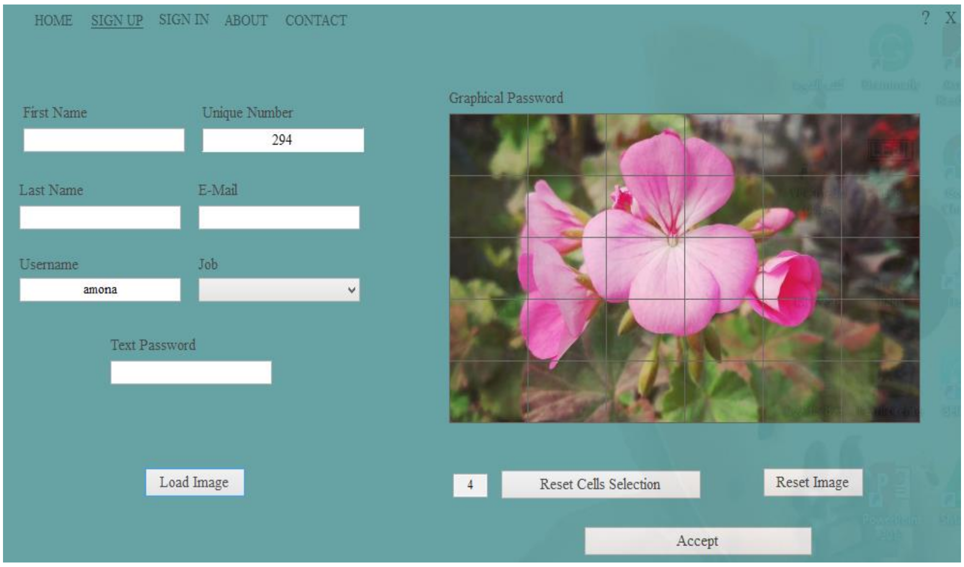
Load Image First

0

User do not enter the graphical password.


Select an Image
هذا الكمبيوتر ‹ الصور
البحث في الصور
تنظيم
مجلد جديد
مواضع حديقة الزيارة
سطح المكتب
التنزيلات
هذا الكمبيوتر
التنزيلات
الصور
المستندات
الموسيقى
سطح المكتب
ملفات الفيديو
القرص المحلي (C:
الشبكة
3fb668f5-b777-49ea-a8df-1c394eb96d35
504f8169-cdc5-4945-8800-a749d20cc537
28596c7d-435a-47bd-a714-e032473d7921
deca1ec1-a97a-43ad-9c59-ceab12b90e24
29dccf76-9ae1-457d-a7f9-311492050685
77c603af-d240-496d-96f9-dc14890574c4
afda2fb7-dc14-43e8-a1ef-5a42a44fb07c
5d30a7c5-62f3-4861-8efa-9db9f25fc3e1
File name:
Open
Cancel
? X
Reset Image
Accept

The user can choose the image from anywhere in the computer through the hierarchical organization in the previous window.



First Name:

Unique Number: 294

Last Name:

E-Mail:

Username: amona

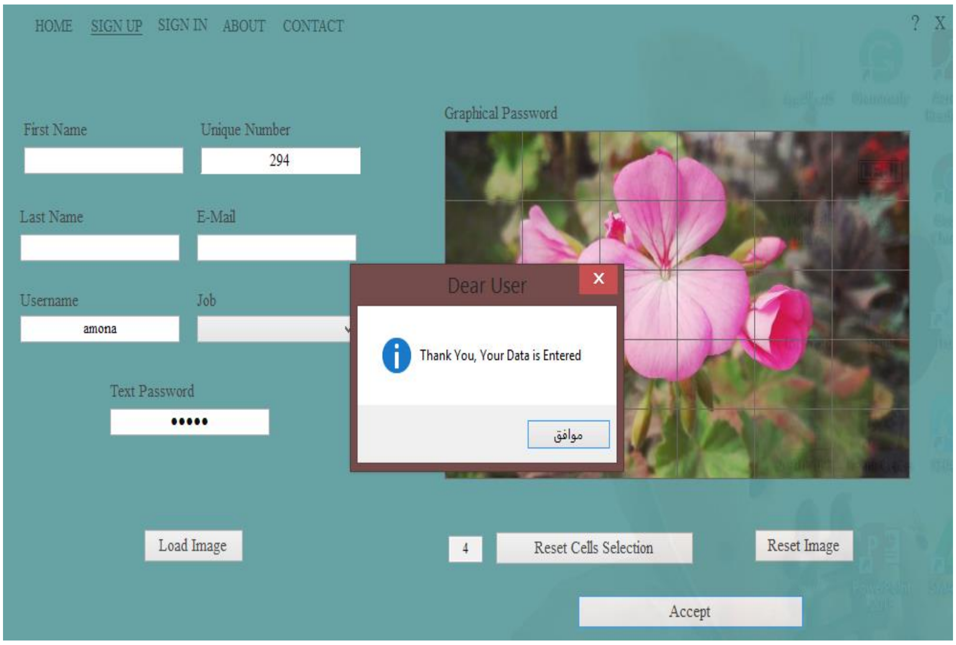
Job:

Text Password:

Graphical Password

4

After the user selects the image, it will be divided and displayed as a grid.



First Name:

Unique Number: 294

Last Name:

E-Mail:

Username: amona

Job:

Text Password: •••••

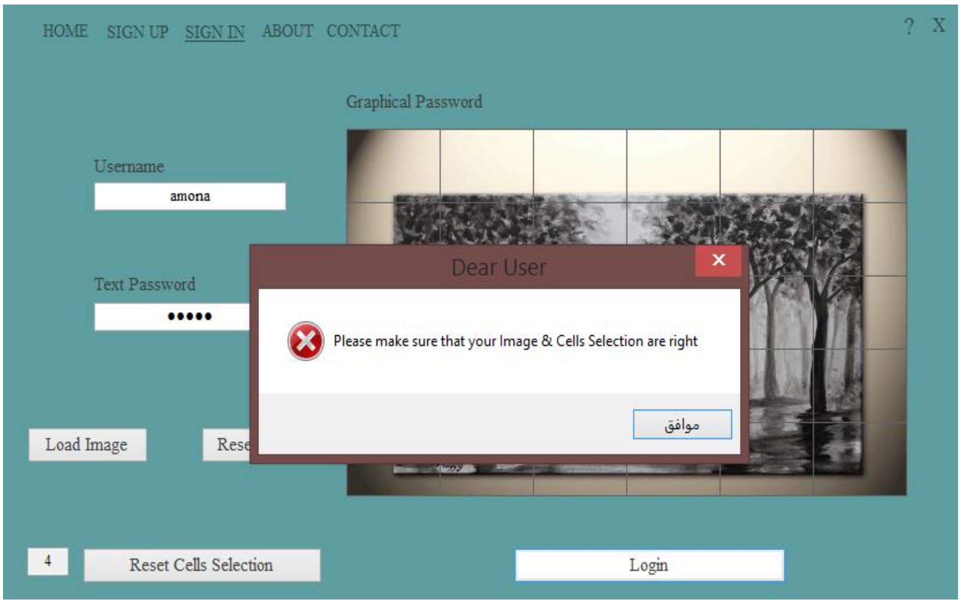
Graphical Password

4

Dear User

Thank You, Your Data is Entered

Successful registration message in the system.



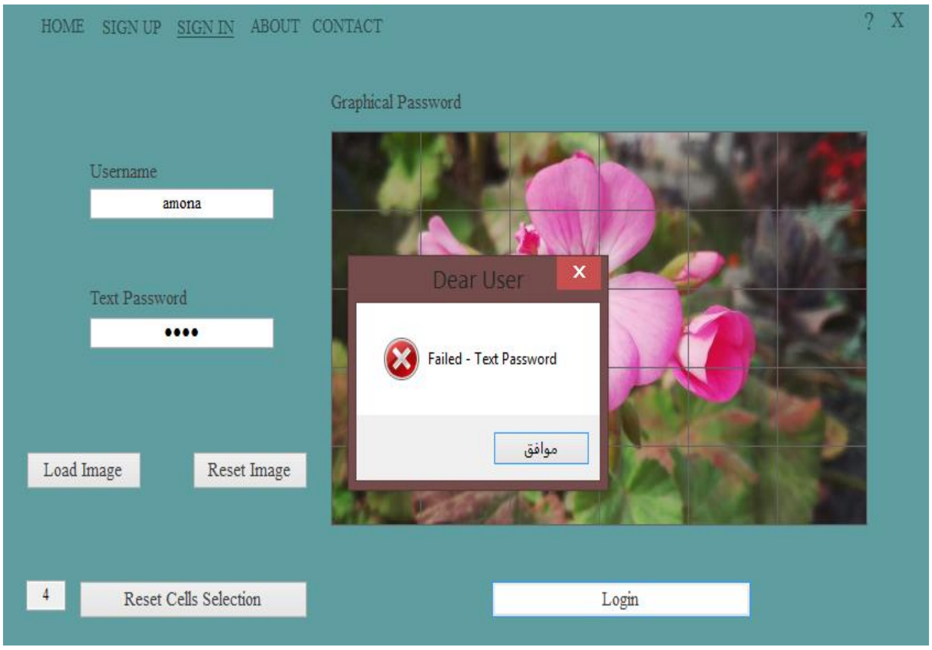
Username: amona

Text Password: •••••

Dear User

Please make sure that your Image & Cells Selection are right

Wrong graphical password message.



Username: amona

Text Password: ••••

Dear User

Failed - Text Password

Wrong text password message.

نظام مصادقة كلمات المرور الرسومية مقاوم لهجمات تصفح الكتف

اعداد

آمنة جمال عبدالسلام إبراهيم

المشرف

د. كنز بوزيد

الخلاصة

تستخدم كلمات المرور على نطاق واسع للمصادقة في أنظمة المعلومات، ولا تزال الطريقة السائدة على الرغم من نقاط ضعفها، وذلك يرجع إلى بساطتها. حيث يميل العديد من المستخدمين إلى إنشاء كلمة مرور قصيرة لتذكرها بسهولة، مما يجعلها غير آمنة وعرضة للقرصنة. لحل هذه المشكلة، تم اقتراح تقنية كلمة المرور الرسومية والتي تعتمد على استخدام الصور والأشكال أو رسم شيء ما من قبل المستخدم، إلا أن هذه التقنية تعاني من بعض أوجه القصور. حيث أن معظم مخططاتها الحالية غير قادرة على الموازنة ما بين توفير سهولة الاستخدام ومستوى آمن عالي. الهدف الرئيسي من هذا البحث هو تقديم مخطط جديد في مجال تقنية كلمات المرور الرسومية، مع الموازنة ما بين سهولة الاستخدام ومستوى الامان عالي. للتأكد من تحقيق الهدف الرئيسي للبحث، تم تصميم وتطبيق نظام جديد يعتمد على المقارنة بين مخطط كلمة المرور الرسومية المقترح وكلمة المرور النصية. تم اختبار النظام وتقييم ميزات سهولة الاستخدام، وكانت النتائج إيجابية. كما تم تقييم أمان النظام وأثبتت النتائج أن النظام يوفر آلية دفاع ضد الهجمات الشائعة التي تتعرض لتقنيات كلمات المرور الرسومية.

نظام مصادقة كلمات المرور الرسومية مقاوم لهجمات تصفح الكتف

قدمت من قبل:

آمنة جمال عبدالسلام إبراهيم

تحت إشراف:

د. كنز بوزيد

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في علوم الحاسوب

جامعة بنغازي

كلية تقنية المعلومات

مارس 2022