



Sudan University of Science and Technology

Collage of Graduate Studies

**Enhance Graphical Password Authentication using One
Time pad**

تحسين تحقق كلمة السر الصورية باستخدام كلمة السر لمرة واحدة

A Thesis Submitted in Partial Fulfillment of the Requirements of
M.Sc. in Computer Science (Information Security Track)

August 2020



Sudan University of Science and Technology

Collage of Graduate Studies

**Enhance Graphical Password Authentication using One
Time pad**

تحسين تحقق كلمة السر الصورية باستخدام كلمة السر لمرة واحدة

A Thesis Submitted in Partial Fulfillment of the Requirements of
M.Sc. in Computer Science (Information Security Track)

Prepared By:

Esraa Awad Alhaj Naem

The Supervisor: Dr. Faisal Mohammed Abdallah

August 2020

Dedication

I would like to dedicate this research To my mother who spent her life for us until she died ,To my father who has to raise us by his own, To my brothers for their patience with me, To my friends for their patience, support and for helping me, With love and appreciation.

Esraa.

Abstract

The authentication is one of the top topics in security field, therefore many methods were provided, and the most famous method is text password. It has been used for decades but still sensible for many attacks and has many drawbacks, because of all these security issues a new method must be provided to resist the security problems and accomplish the protection of user's data. In nineties, a new type of password provided called graphical password, which is using the Images or part of these images as password but also graphical password is vulnerable for many security attacks.

The proposed system was provided and implemented in this thesis, has many different features for resist different security attacks by using combination of text and graphical password and one time password. The system has two phases, login and registration phase, login phase is consisting of two phases of authentication. First phase is entering username and text password with data encryption using RSA (Rivest-Shamir-Adleman) cipher, the second phase is graphical password using recognition based graphical password method which using images as password and recognize these images in login phase, then using one time password which is sends as SMS (Short messages services) to user's cell phone, if success then the user can log in the system, otherwise logged out. In registration phase, the user enters the required information then upload and selects at least three images as graphical password.

By implement and design this system, decrease the unauthorized access to the system and it is resistible for many security attacks, therefore it is secure and complicated for attackers to break or log in to the system without have the proper privileges, and also it is user friendly and not tedious process to the user.

المستخلص

عملية المصادقة واحدة من أهم المواضيع في مجال امن المعلومات، لهذا قدمت العديد من الطرق من أهمها كلمة السر النصية، لقد تم استخدامها لعقود ورغم ذلك لا تزال عرضة للعديد من الهجمات والكثير من الثغرات الامنية، وبسبب ذلك كان لابد من طريقة جديدة لمقاومة هذه الثغرات الامنية لحماية بيانات المستخدم. في التسعينات نوع جديد من كلمات السر تم تقديمه وهي تسمى بكلمة السر الصورية حيث يتم استخدام الصور او جزء منها ككلمة سر ولكن لا تزال كلمة السر الصورية عرضة للعديد من الهجمات الامنية.

النظام الذي قدم وتم تصميمه في هذا البحث لدية العديد من الخصائص لمقاومة الثغرات الامنية عن طريق دمج استخدام كلمة السر الصوريه النصية مع استخدام كلمة السر لمرة واحدة. يحتوي النظام علي مرحلتين هما مرحلة الدخول والتسجيل، مرحلة الدخول تحتوي علي مرحلتين من المصادقة، اول مرحلة هو ادخال اسم المستخدم وكلمة السر النصية، المرحلة الثانية ه وكلمة السر الصورية حيث تم استخدام تقنية التعرف علي الصور التي تستخدم التعرف علي الصور للدخول للنظام ثم استخدام كلمة السر لمرة واحدة حيث يتم ارسالها الي هاتف المستخدم، اذا نجح في المراحل السابقة يدخل الي النظام غير ذلك يخرج من النظام. مرحلة التسجيل يدل المستخدم المعلومات المطلوبة ثم يرفع العديد من الصور ويختار منها علي الاقل ثلاثة ككلمة سر.

عن طريق تطبيق وتصميم هذا النظام فانه يقل عدد مرات الدخول غير المصرح الي النظام وهو مقاوم للعديد من الهجمات الامنية، لهذا يعتبر هذا النظام امناً ومعقد بالنسبة للمهاجمين لاخرقاة للدخول الي النظام دون الصلاحيات المناسبة بالاضافة الي انه سهل الاستخدام وعملية المصادقة غير مملة او مرهقة للمستخدم.

Table of Content

Contents

1.1 Introduction.....	1
1.2 Problem definition	1
1.3 Significant of Research.....	2
1.4 Objectives of Research	2
1.5 Hypotheses of Research.....	2
1.6 Scope of Research.....	2
1.7 Methodology.....	2
1.7 .1 Software Requirements.....	3
1.7 .2 Hardware Components.....	3
1.8 Lay Out	3
2.1 Introduction.....	4
2.2 Security Attacks.....	4
2.2.1 Graphical password attacks	5
2.3 Security services	6
2.3.1 Authentication	7
2.3.2 Authentication methods.....	8
2.4 Cryptography	9
2.4.1 Rivest-Shamir-Adleman cryptosystem.....	9
2.5 password schemes.....	10
2.5.1 Text password.....	10
2.5.2 Graphical Password	11
2.5.3 One Time Password.....	25
2.6 Related work	26

2.7 summery.....	39
3.1 Introduction	40
3.2 System components and platform	40
3.3The authentication system	40
3.3.1 How the system works	40
3.4 System analysis.....	46
3.4.1Software Development Methodology	46
3.4.2 System use cases.....	46
3.4.3 The sequence diagrams of the system	50
3.4.4 The class diagram.....	53
4.1 Introduction.....	56
4.2The system interfaces.....	56
4.2.1 The Login interfaces	56
4.2.2 The Registration interface.....	61
4.3 Results.....	62
4.4 The security analysis.....	63
5.1 Conclusion	66
5.2 Recommendation	66
REFERENCES	68

List of Tables

Table	page number
TABLE 2.1 ATTACKS RESISTANCE IN RECOGNITION BASES TECHNIQUE	25
TABLE 2.2 RELATED WORK	38
TABLE 3.1 REGISTRATION TABLE.....	54
TABLE 3.2 UPLOADS_IMAGES	54
TABLE 3.3 CHECKED TABLE.....	55
TABLE 3.4 OTP TABLE	55
TABLE 4.1 RESISTANCE ATTACKS COMPARISON BETWEEN RELATED WORK AND PROPOSED SYSTEM	65

List of Figures

FIGURE 2.1 TYPES OF AUTHENTICATION TECHNIQUES	7
FIGURE 2.2 GRAPHICAL PASSWORD CATEGORIES	12
FIGURE 2.3 DAS	13
FIGURE 2.4 GRIS SELECTION.....	14
FIGURE 2.5 PASS POINT	15
FIGURE 2.6 CCP	16
FIGURE 2.7 DEJA VU.....	18
FIGURE 2.8 PASS FACES	19
FIGURE 2.9 TRIANGLE SCHEME	20
FIGURE 2.10 MOVABLE SCHEME	20
FIGURE 2.11 PICTURE PASSWORD	21
FIGURE 2.12 MAN ET AL.....	22
FIGURE 2.13 STORY.....	22
FIGURE 2.14 JETAFIDA	23
FIGURE 2.15 REGISTRATION PHASE [13].....	31
FIGURE 2.16 LOGIN [13].....	32
FIGURE 2.17 REGISTRATION [14]	33
FIGURE 2.18 LOGIN [14].....	34
FIGURE 2.19 REGISTRATION [15]	36
FIGURE 2.20 LOGIN [15].....	37
FIGURE .1 LOGIN ACTIVITY DIAGRAM	44
FIGURE 3.2 REGISTRATION ACTIVITY DIAGRAM	45
FIGURE 3.3 LOGIN USES CASE.....	47
FIGURE 3.4 REGISTRATION USE CASE	48
FIGURE 3.5 OTP USE CASE	49
FIGURE 3.6 LOGIN SEQUENCE DIAGRAM.....	49
FIGURE 3.7 REGISTRATION SEQUENCE DIAGRAM.....	50
FIGURE 3.8 OTP SEQUENCE DIAGRAM.....	51
FIGURE 3.9 DATA BASE RELATION.....	52

FIGURE 4.1 LOGIN INTERFACE.....	56
FIGURE 4.2 USER NOT FOUND ERROR	57
FIGURE 4.3 INVALID USER NAME/ PASSWORD.....	57
FIGURE 4.4 ENTER INVALID LOGIN INFORMATION	58
FIGURE 4.5 UPLOAD IMAGES	58
FIGURE 4.6 ONE TIME PASSWORD VERIFICATION.....	59
FIGURE 4.7 USER’S DASHBOARD	59
FIGURE 4.8 CHANGING TEXT PASSWORD	60
FIGURE 4.9 RESET PASSWORD	60
FIGURE 4.10 SIGN UP.....	61
FIGURE 4.11 IMAGES UPLOAD	62

Abbreviation table

Abbreviation	Description
API	Application programming Interface
CAPTCHA	Completely Automatic Public Turing Test to Tell Computers and Humans apart
CCP	Cued Click Point
CIA	C onfidentiality I ntegrity A vailability
DAS	Draw As Secret
GPI	Graphical password with icons
HMAC	Hashed message authentication code
HTTP	Hypertext transfer protocol
OTP	One Time Password
PCCP	Persuasive Cued Click Points
RSA	Rivest-Shamir-Adleman
SMS	Short messages services
SSL	Secure Shell

CHAPTER I

1.1 Introduction

One of the most requirements in all computer system is security, which is the protection the data and the information of the organization or users from the security attacks. To make the data secure must implement the CIA trade. In addition to the CIA there is authenticity and accountability.

Authentication is to ensure this user is who is claim, implement the authentication methods will provide appropriate protection to the data and the information of the organization. The security groups invented and provided many authentication methods as passwords, one of the most famous protection method is the text password, but it is vulnerable for many types of attacks and has many drawbacks, so it is inefficient since the hacker and crackers tools and methods in continues development, therefore a graphical password is proposed to be alternative to the text password and to overcome the text password drawbacks.

Graphical password is using images as password, it is a strong authentication method but also need for enhancement to overcomes its drawbacks and the security attacks and provide better protection for the data and the information.

1.2 Problem definition

The graphical password provides many techniques for authentication, but still vulnerable for many security attacks [4], therefore the graphical password authentication methods must be enhanced.

1.3 Significant of Research

By enhancing the authentication of the graphical password will increase security and protection of data and information.

1.4 Objectives of Research

Solve the drawbacks of alphabetic passwords, enhance of authentication method that use graphical password, to make accessing the systems more friendly and secure.

1.5 Hypotheses of Research

Using one time password (OTP) with Recognition based graphical password technique will enhance the graphical password authentication.

1.6 Scope of Research

Uses for logging and registration in the systems, Uses images with all its formats, only for online web application systems.

1.7 Methodology

The system is combination of text password and graphical authentication techniques and has two levels. In the registration phase user sign up, chooses user name and password and fill other required fields in the form, the next phase is uploading images, then selects at least 3 images as graphical password, then save in the database.

In the log in phase the user signs in with valid user name and the text password and the system checks the validation, the next stage is reselecting the images that have been chosen in the registration correctly, then the server generates and saves one time password and send

it to the user's mobile as SMS with 1minute session to enter the code correctly, otherwise the system log out the user, after enters valid code the user can logging to the system.

1.7.1 Software Requirements

The proposed system does not need special software but still there is minimum requirement as windows 7 and later versions of windows or any operating system also web server like WAMP or XAMP or any suitable web server, MYSQL database, web browser to get access to the system.

1.7.2 Hardware Components

Computer pc with at least processer core I3 and 1 Tera hard disk storage, and also need a server with good requirements.

1.8 Lay Out

“Chapter two” contains the literature review of passwords and authentication and related work of graphical password, used techniques for graphical password.

“Chapter three” design structure and requirement analysis of the system will be discussed and sequence diagrams along with use case diagrams will be explained.

“Chapter four” covers the system screens and the results of the proposed system.

“Chapter five” covers conclusion and recommendations.

CHAPTER II

2.1 Introduction

Now days computers are used in every aspects of life, hospital, banks and others things, therefore a strong authentication technique is required to prevent and detect the security attacks and protect the user data. There are security attacks everywhere whether they are standing right next to you and all the way up to hacking into your computer which makes learning user authentication techniques critical. To enforce security password were introduced.

2.2 Security Attacks

Despite of security has many aspects as authorization, availability, auditing, confidentiality, integrity and the authentication which consider one of the most crucial aspect of security but still sensible for many security attacks. Below the most famous security attacks and their Countermeasure. [5].

Eavesdropping Attack is consider as a type of reply attack. In this attack, the attacker only monitor data flow through the network and uses data transfer for malicious purposes. It can be passive or active attack. In the passive attack the hacker attempts to use the transferred data without affect the system resources, in active attack, the attacker attempts to modify the data and uses the system's resources. Countermeasure is using encryption ciphers to encrypt the messages as DES, RC4, also using SSL and single sign-on protocol. [5]

Man-in-the middle Attack, it is a type of Eavesdropping Attack. In this attack, the attacker is in the middle between the two hosts, receiving data from both sides and can manipulates the data. Countermeasure is using the SSL and using certificate authority and HMAC. [5]

Reply Attack, this attack like man in the middle attack. The attacker masquerade as one of the users to control and modify the transfer data between the hosts, masquerading is one type of this attack. Countermeasures are Using OTP one time password, Cookies time out, makes cookies valid for short time. [5]

Phishing attack, the attacker makes a fake website like bank website to fraud the users to enter their information or any sensitive data to steal. This attack based on the user error in writing the target URL. Countermeasures are using the digital certificates, Caution with unknown emails and unsecure hyperlinks, only using websites with secure HTTP. [5]

Insider attack, this attack in not malicious software attack, it is company man attack, it done by the employee or user with privileges of accessing the system from the company itself. To resists this attack using intrusion system detection (IDS) can help to reduce the attack, Access Control Mechanism, Monitoring the system and update the passwords periodically. [5]

2.2.1 Graphical password attacks

Brute force attack, it is one of the hardest attacks to protect against, because it is based on trial and errors. Tries every possible combination in the keyboard to get the password. The number of attempts depend on the password size whereas the password size is big the possibilities are increase and becomes harder to break and consuming more time but it is not useful with online services because IP tracking is possible. Countermeasures are Using trapitting techniques, which is makes delay in authentication, Honeypot mechanism, using RECAPTCHA to determine if the user is human or bot. CAPTCHA is computer software makes challenges by using images. [5]

Dictionary attacks, it similar to brute force attack, both of them using the trial and error concept but this attack is less hard and quicker and consuming less time. This attack is using all the possible words in the dictionary therefore, it is uses for weak, short passwords.

Countermeasures are using encryptions cipher to encrypt passwords, making a strong password by making password combination of special character and numbers and alphabet, generally not using a word in the dictionary or weak passwords. [5].

Shoulder surfing attack is done by human. The attacker observes the user by using camera or stand behind the user to obtain the password. Countermeasures are Writes wrong password more than one time, do not write the password in front of any person. [5].

Guessing attack, unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Pass face technique have shown that people often choose weak and predictable graphical passwords based on their favorites or raced. [14].

Spyware Attack. It is a computer program design to record user keystrokes to steal the password. Countermeasures are using virtual keyboard to enter the password, using One Time Password, using Anti logger software as sandboxie. [5].

2.3 Security services

Security is Protection of data and information form intruders and attacks and unauthorized users. Computer/Network security has two simple goals keeping unauthorized users from gaining access to resources, ensuring that authorized users can access the resources they need.

To make the data secure must implement the CIA trade, which are Confidentiality, only authorized user can access the system, Integrity protect the data from unauthorized modification, Availability the data is available for the authorized users. In addition to the CIA there is authenticity and accountability.

2.3.1 Authentication

Authentication is the process to check the user identity and ensure that the user who is claim to allow or disallow accessing the system's resources.

The authentication techniques can be categories into three categories, Token based authentication system, based on what you have carrying for authentication as key cards e.g. ATM Machine. In this technique the user enters a smart card to the ATM machine then enters the PIN to confirm the user identity. This type of authentication can be vulnerable to social engineering. [1]

Biometric based authentication system, based on what you are, in this authentication technique used biological parts of human body as way for authentication as fingerprint, palm scan. It is very difficult to falsify, but they are expensive to implement. The last category is Knowledge based authentication system, based on what you know, this is the most used technique its include passwords as text password and graphical password. [1].

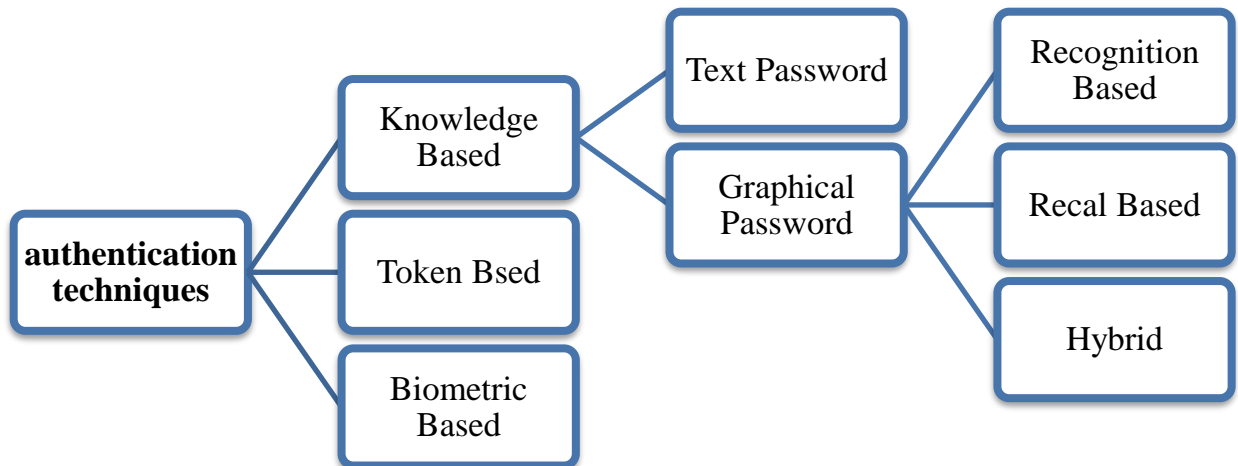


Figure (2.1) Types of authentication techniques

2.3.2 Authentication Methods

Because of all security breaking there were a need for authentication methods for protecting the systems. Below some of the most famous authentication methods were provided

Conventional password method, it is known as text password, it is a sequence of letters, numbers, and special character. It is the most famous and most used for a long time, it is easy, simple and can be short or long but still vulnerable for many types of attacks as brute force or dictionary attacks and other types of security attacks. [5]

Key stroke dynamic, it is a biometric technique, depending on the time between stroke a key and stroke the next key. The system records the time between key strokes, in the registration the system compares the time between the key strokes with the registered time in the data base, if match, gain access otherwise aborts the user. It is not accurate and depending on the user different typing speed, therefore it exposes for many types of attacks but it is does not need any additional equipment. [5]

Click, the user chooses colors as password instead of text password but in a particular pattern. It is easy to enter wrong password, does not need any additional devices. [5]

Graphical password, invented to be the alternative for the text password. This method using images as password, it is having different techniques for authentication. [5]

Digital signature uses the public key to prove the integrity and user authentication, it is uses to check the document modification. [5].

2.4 Cryptography

Cryptography (from Ancient Greek means hide, secret). In the presence is the practice and study of techniques for secure communication. Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Modern cryptography is heavily based on mathematical theory and computer science practice. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. There are two main operations in cryptography which are encryption and decryption. Encryption is convert the plain text into unreadable message using a key, the decryption is the reverse operation, the key used to encrypt and decrypt the text. [12].

There are two kinds of cryptosystems: symmetric and asymmetric. In symmetric systems the same key (the secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Examples of asymmetric systems include RSA. [12]

2.4.1 Rivest-Shamir-Adleman cryptosystem

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. The encryption key is public and it is different from the decryption key, which is keeps secret (private). Public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be keep secret. Anyone can use the public key to encrypt a message. The RSA algorithm involves four steps, key generation, key distribution, Encryption and decryption.

Suppose that Bob wants to send information to Alice. If they decide to use RSA, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message. After Bob obtains Alice's public key, he can send a message M to Alice. [11].

2.5 passwords schemes

Password with its different types considered as one of authentication type, since its uses to ensure the user's identification and the user's privileges. Password has many different types as text password, graphical password and one time password.

2.5.1 Text password

Text password is the most used authentication mechanism, usually using user name and text password for logging. Alphanumeric password was introduced in 1960 as solution to unauthorized login. It is sequence of alphabetic, number and special characters as password. Although of the good security provided by the alphanumeric password but still vulnerable for various password attacks. [2],[4].

Users choose easy password to remember as their birthday, name, favorite's pets also sometimes they put down their passwords out in paper, the solution was the password policy which is enforce the users to choose password with certain manner like Password start with capital letter, must contain upper and lower case, At least be eight characters, or any policy. [2].

The text password has many vulnerable as weak password and easy to guess, sometimes write down the password in paper also users can forget the password, or using the same password to registration to many sites.

2.5.2 Graphical Password

There was a need for new authentication method, because of the text password vulnerable, therefore a graphical password invented to solve the drawbacks of the alphanumeric password.

It was invented in 1996 by Greg Blonder [5]. The graphical password is using of images or set of images or portion of image as password. The psychological studies proven that the human memory is remembering the images better than text, human remember a person face or objects in seconds while the computer takes some considerable time for the same operation or process. [5]

Graphical password is providing better security than text password. Attacks are infeasible and it is provides a new way of setting password, which users click on images to authenticate rather than typing the password, a picture worth a thousand words. It is covers on the text password drawbacks and vulnerable, beside Password space is also quiet large. Also Less vulnerable to security attacks like online guessing attack, dictionary attacks.

There are three main categories of graphical password shown in figure (2.2), Recall based graphical password, Recognition based graphical password, Hybrid scheme. [1].

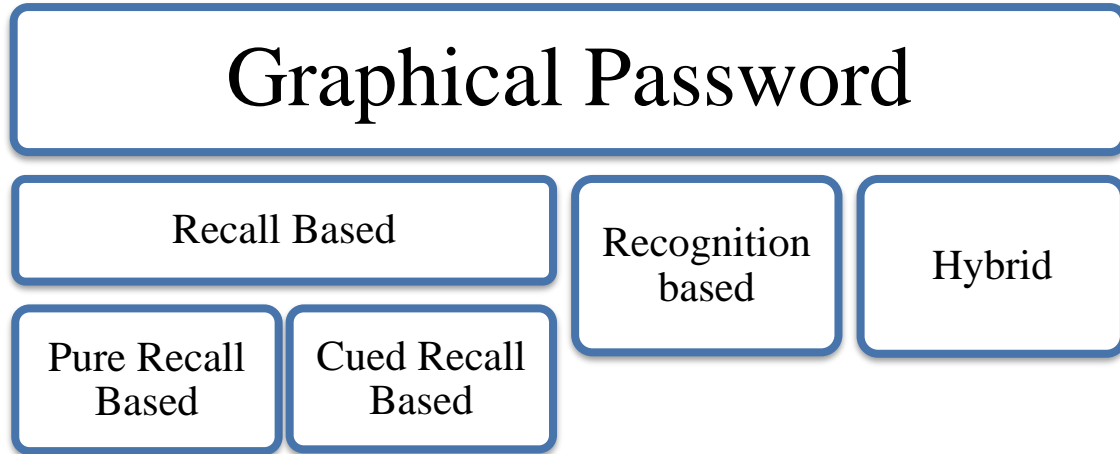


Figure (2.2) Graphical password categories

Recall based graphical password, this technique uses a portion of the image as password in the registration phase, and the user may or may not has a hint to help remembering the chosen portion of the image. [4]. this technique has two categories, pure recall based and cued recall.

Pure recall is known as draw metric system because the user draws the password, reproduce the password in 2D. In registration the user chose a portion of image or portion of images set as password. In the login phase the user has to remember the image coordinates without any hint to help the user to remember the coordinates. The disadvantage is easy to forget the coordination but it is more secure than recognition based. Pure recall has many algorithms here are some of them. [2], [4].

DAS was the first graphical password proposed, in this algorithm user is required to draw in 2D grid correctly the password using mouse or pen or any available technique of drawing, the system is store every stroke as coordination pair(X,Y), The length of the password is the coordinates pair. In the time of login, the user has to remember every stroke coordinate correctly to access the system. It is hard for the user to remember the exact coordination position for every stroke. It is widely used in mobile application like lock system as drawing pattern.

The advantages of this algorithm are no language complex (natural language) or restriction and Easy to implement and no additional equipment required. The disadvantages are the user can not always remember every stroke coordinates and It is not user friendly, if the user not familiar with mouse or joystick then becomes hard to use. Below figure (2.3) shows the DAS. [1], [2], [4].

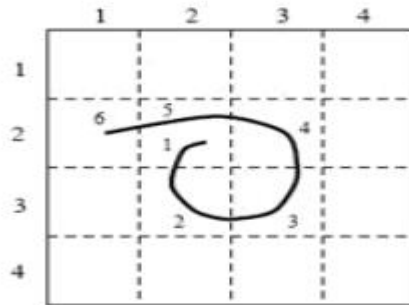


Figure (2.3) DAS [1]

Grid selection overcomes the DAS limitations. In this algorithm the system displays a large grid rectangular, the user demanded to choose a small of this rectangular, the system zoom the chosen portion, then the user draws the desired password. The advantage is password space is larger than DAS, therefore it is harder to break comparison to DAS. The disadvantages are also the user can not always remember the stroke coordinates correctly, it is not always user friendly with whom not familiar with the different input devices. [1]

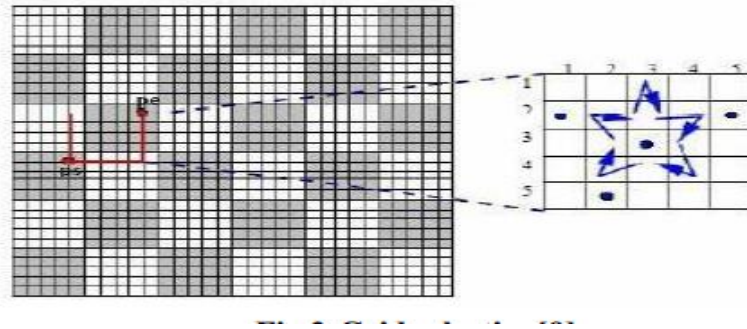


Figure (2.4) grid selection. [1]

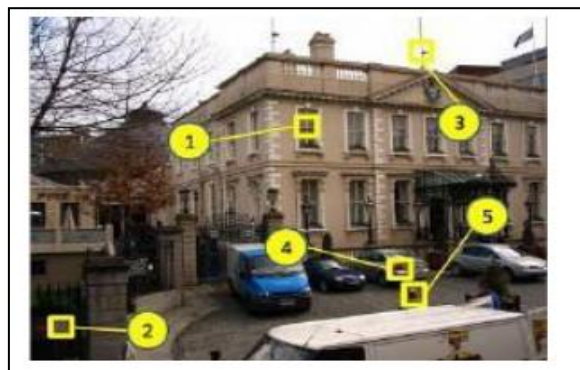
Pass doodle, it was proposed by Varen Horst. It is similar to DAS, in both of them the users draw the password but in pass doodle no use of grid, it is free hand drawing, the users can use colors in drawing the password. It is consisting at least 2 strokes, the system saves the password coordination in registration. In login the system compares the drawing password with the saved coordinates in the data base, this process of comparison is more complex than DAS. [1]

Pass shapes, it was proposed by Weiss, it is similar to pass doodle, also no grid is used but instead using geometric shapes and specific strokes number which is 8 pen strokes. It is easy to remember but the password space is small therefore it is vulnerable to guessing attack. [1]

sykuri algorithm, in this algorithm the users draw their signature as password using mouse or stylus, it is having two phases registration and verification. In Registration the user draws a signature, using one of the input devices then the system extracts the signature and it's angular and stores them in the data base. In Verification, the system takes the user input and extract the parameters of the user's signature, the system compares the entered signature using geometric average. The advantages are the signature is hard to fake and it is easy to remember. The disadvantage is the comparison process is complex and consumes time. [2], [4].

Cued recall based, it the second type of recall based graphical password. It is known as locimetric system. In this schema the user has to choose a specific location in the image and click on it to use it as password in the registration phase. In login phase the user has to remember the clicked location in the registration in the correct order to get into the system, the system provide hint to help the user to remember the clicked locations. The advantages are it is more memorable than pure recall because of the hints and it is enhancing the security and usability for users, but it is still vulnerable for many attacks. [4].

The cued recall algorithms has many algorithms. Pass Points, proposed by Wieden Beck, it is consider an extended for Blonder's schema but this schema is enhancement of Blonder's schema, it over comes many limitations. The user can choose any image but with many possible click points, this algorithm is providing hint to user to help the user to remember the clicked points, the user must remember the order of the click points in the registration. The advantage is the user can choose click points as much as possible, therefore it is more secure. The disadvantages are Consuming time, not easy to remember the click point orders. [1], [2]. Below figure (2.5) shows pass point scheme.



S

Figure (2.5) pass point scheme. [1]

Cued Click Point is proposed in 2007 as alternative to pass point. It can be viewed as combination of pass point, pass faces and story schemes. In this scheme, the user clicks one point each image for a sequence of images, the next image is display based on the previous click point. Users tend to selects points within known hotspot region (area of image that users are more likely to use). [4].

This scheme also introduces visual cues which instantly alter the users if they made a mistake entering the last click. Users can create a new password with different points to get different images. The advantages are providing more security than pass point, increase security by increase the number of images in the system, It is easier to recognize than pure call, login time is acceptable which 6.0 seconds, Success rate for login is high, implicit feedback when users see unfamiliar images, they know they are in the wrong direction, quickly create and re-enter the password. But still suffers from the hotspot problem, users tend to select images within known hotspot regions and Shoulder surfing attack. Below figure (2.6) shows the CCP scheme. [1], [4], [8].

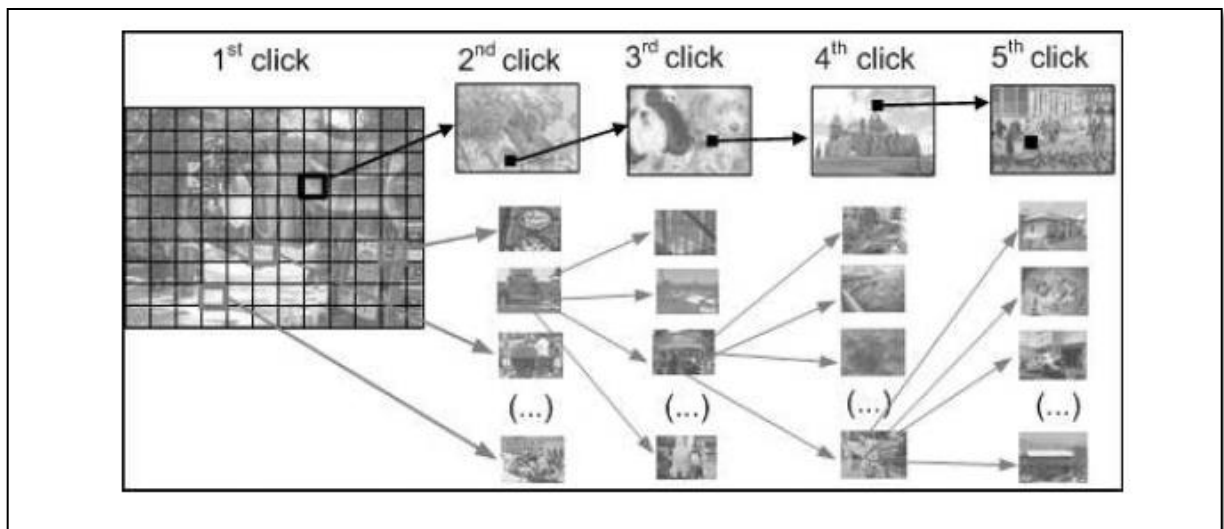


Figure (2.6) CCP. [8]

Persuasive Cued Click Points was proposed by Chiasson. In setting up the password images slightly shaded excepts for random small view port area which positioned on the image, the user has to select a click point with in the view port, users can shuffle the viewport position until the ideal location is found by the user. In login, the system displays the image without shade, user clicks point per image. The advantages are Persuasive Cued Click Points overcomes the hotspot problem, Enhance the usability. The disadvantages are, these schemes is vulnerable to shoulder surfing attack, since the image position not change and the attacker can use a screen scraper to find the location of the click point and observe the user while entering the password. [1], [4], [8].

Recognition based graphical password, it is second category of the graphical password. Also it is known as cognometric. In this technique the user has to recognize the image or images which chosen in the registration phase correctly without hint to help the user, images can be faces of human, animals or flower or whether the user wants, so this technique depend on the user memory to remember the images correctly. Whenever more images chosen whenever the security improve and vice versa. [3]

This technique is easier to remember than others graphical technique, the research shown that users can remember their password even after month or two with 90% correctly. .Recognition algorithms, it is the easiest algorithm in the graphical password because, it is easy to remember. It is having many different algorithms to implement. Below some of most used recognition algorithms. [4].

Déjà vu, it was proposed in 2000 by dhamija. To register a new user, an initial seed is given to the user, then one random mathematical formula generates which define the color value for each pixel in the image, the output will be random abstract image, because the image depends only on the initial seed, therefore only the seed needs to be stored in server data base. In login the user should pass through a challenging set, which his portfolio mixes with some decoy images, if could identify the chosen password successfully, the user will be authenticate. [3]

It is secure and resists shoulder surfing attack. But if the server crash down, the seed will have corrupted and lost. Login time longer than text password login, therefore it consumes time and The password creation time is about 60 seconds, which is longer than time needed to create text password, also The process of selecting a picture from data base can be tedious and consuming for the user, it is hard for the user to remember the art images. Below figure (2.7) shows Déjà vu. [3], [2].

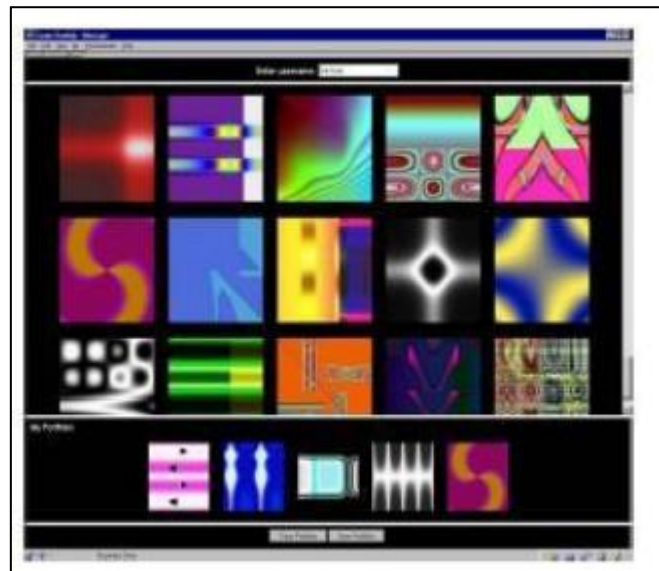


Figure (2.7) Déjà vu [1].

Pass face, it was Proposed 2000 by Brostoff [4]. This method using the faces as password, the user chooses faces in registration phase. In registration users select whether their pass face consists of male or female pictures, they choose four faces from database as their password.,the system displays a trial version to confirm the password. The procedure password will complete when the users identify correctly for their password twice in a row with no prompting. For selection decoy images used different methods which are randomly by the system, visual similarity to the password face, similarity to verbal description.

In the login a grid contain a picture is displayed to the user, the grid only contains one of the password pictures and the other eight are decoy images, so the grid is displays four

times and the order of faces within each grid is random. The advantages are it easy to remember, Easy to use, Ease to create, Resistance to shoulder surfing and packet sniffing. But it is vulnerable to spyware because face images are clear to vision,also guessing attack because, some user's choices for images affected by their race or gender or some others factors. Below figure (2.8) shows the pass faces. [4]



Figure (2.8) pass faces. [8]

Triangle scheme, it was proposed in 2002 by a group of researchers whom created several schemes to overcome the shoulder surfing attack. The system randomly displays a set of N objects; the user has to select K objects which are the password. During the login, the system randomly selects a placement of n objects, user must find the K objects and click inside the visible triangle which created by the three objects. For each login this challenge is repeated a few times using different displaying of N objects. Advantages, the probability of randomly clicking in correct region in each challenge is very low, this method can be resistance to shoulder surfing attack. The use of unlimited objects, make the display very crowded and unclear, by using a few object leads to very small password space. [8]. below the figure (2.9) shows triangle scheme.

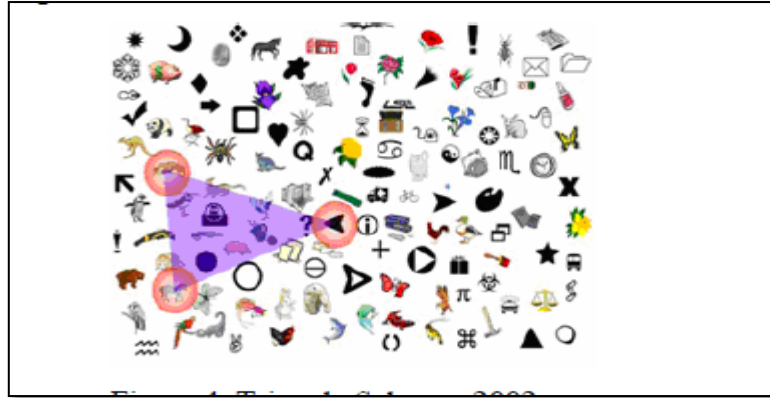


Figure (2.9) triangle scheme. [8]

Movable frame scheme was proposed in 2002[8], using the same idea of triangle scheme. In this scheme user must locate three out of K objects (the password), in the login the user has to move the frame with object inside it using mouse until the objects placed in one line. This procedure repeated a few times. The drawback of this scheme, the login process is not easy and tedious and it is consuming times to login. Below figure (2.10) shows the movable frame scheme. [8]



Figure (2.10) Movable frame scheme. [8]

Picture password scheme was proposed in 2003 for devices like Personal Digital Assistance (PDA). In registration user chooses a theme with thumbnails images to use as password then register a sequence of the thumbnails which were used. In the login, the user must identify the chosen theme, since the number of images are small the password space is small, therefore, the scheme designer added a second method of selecting thumbnails images using a shift key to select upper case or special character on traditional keyboard but recognition of password becomes harder and complex. Below figure (2.11) shows the Picture password scheme. [8]

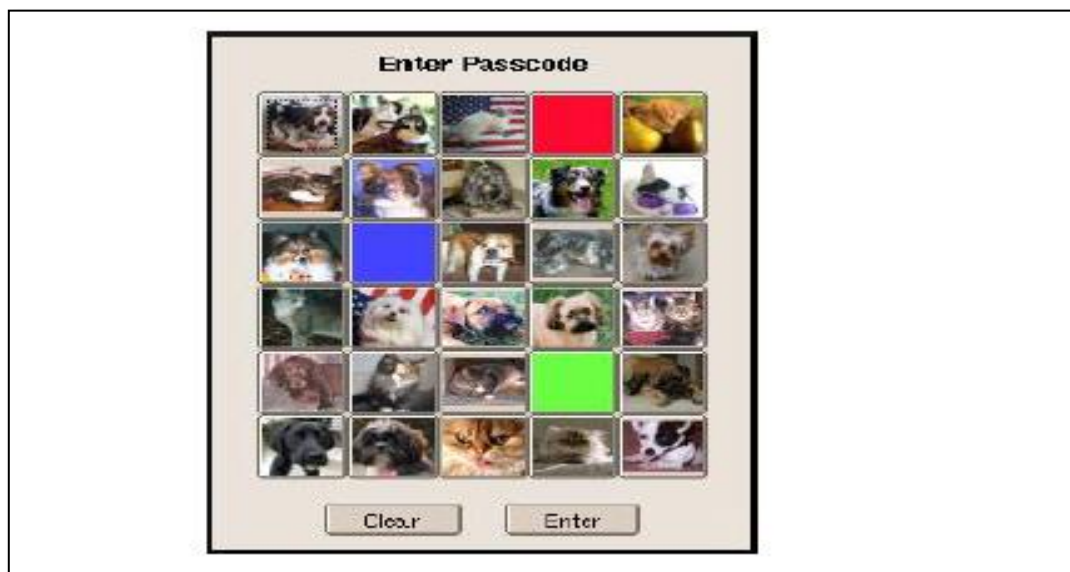


Figure (2.11) Picture password scheme. [8]

Man et al. scheme proposed in 2003, to resist the surfing shoulder attack. In this scheme all pictures have a unique code. To login the user has to pass a challenge which is a scene with several password objects and many decoys images the user must enter the string of code for each password. It resists the surfing shoulder attack but the user has to memorize of each password code and this process is inconvenient. Below figure (2.12) shows the Man et al. scheme. [8]



Figure (2.12) Man et al. scheme. [8]

Story scheme proposed in 2004. Similar to pass faces but here the order of images is important. The users have to select their password from mixed pictures of different nine categories in order to make a story. This scheme is harder to remember than pass face. In login the user has to recognize the images sequences in the correct order. It secure more than pass faces but the images order is not easy to remember correctly, over 80% of users remember the images but with incorrect order. Below figure (2.13) shows the story scheme. [8]

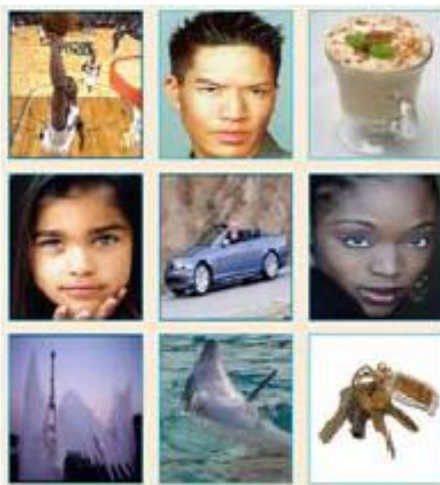


Figure (2.13) story scheme. [8]

Jetafida scheme, proposed in 2008, on trying gather the usability features (easy to use, easy to create, easy to remember, easy to learn and acceptable design and layout). In registration user selects three pictures as password then sort the password as the user wish to see them in login. In login a set of seventeen images with password images will display, the user has to recognize previous selected password. The researchers have done a study for the users of this scheme and there are the results, 40% of users thought it is easy to use, 50% said it is easy to create, 55% thought it is easy to memorize, 57% thought it is easy to learn, 53% thought the design and layout are acceptable, it is new, there is no special drawbacks in any survey until today. Below figure (2.14) shows Jetafida scheme. [8]



Figure (2.14) Jetafida scheme [8]

Graphical password with icons, It was designed as solution to hotspot problem. In the registration, the system displays a set of 150 icons, the system generate a password consists of 6 icons, if the user does not like it, the system will generate a new password until the user satisfies. It is easy to remember but it is consuming long time to login and has small size of icons.

Hybrid schema is the last category of graphical password. Hybrid schema is one or more graphical password schemes proposed to overcome the single schema of graphical password limitations. For this purpose, many schemes are proposed as Jimmy proposed a scheme which image used as remainder to help user to remember the password. In registration the user chooses an image and selects a colored template, then clicks on a specific location in the image and place the template. In login the user has to choose the correct template and place it in the correct location on the image then enters the visible character in the holes. Users only require remembering the correct template location on the image. Therefore, the password memorability is higher than textual password.

Gao proposed a scheme using CAPTCHA. In registration users select the image as password. For authentication, users must recognize the password image from decoy images and typing CAPTCHA string below for every password images. It is almost unbreakable, but spy ware attack is still an issue. [2]

Gao proposed another scheme called pass hands. It is combination of recognition based graphical password and biometric based technique. In this scheme the process is done for recognition palm instead of images. In login, nine images of Palm are displayed in 3X3 grid where one of the images is the password image, the users compare their left or right hand to particular region with the palm images, then click on the correct image. The usability is an issue also the login process become inconvenient to users since the hand comparison process needs time. Following table (2.1) shows Attacks Resistance in Recognition-Based Techniques. [2].

phone as a part of authentication process. Below a list of solution of using mobile phone for authentication:

SMS authentication with session ID verification, a session ID is sent both to the user's computer, and is shown in the web browser, as well to the user's mobile phone. The user then verifies that the session IDs are duplicates and confirms by returning a text message to the sender.

One time password from SMS to pc, the server generates an OTP code and sends it to the user's phone, then the user enters the code to the browser for verification.

One time password from pc to SMS, this method requires an applet software installed in the user phone. First the server generates a challenge and sends it to the user's browser, the user using the applet to enter the challenge and OTP code generation then the applet sends the answer as SMS to the server. If the answer is correct the user can have logged in. [10]

SIM strong authentication via mobile phone, this solution also uses software installed on the user's cell phone, using this software to access the access. Not required sending or receiving any SMS for authentication.

Software token in the phone, also using installed software in the cell phone, the software generates OTP and connects with the system directly without using any SMS verification. [10]

2.6 Related work

Delphin Raj and M. Nancy Victor in [2] proposed authentication scheme. Uses different combination of approaches and techniques. The proposed system has three authentication schemes, setting up the password, the registration and the login. Setting password, the system is displays a set of images, user chooses an image from the set. User

selects portion of the chosen image, the system saves the pixel coordination. The next phase is choosing a numbers form rolling list, user has two options for choosing, choosing from the rolling list random numbers or enter numbers which the user chooses from the rolling list.

The system is displaying images with random numbers with each image, the user must recognize the chosen image and the numbers from the rolling list correctly. Then the user enters username and text password. The last phase is entering the CAPTCHA. To access the application user has to pass all this phases correctly, the user has three chances to get access to the system if the user fails the system will lock the user account for 5 hours.

The login, the system will display a set of images, the user must recognizes the correct image, then select it correctly the chosen region of the image. The system displays a set of rolling numbers and asks the user to select the correct number. The last phase, the user has to enters the user name and the password and enters the CAPTCHA challenge correctly. This scheme used different combination of techniques and approaches, such as click based and choice based approach. The click approach used to select the image form images set, the choice approach used to select the sequence of images, for selecting image again a recall based should use to identify the image portion which selected during the registration. In this schema can use different combination of graphical password to setting up the password.

The system provides more security even to the network, by using the CAPTCHA to ensure the application user is a human not robot which is used in hacking systems, therefore it is resistance to malicious software attacks, it is shoulder surfing attack resistance. Biometric systems can be implemented for better security. The proposed system does not contain any hint, so the user can forget the pixels coordination of the image and used all the login attempts and fail then the system locks the user, therefore, the login process is tedious and inconvenient specifically if the selected region is small.

Nilesh Kawale , Shubhangi Patil proposed in [3], a system used the recognition based technique. The registration the user chooses an image or more than one from the image pool.

In this system the user chooses three images and every image matrix is containing a password. The login phase, user enters user id, password sends on the user's cell phone, then the entered password is compared with the stored password in data base, if match the user reselects the three images which were selected in the registration, again another comparison of matching generated number of the selected images the with saved password, if match the user gain access.

The system is more resistible for graphical password attacks. Brute force attack and dictionary attack, by selecting unfixed number of images and generate random number for each image every time this minimize the brute force attack and dictionary attack. Also resists spyware attack because cannot capture the password by the use of mouse or keyboard. Shoulder surfing attack, the attacker cannot guess the movement of the mouse and keyboard. There is no login attempts to prevent the unauthorized login, also generated password is fixed if the hacker gets the password then can login each time.

A.Abuthaheer N.S.Jeya Karthikka T.M.Thiyagu proposed in [6] a system used the cued click point as graphical password technique but it is suffering from the click point's area. Therefore, the propped system provides three ways for authentication and better security.

In registration phase, the user selects five photos from images set or the user can upload the images from the user's local drive. The server generates a signature based on an algorithm and saves the signature to the database. In login, the user reselects 5 images correctly, then the server generates the signature based on the images selection, the server compares both signatures, the signature stored in the data base and the generated signature. The server generates one time password based on the images pixels then sends the one time password to the user mobile, if match can login, Otherwise log out the user from the system.

Resistance Guessing attack by using images shuffling and reduce the hotspot and pattern problem (cued click point security issue), also increase the password space thus the password is more secure and effective. Although of all the results, the project covers small fictions of all possible points and also focus on the individual clicks not complete password.

Nilesh Changune, Ganesh Shinde, Sagar Chaugule, Sandeep Helkar proposed in [7] a system used persuasive cued click, dead Zone concept to resist shoulder surfing attack and using sound signature to rest the password. In registration, the user enters the registration basic information, selects the click point for each image, then the system calculates the hash function for each image, the users selects an audio in case of forgetting the password then saves the data in the data base.

In login, the user enters the required information, then clicks on each image, the system calculates hash function for verification, if all images authenticate correctly the user can login, otherwise abort the user. The dead zone concept, it is a Concept invented by the researchers of this project to avoid the shoulder surfing attacks by making the user clicks the wrong area in the image to confuse the attacker. Forget the password is a common situation in any system, therefore any system must provide a technique or method to rest the password. In this system uses a sound signature as technique to rest the password, when the user forgets the password, the system plays a sound which is uploaded in registration, the system gives the user the permission for creating a new password, then continue the registration steps.

The proposed system enhance the PCCP security by using the hash function and dead zone concept. Using the sound signature for setting up a new password, using the dead zone as method for avoiding the shoulder surfing attack. Users cannot remember the audio file if not use it for long time.

Prashanthi Muddam, D.Raman proposed in [9] a system which the user clicks on particular point or pixel per image in a sequence of pictures. The next image depends on the previous click point is correct. User's login with three credentials, a user id, encrypted password, and the last credential is proposed graphical password scheme. If an intruder

attempts certain attempting to hack the system, the account is lock. This scheme is used cued click point technique.

The proposed system provided a protection against online guessing attack and denial of services. Using more number of images increase the security but Because of using the cued click point technique, it is hard to remember the selected points accurately.

Arash habibi Lashari, Azizah Abdul Manaf, Maslim Masrom. In [13] proposed a system using watermarking technique as solution to solve image gallery attacks and using random character set generation for each image for resistance shoulder surfing attack to provide better system, this system provided a method for guarantee the legitimate of the images among the attacked ones by using watermarking techniques.

Watermarking is a process of embedding a type of mark in multimedia objects as images, it is similar to adding the owner's signature to the multimedia object, it is uses as a form of copyright protection, authentication content, detecting unlawful editing. The embedding process uses a secret key that determines the location if the watermarking will be placed in the object in the images. The system has two phases, the registration and the login phase.

On the registration, the Images matrix contains password, user selects images from the matrix s password for example user selects three images as password, the user's string will be generated, these images have a storage area number i.e.(21,17,44), the algorithm will selects a random number of the three images e.g. 17, this technique will store a unique ID such as (1452) in image number 17 along with images numbers 21,17,44 resulting in 1452,21,17,44., then sending this string from the client to server.

Login phase, three random character for each images in the matrix will be generates by the algorithm, the user must enter this code with the password in the text box. This is to secure the login process from the shoulder surfing attack and keep it simple for the users, the

algorithm will find the related images of the selected character from the login matrix, in this case 44,21.14 then checks the copyright information in the images and generate data pack such as 1452,21,17,44, the algorithm checks data pack with user's information in database if match user gain access otherwise, abort the user.

The attacker can change the images in the matrix but with images copyright it is difficult to change the images. The system has unlimited and unfixed number of images to be selected as password and randomly generates character set for each image during the login to minimize any chances to discover password. But watermarking is still vulnerable to attacks because digital content can be edited like cropping or like gamma correction, compression or low pass filtering.

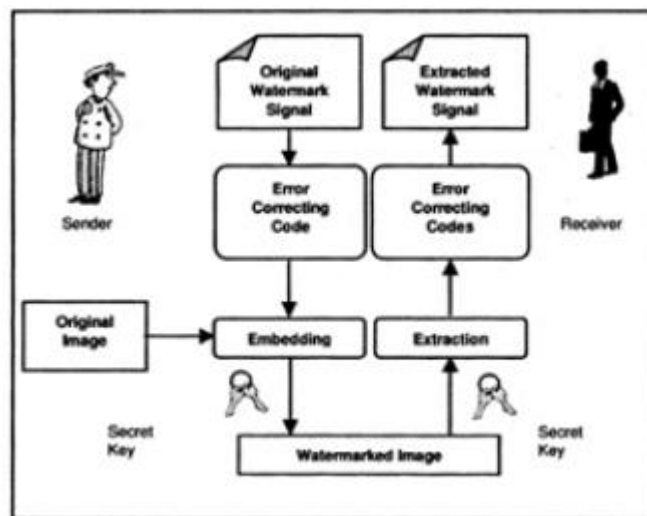


Figure (2.15) the registration phase. [13]



Figure (2.16) the login phase [13]

Veena Rathanave11, Swati Mali. In [14] proposed system is based on passlogix graphical password scheme which is a recall based graphical password system. The user needs to click of a few items from an image, the item to be clicked are one time. Password which will be send to the users mobile by text message from the database. The proposed system consists of two phases, login and registration. In registration, the user register by providing user id, password and mobile number then information will be store in database. Below figure (2.17) shows the registration phase.

Login phase, the user enters user id and password correctly, then an image with several items will displays to the user, the system sends some items from the image to be clicked to the user's mobile number as an OTP. The user must click then items in the correct sequence also the OTP has limited time, if the OTP session expired a new image loaded and send to user again. If the user enters the OTP correctly, then can login to the system otherwise the whole process will start again. Below figure (2.18) shows the login phase.

The system reduces the task for the users to remember the images they selected, provide multilevel authentication (text password, graphical password) and tries to avoid

shoulder surfing attack by using items to clicked which is sends the user's mobile so the other people cannot copy or reenter the password but entering many items is a tedious process to the user and takes time.

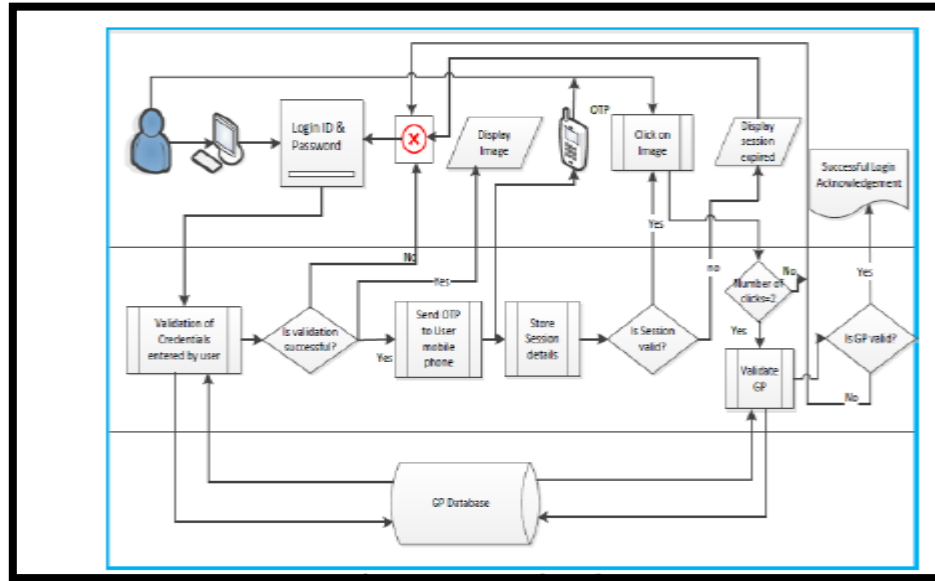


Figure (2.17) registration [14]

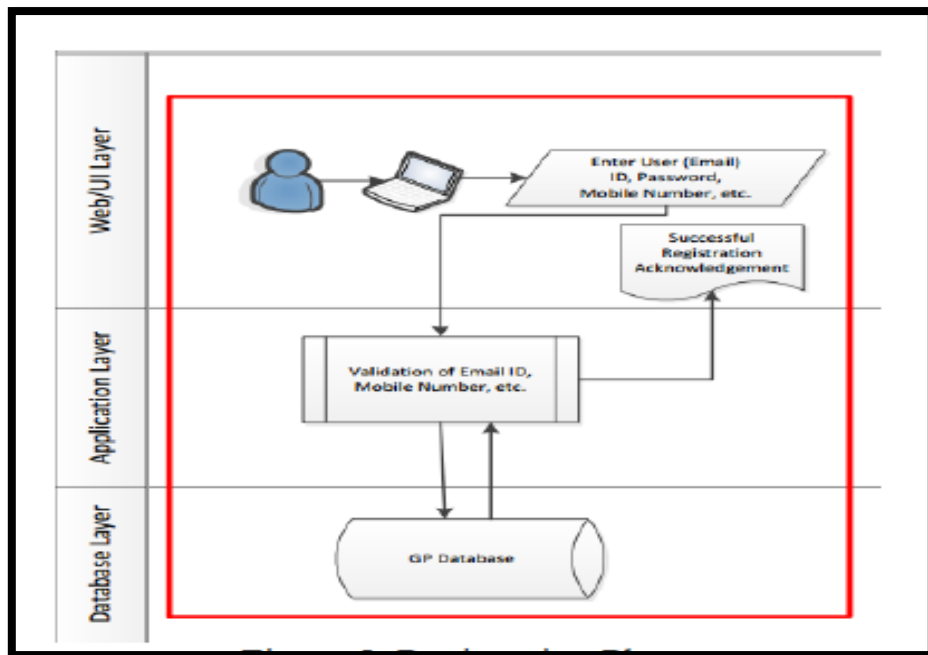


Figure (2.18) login phase [14]

Aman Kumar, Naveen Bilandi. In [15] proposed system a hybrid scheme, it is a matrix of both recognition and recall based graphical password. The proposed system is an approach towards more reliable, secure, user friendly and robust authentication, it is reducing the shoulder surfing problems.

Proposed system comprises of 9 steps out of which steps 1-3 are registration steps and steps 4-9 are the authentication steps. Step one type the user name and textual password, step two objects are displayed to user and the user selects at least 3 objects from the set, there is no limit for maximum number of objects. The user draws the selected objects which are store in the data base. Step three, the user draws preselected objects and the password on a touch sensitive screen with mouse or stylus (pure recall based method). Below figure (2.19) shows the registration phase.

Step four, the system performs preprocessing. Step five, the system gets the input frame user and merges the strokes in the user drawn sketch. Step six, the system constructs

the hierarchy. Step seven, sketch simplification. Step eight, three types of features are extracted from the sketch drawn by the user. Step nine, is called hierarchical matching. Below figure (2.20) shows the login phase.

During the authentication, the user has to give username, password then draws preselected objects, these objects are matched with the templates of objects stored in the data base, and then the user will be authenticated if only the drawn sketch is fully matched with the selected objects template. Preprocessing of hand drawn sketch is done prior to recognition. If the user draws very large or small the system adjusts the symbols to a standard size. Next step is merging the strokes which are broken at end points if the end points are not close, then that stroke is considered as open stroke and it may be merged with another open stroke if the end point of one stroke is close to the end point of the other. The strokes are then represented in a hierarchy to simplify the image and to make it meaningful. In the next step of sketch simplification, a shaded region is represented by a single hyper-stroke, three types of features are extracted from the user re-drawn sketch. These features are hyper stroke features, Stroke features, and bi-stroke features.

The proposed system reduces the problems with the existing graphical password but need to be more secure overall process, it is difficult because free hand sketching.

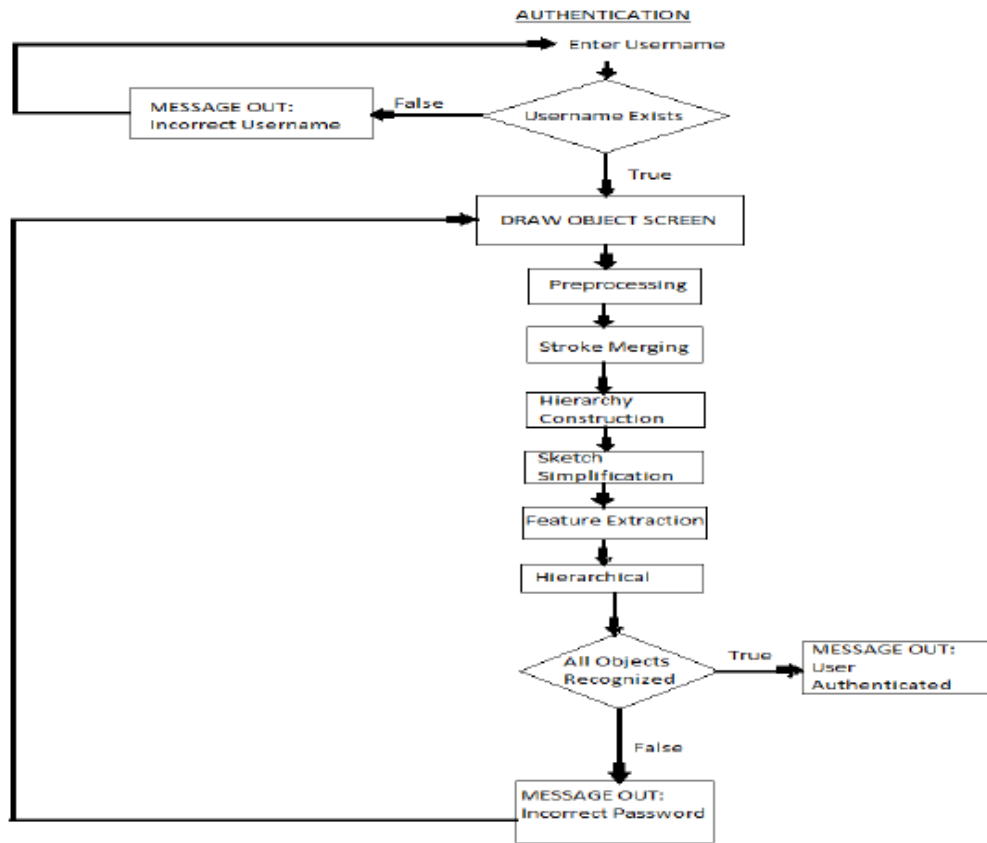


Figure (2.19) the registration [15]

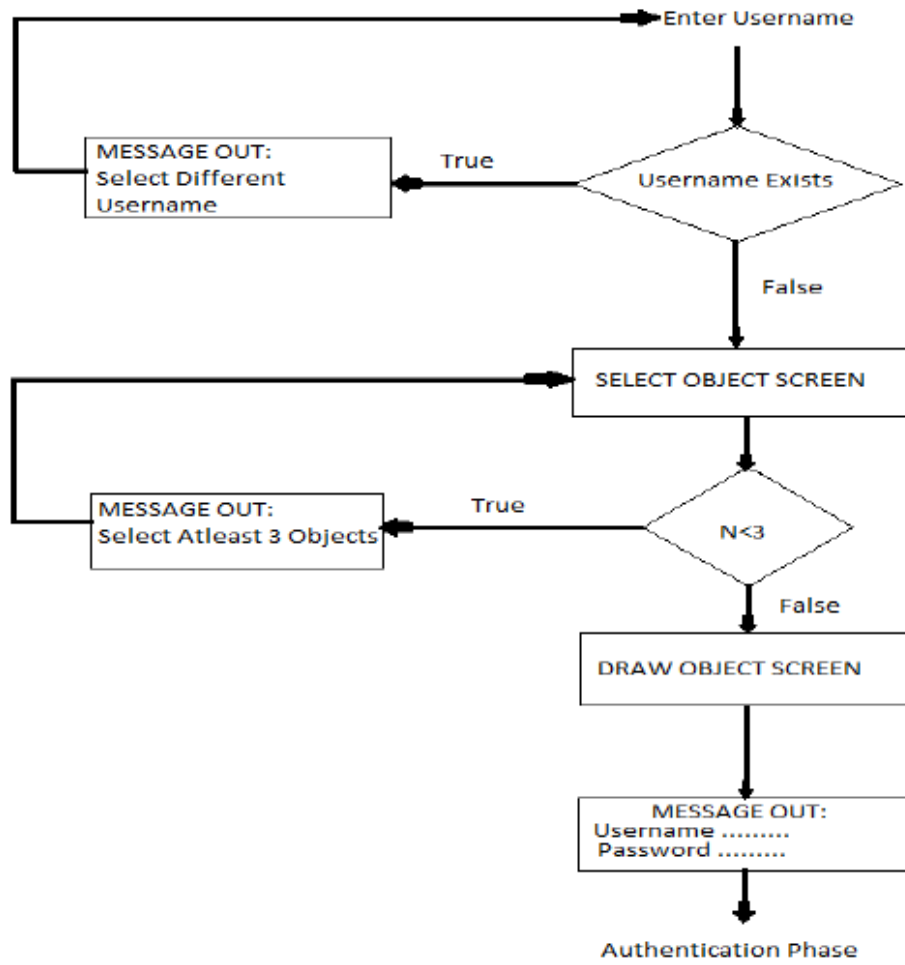


Figure (2.20) login [15]

Table (2.2) Related work

Study	Technique	Results	Open issue
2	click based and choice based approach	it is shoulder surfing attack resistance. By using the CAPTCHA, it is resistances to Malicious software attacks.	does not contain any hint, therefore, The user can forget the pixels Coordination.
3	recognition based technique	The system is more resistible for graphical password attacks as brute force and dictionary attack.	No login attempts. The password is fixed.
6	Recognition based and Sykuri	Resistance Guessing attack and Reduce the hotspot, increase the password space	Covers small fictions of all possible points and also focus on the individual clicks not complete password.
7	PCCP, Dead Zone concept, sound signature	Enhance the PCCP security using the dead zone as method for avoiding the shoulder surfing attack. Using the sound signature for setting up a new password.	Users cannot remember the audio file if not use it for long time. The login process is tedious to the user.
9	cued click point technique	Provide protection against online guessing attack and denial of services.	Decrease the usability and the user cannot remember the accurate coordination of the image.
13	watermarking technique, recognition based	The system has unlimited and unfixed number of images as password	Watermarking is still vulnerable to attacks like cropping or like gamma correction, compression or low pass filtering.
14	a recall based graphical password, OTP	The system reduces the task for the users to remember the images. provide multilevel authentication tries to avoid shoulder surfing attack	Entering many items is a tedious process to the user and takes time.
15	recognition and recall based graphical password	Reduces the problems with the existing graphical password.	Need to be more secure overall process. It is difficult because free hand sketching.

2.7 Summery

Authentication is one methods to resists the security attacks, therefore different authentication methods were invented with different techniques like knowledge based, token based and biometric based.

Knowledge based having different types, like text, graphical. But every type of these password is sensible to different type of security attacks. Text has many drawbacks as easy to forget, weak password, therefore graphical password was invented.

Graphical password is having many techniques to be used as recall based, pure based and recognition but still suffering from many attacks as shoulder surfing attacks, guessing attacks and other attacks. Therefore, to achieve the aim of the research, the objectives the methodology of the application will be discussed in the next chapter.

CHAPTER III

3.1 Introduction

The proposed system is a web application, it is used for online application authentication, works with every platform. This system is a combination of recognition based graphical password technique and one time password.

3.2 System components and platform

The system can work under windows operating system or any other operating system, because it is a web application. The system is consisting of a web server as XAMP or WAMP server or any type of web server and web browser like chrome or Mozilla Firefox.

The web server used was XAMP web server. The web browser also can be used any available versions but it is recommended to use update versions of chrome web browser. The database used in designing data base is MYSQL. Also used RSA to encrypt the password and combination of character and number to generate the OTP and used PHP language to implement the system.

3.3 The authentication system

The description below explains the implementation and the analysis of the proposed system and the system interfaces.

3.3.1 How the system works

It is an authentication online system using graphical password and OTP as authentication techniques, the system is a combination of using Jetafida scheme based recognition technique

with one time password. The system is divided into two parts, the first part is registration and the other one is login.

The registration phase is only two level, sign up and setting up graphical password. In sign up, the user enters the required information which are user name, password, and email and phone number then the system saves the data.

The system has a various validation rules to confirm the validation of the entered data to reduce the security attacks. In sign up, the system forces the user to enter the required fields (username, password, email, phone number) then the system checks of the user name, email and the phone number exists in the database and the correct syntax for email and phone number, if not exist redirect the user to next phase.

It used password policy such as the password length at least 6 character, for more secure the system used RSA cipher to encrypt the password using public key, to implements the RSA cipher used a PHP security library contains classes to encrypt and decrypt the strings.

However, if the user could not pass all the validations the system redirects the user to the registration page to start the registration phase again, otherwise the system sends the data to the data base to save and redirects the user to the upload page.

The second part in registration, is uploading images from the user hard drive, any number of images the user's wants. The system checks if the uploaded files are only images with file size (2MB), and allowable extension (JPEG, JPG, PNG), otherwise, the system displays error message. After uploading images, the system saves the images information into the database as images names, file size, file type, file paths and user id, then displays the uploaded images which uploaded by the user.

The user selects the images from the images set, the system forces the user to select at least three images as password, then save images in the database as the user graphical password. At last, the system sends successful message to the user and redirects the user to the login page. Below figure (3.2) shows the activity diagram for registration.

The login consists of two levels. The first level of authentication is sign in the user name and password. The system checks the data validation and filter the input data to resist the SQL injection attack, then checks if the user exists in the database or not, if exists the system decrypt the saved password and compared with the entered password. If they match, then redirects the user to next phase which is display the user's uploaded images for graphical password confirmation. Otherwise, the system gives the user three attempts to login, if failed the user's account will be disable for 2 hours.

After sign in successfully, the user reselects the images correctly from the images set, if they do not match the user will log out and redirect to login page. If success, the system generates OTP code and send it to the use's mobile via SMS with limited time to enter the password or the session will be destroy.

To generate the OTP, the system uses several of built in functions, first defines all the variables of upper and lower alphabetic and numbers, then suing substr function which is abstract a strings using the letter location number and how string to cut, in the same function using another function which is str_shuffle which is shuffle the string, the result is abstract numbers of sting and shuffle theses abstracted strings, the second step is mixing all these predefined variables , then using again the substr function with the str_shuffle function. The length of the password is 5 letters. To send the code to user's number an API of text local used to send to the user via SMS. Text local is providing a services as SMS gate way to send the code through the SMS API. To get the services must sign up using email and complete the sign up information then the text local will provide an API compatible with PHP code to use it to send any content., in this system uses the text local SMS API to send the verification code to the user.

When the user enters the OTP, the system will compare the entered code with the saved code in the database, if matches then the user can login to the system, otherwise, will log out and start again the login process, also the system can send the code again in case the user does not receive the code.

The system has a user dashboard, the user can update the current text password with new encrypted and saves it in data base. In addition, the user can update the graphical password either, the system deletes all the uploaded images by the user, then redirects the user to the upload page to uploads images and selects from images set the graphical password.

Login activity diagram in figure (3.1) shows all the main process of login starting sign in and confirm the graphical password, generate and send the code the user's cell phone until login to the system successfully. Registration activity diagram in figure (3.2) shows all the main registration process between the user and the server, from sign up the user information and upload the images, to choose the images as password and save them in database.

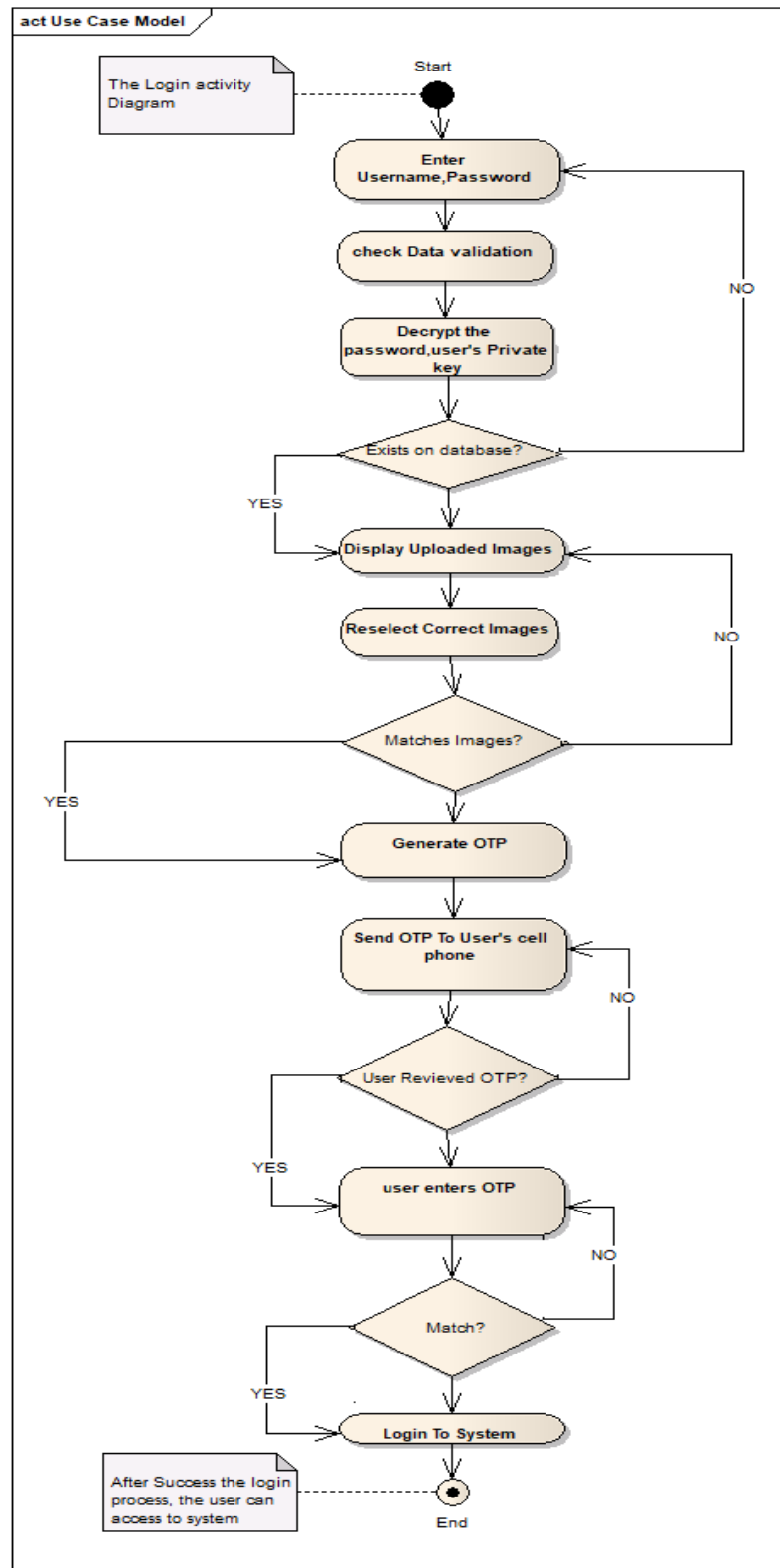


Figure (3.1) login activity diagram.

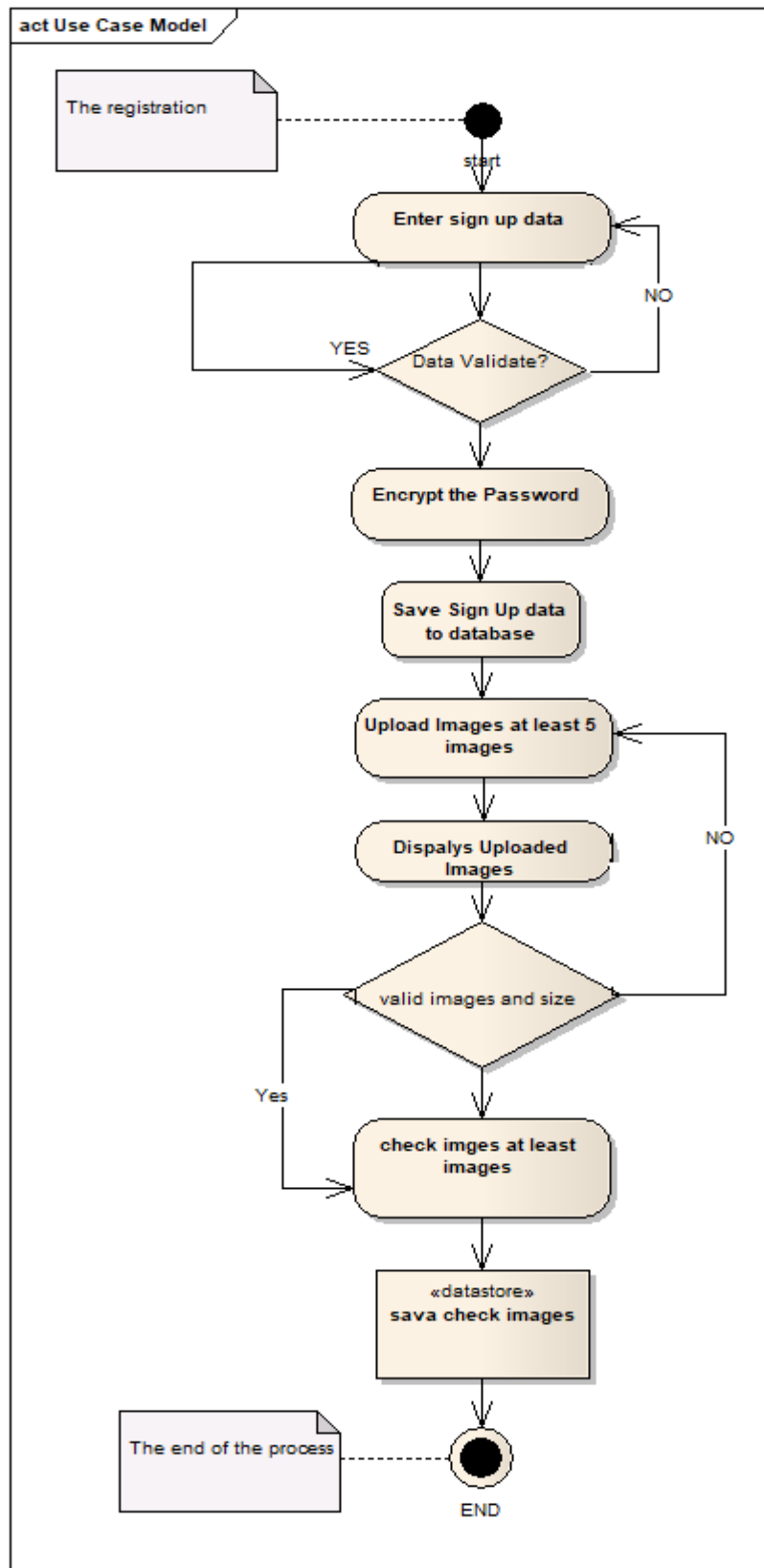


Figure (3.2) registration activity diagram

3.4 System analysis

This section will explain the components of the system, the creation of the database, the tables and their relations using different types of diagrams to clarify the designed system.

3.4.1 Software Development Methodology

UML have several different types of diagrams that can be used to describe a model from different point of views. These are Use Case, Sequence, Communication, Activity, and State chart, Class, Component and Deployment Diagram.

3.4.2 System use cases

The use case diagrams describe system functionality as a set of tasks and the interaction between the user and the system or between two systems. In this section used use case diagram and sequence diagram to describe the system operations. Below figure (3.3) describe the login use case, figure (3.4) describe registration use case, figure (3.5) describe OTP use case,

1. The user enters the user name and password.
2. The system checks the input data validation, and decrypt the entered password for comparison with password in data base. If not match, then back to step No.1.
3. The system retrieves the user's uploaded photos from the data base and displays the photos as set.
4. The user re selects correctly the images which selected in the registration, or get back to step No 3.

5. The system checks if they are the correct images from the data base. If not, return to step No 3.

6. The system generates OTP password and saves it in the data base, then sends it as code via SMS to user's phone, the system display a text box to enter the OTP code.

7. The user receives the SMS and enters the code.

8. The system checks if the code is match with the saved code in. If not, redirects the user to step No 6, otherwise the system will log out the user from the system and delete the sent verification code.

9. If success, the user can access to the target system.

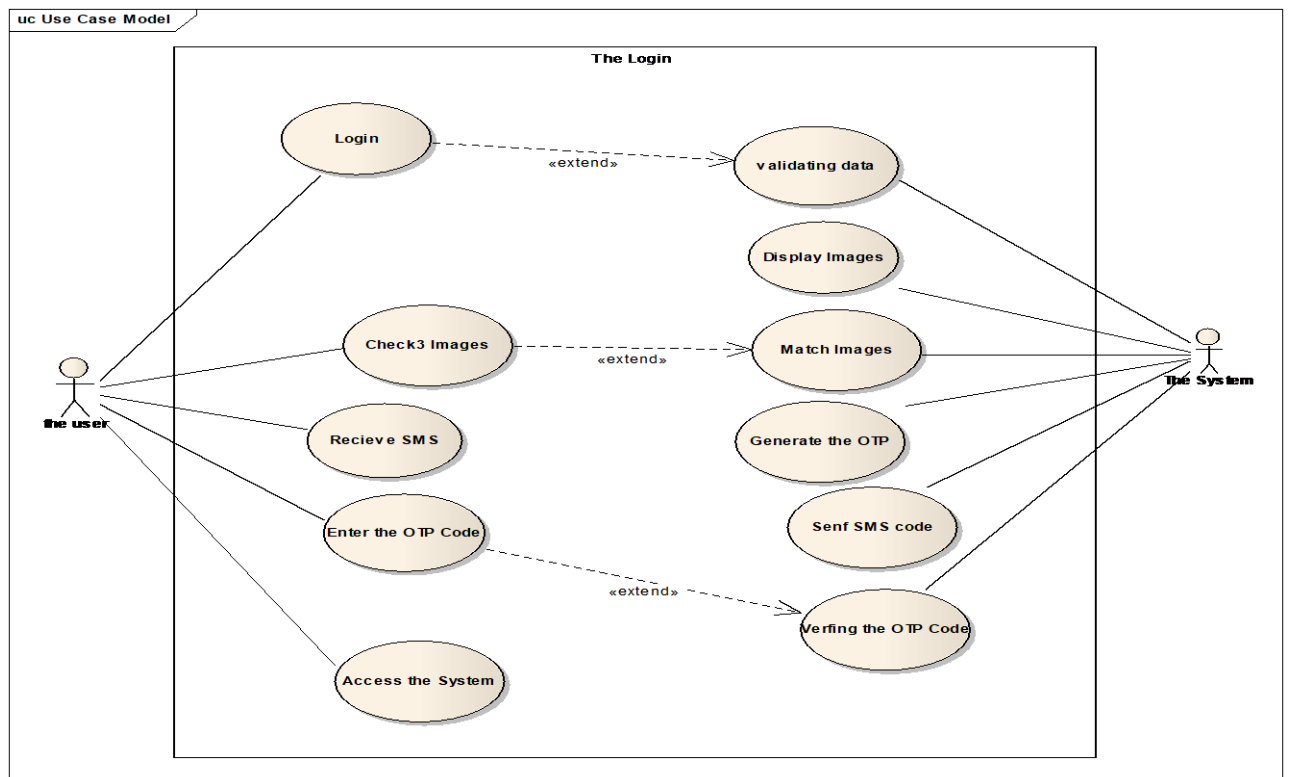


Figure (3.3) login use case

1. The system displays the registration form.
2. The user enters the required information for registration.
3. The system checks data validation, encrypt the password with the public key. If input data not valid the user will return to the step no 2.
4. The system redirects the user to the images upload page.
5. The user uploads at least 5 images or more, otherwise return to step no 4.
6. The system displays the images and save them in the data base.
7. The user must select 3 images at least or any numbers of images as graphical password.
8. The system saves the checked images and redirects the user to the login page.

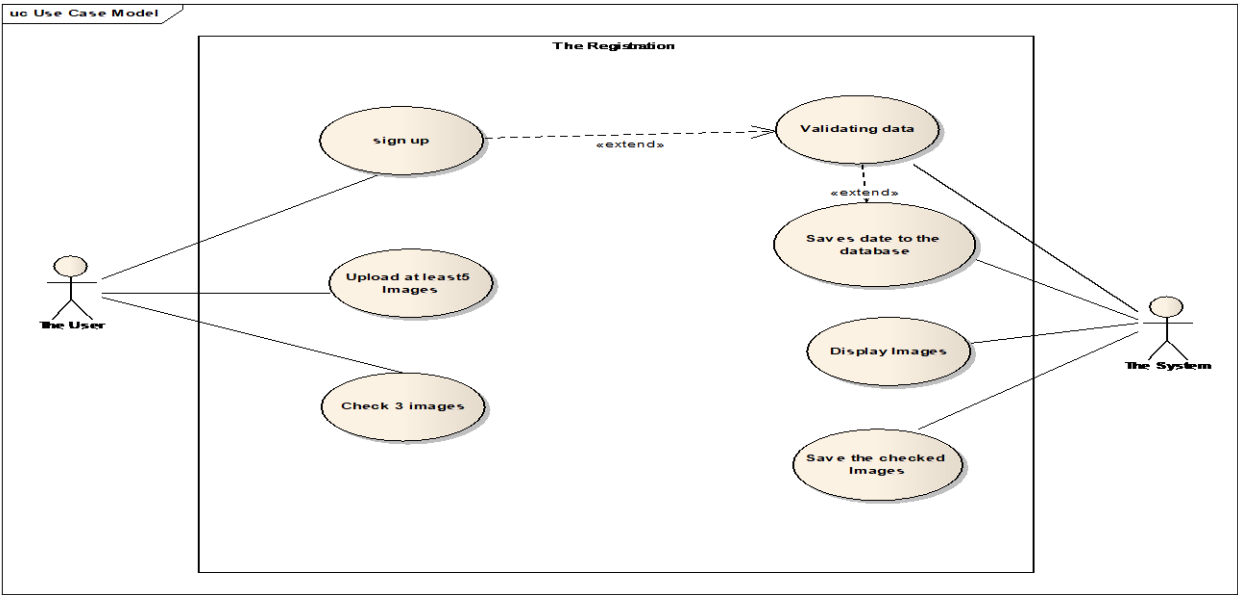


Figure (3.4) registration use case.

1. The system generates a unique password only for one time and sends the code to the data base.
2. The system sends the code to the user's cellphone.
3. The user receives the code, enters the code in the verification section after successfully enters the graphical password.
4. The system gives the user 59 seconds to enter the verification code, otherwise the systems log out the user from the system and delete the code from the database.
5. If the user successfully enters the code, the user access to the target system.

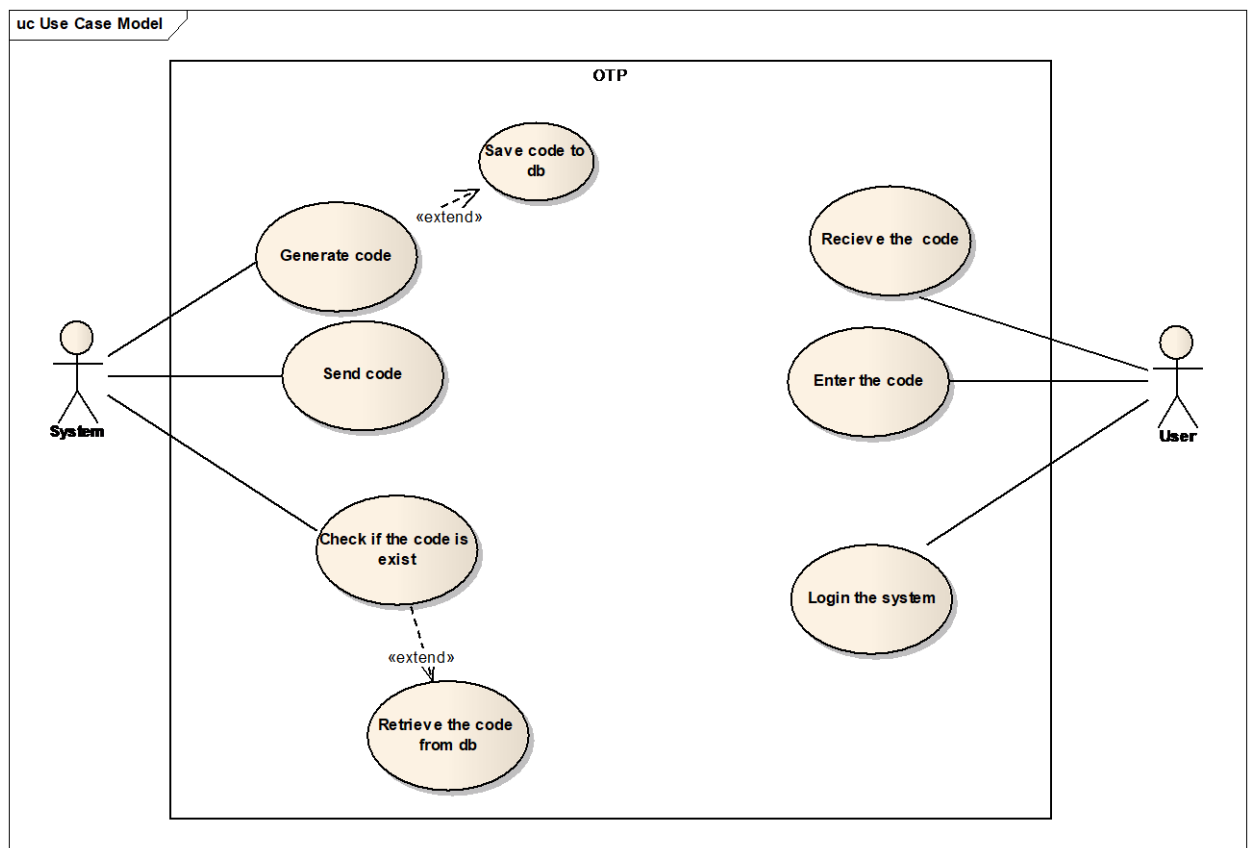


Figure (3.5) OTP use case.

3.4.3 The sequence diagram for the system

Sequence diagrams are used to represent or model the flow of messages, events and actions between the objects or components of a system. Below figure (3.6) show the login sequence diagram, figure (3.7) shows the registration sequence diagram, figure (3.8) shows the OTP sequence diagram.

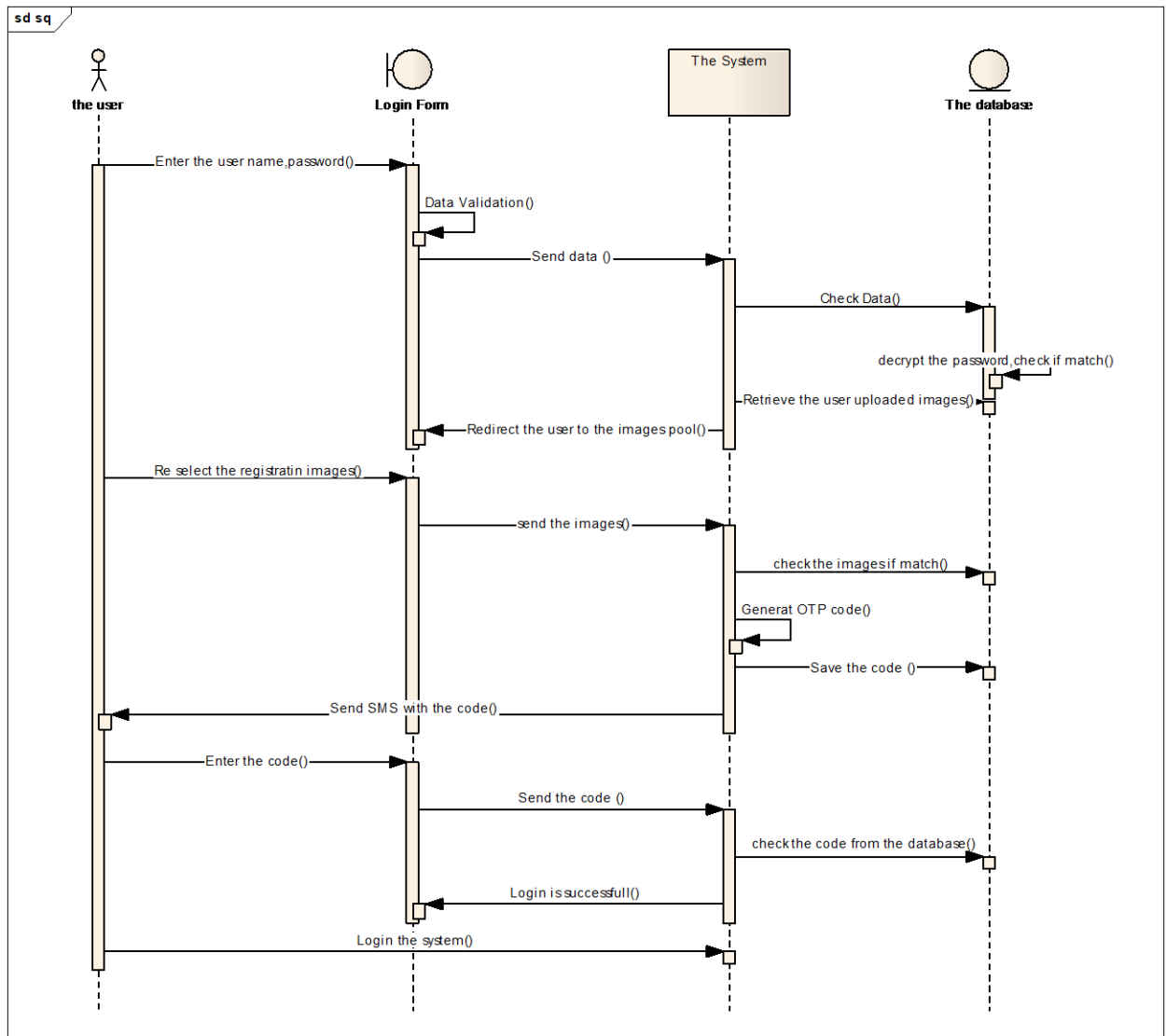


Figure (3.6) The Login sequence diagram

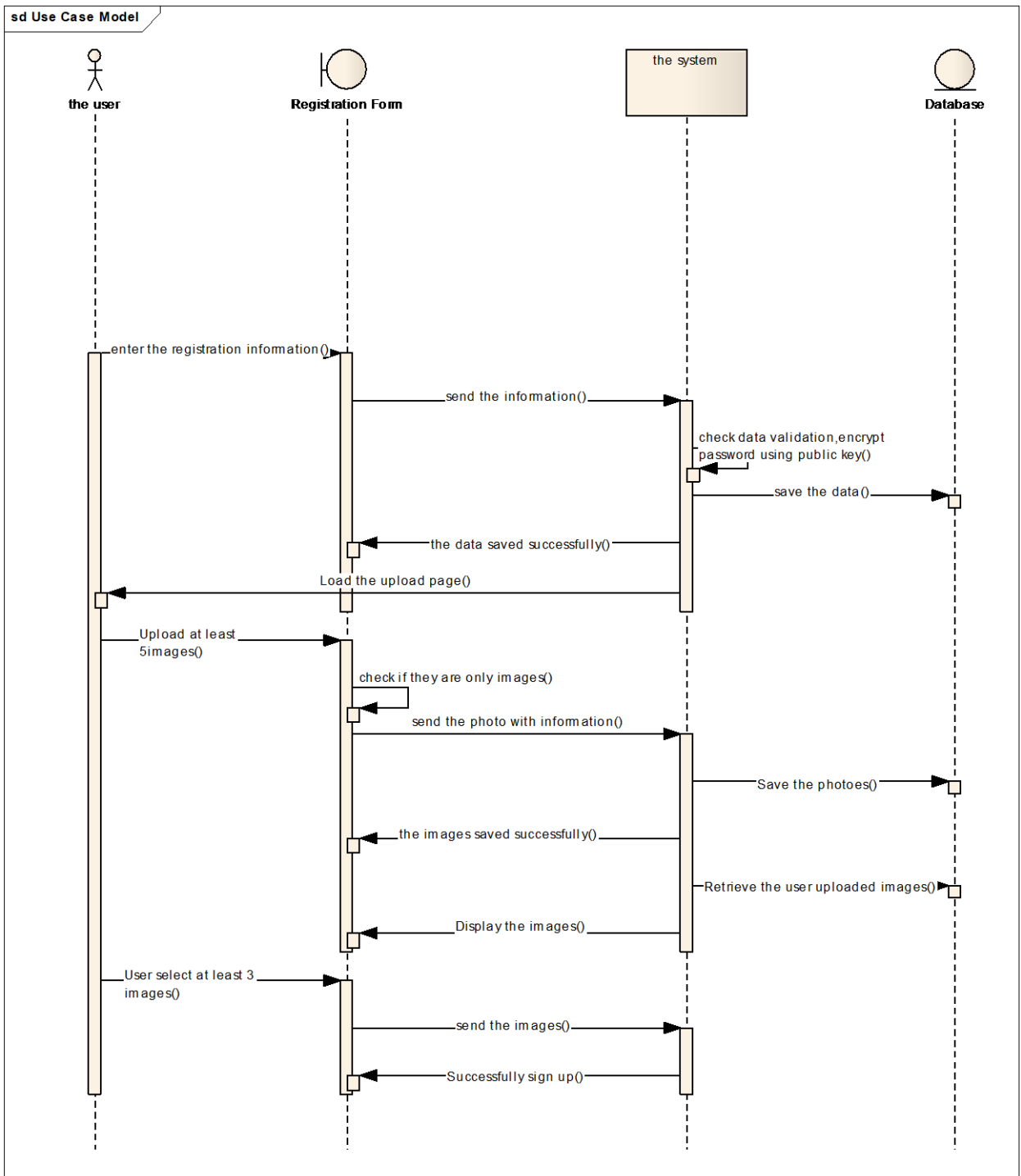


Figure (3.7) the registration sequence diagram.

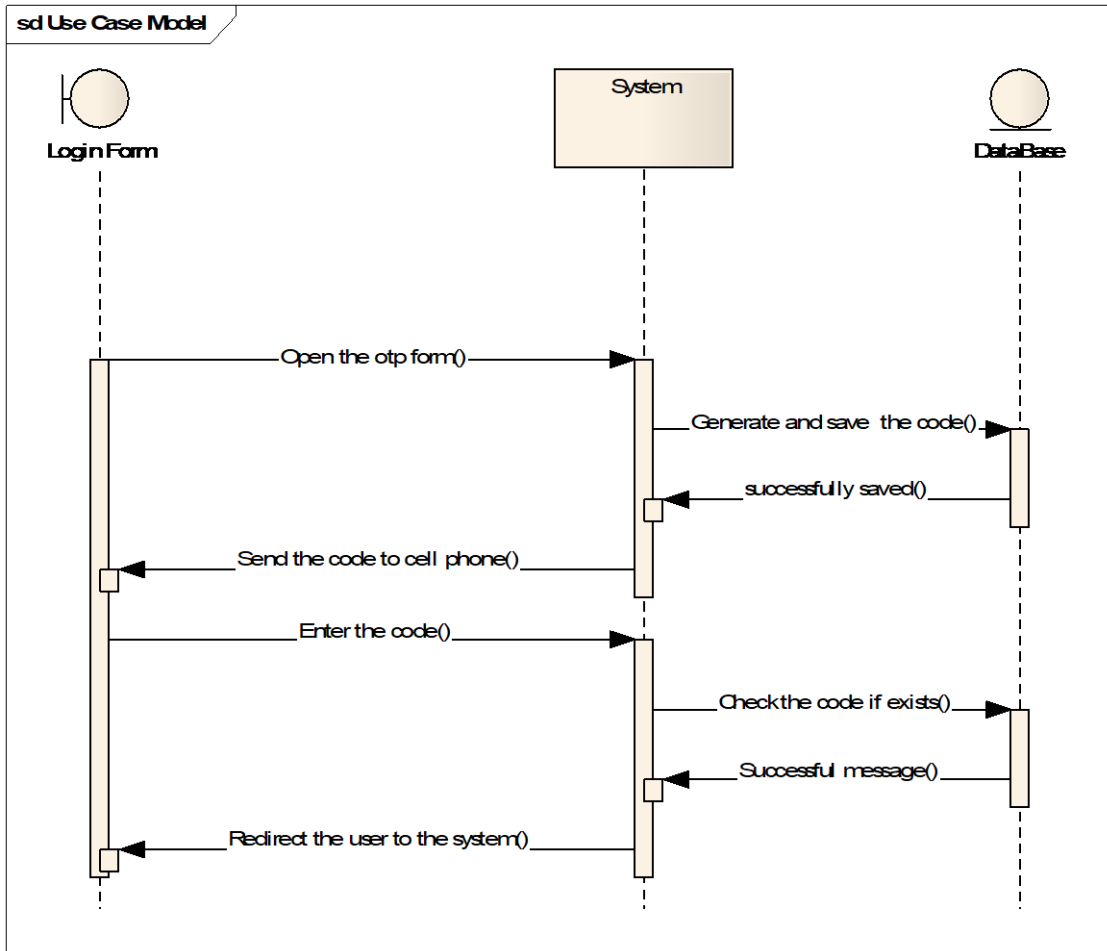


Figure (3.8) the sequence diagram for OTP.

3.4.4 The class diagram

A class diagram defines the classes of objects in the system, the attributes and operations of the classes, and the relationships between classes. Below figure (3.9) describes the data base table's relation.

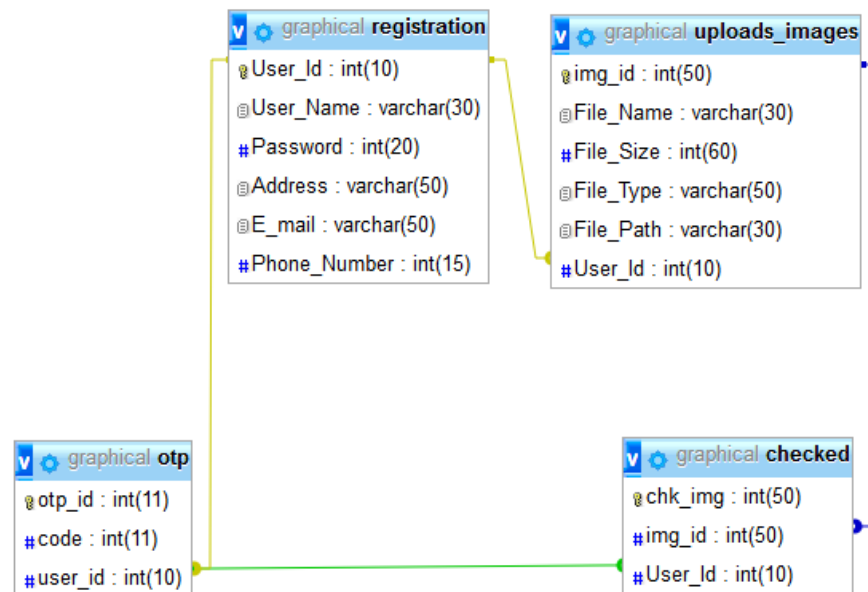


Figure (3.9) shows the data base table's relation.

3.4.5 The system's tables

Below Table (3.1) describe the registration and login data. Table (3.2) describes the photos data and images paths. Table (3.3) describe checked images data which selected in registration and graphical password data confirmation. Table (3.4) describes the data of generated one time password.

Table (3.1) registration table

The column name	constrain	Data type	length	The function
User_id	Primary key	Int	10	It is auto increment column
User_Name		Varchar	900	Contains the users names of the users
Password		varbinary	900	Contains the users registered password
E_mail	unique	Varchar	20	Contains the users email address
Phone_Number		bigint	18	Contains the users cell's phone number
Private_key		varchar	900	Contains the private key of RSA cipher

Table (3.2) uploads_images

The column name	constrain	Data type	length	The Function
Img_id	PK	int	50	Contains the images id, auto increment column
File_Name		varchar	30	Contains the Images names
File_Size		int	60	The length of the uploaded photos
File_Type		varchar	50	The images extension(jpg, png)
File_Path		varchar	30	Contains the uploaded images saved path
User_Id	Index	int	10	Contains the user's id who uploaded photos

Table (3.3) checked table.

The column name	Constrain	Data type	length	The Function
chk_img	PK	int	50	Auto increment
img_id	Unique	int	50	Contains the images unique ids
User_Id	Unique	int	10	Contains the user's ids whom checked the images in registration

Table (3.4) otp table

The column name	Constrain	Data type	length	The job
otp_id	PK	int	11	Auto increment
Code		int	11	Contains the generated one time password code
User_Id		int	10	Contains the user's ids whom checked the images in registration

CHAPTER IV

4.1 Introduction

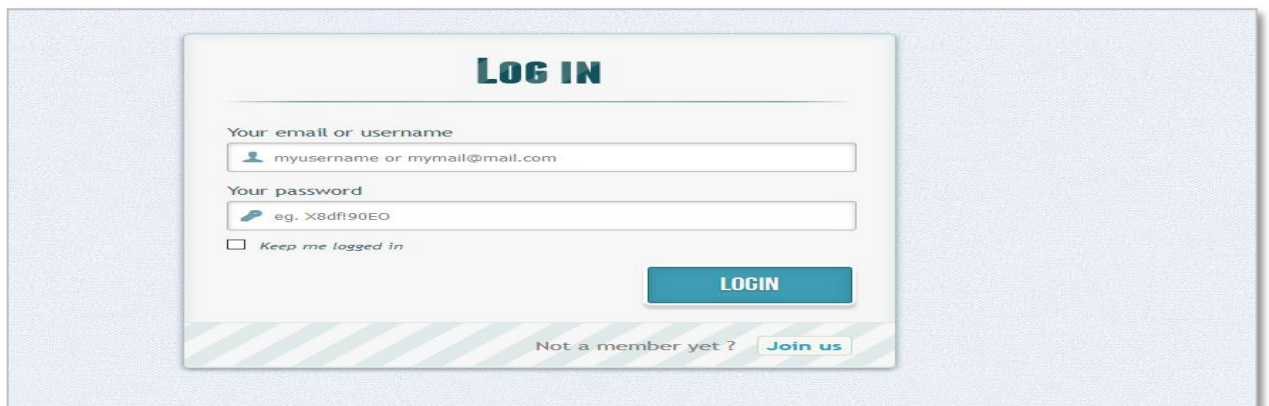
This system is an authentication system, it is having two phases, the registration and the login and each one has different interfaces and procedures. The next section, will explain the proposed system interfaces.

4.2 The system interfaces

This section will show the proposed system phases, login and registration and also will shows each pages for each one of them with clarification for the process of both phases.

4.2.1 The Login interfaces

The login has three levels for authentication and accessing the system, the text password, checks the graphical password, and enters the one time password correctly.

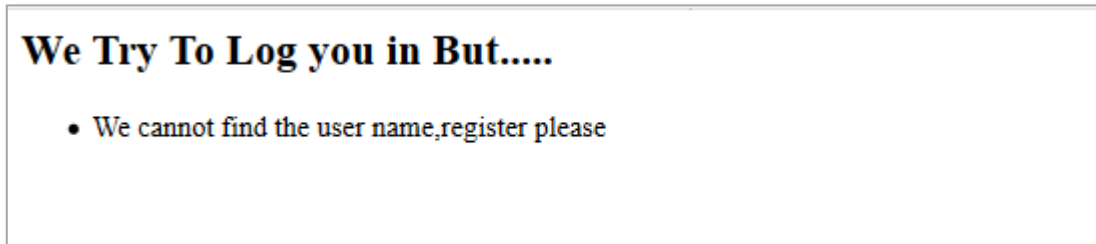


The image shows a login form with the following elements:

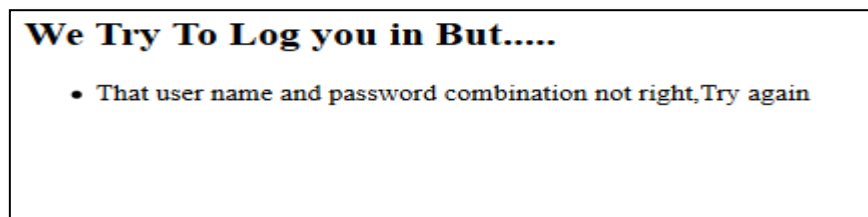
- Header:** "LOG IN" in bold, dark blue text.
- Form Fields:**
 - "Your email or username" with a placeholder "myusername or mymail@mail.com".
 - "Your password" with a placeholder "eg. X8df90EO".
- Checkbox:** "Keep me logged in" with an unchecked box.
- Button:** A blue "LOGIN" button.
- Footer:** "Not a member yet ?" followed by a "Join us" button.

Figure (4.1) login

Figure (4.1) shows login interface, in this interface the user enters the user name and the password, press login button to submit and redirects the user to figure (4.5) if the user entered the login data correctly. When the user tries to login, the system will check if the user name is exists in data base or not, if the user not registered, the system will display figure (4.2) error message, if the user enters incompatible user name or password, the system will display figure (4.3). If the user tries to login without entering data the system will display figure (4.4).



Figure(4.2) user not found error.



Figure(4.3) invalid user name/password.

We Try To Log you in But....

- enter the user name and the password

Figure (4.4) invalid login information.

Figure (4.5) below shows the second phase of login is graphical password, confirms the images correctly as password in this interface, the system displays all the uploaded images by the logged user, the user identifies and selects correctly the graphical password, otherwise the system redirects the user to figure (4.1). The last step and most important step is entering validate code which is generated by the system. The onetime password is sent to the user's phone.

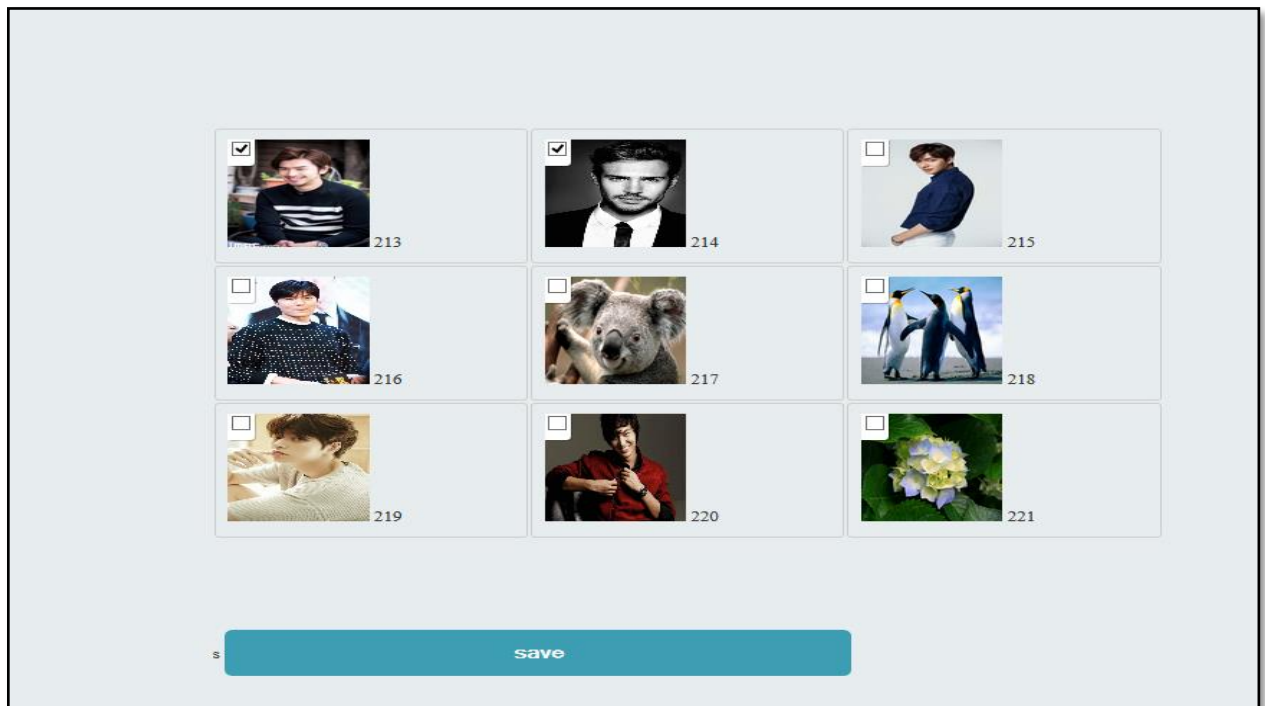


Figure (4.5) uploaded images.

Figure (4.6) bellows shows interface is the second part of confirms graphical password, after successfully identifies the images a text box will appear to the user to enter the code which sent to the user's cell phone via SMS. The system first generates a code, the system checks if the entered code is the correct code with saved one in the data base. Otherwise, redirect the user to figure (4.1). Also the system contains send the OTP again .in case the code not received by the user. If the code correct the system redirect the user to figure (4.7).

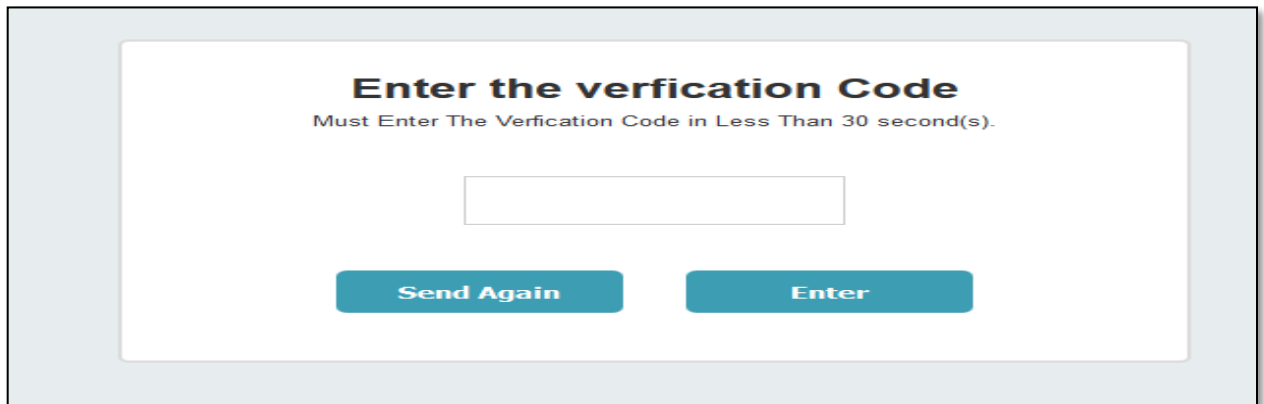


Figure (4.6) one time password verification.

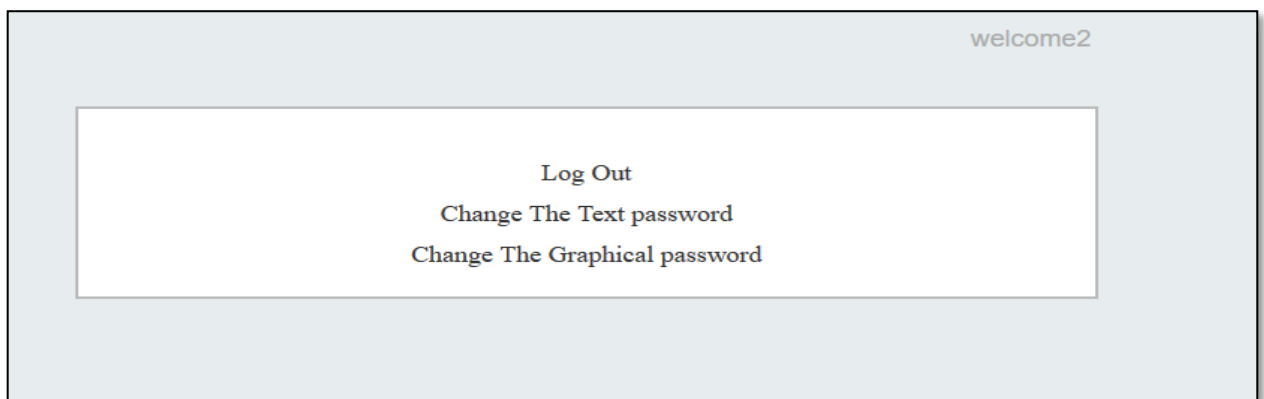
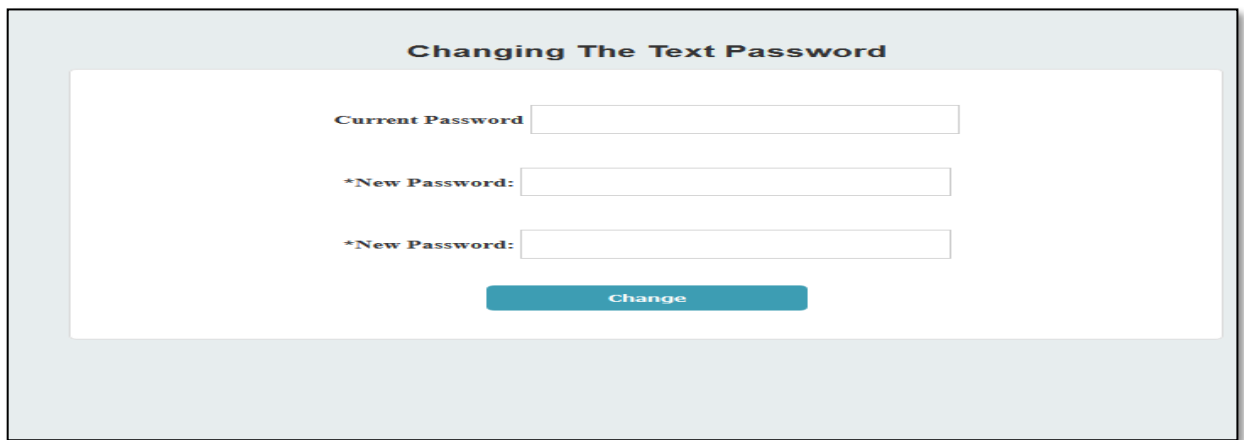


Figure (4.7) the user's dashboard.

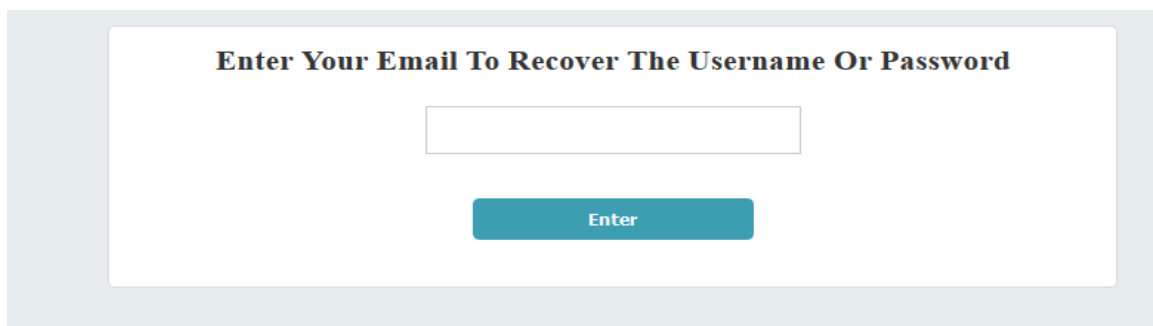
Figure (4.8) shows the password update for text and graphical password. The user can update the text password with a new one, enters the current password, and then enters the new one twice to confirm the new password.

Also can update the graphical password and uploads new images and sets a new graphical password. If the user wants to update the graphical password, the system redirects the user to figure (4.5), after upload the system will redirect the user to figure (4.6). Below Figure (4.9) shows the reset password using registered email address



The screenshot shows a web form titled "Changing The Text Password". It contains three input fields: "Current Password", "*New Password:", and another "*New Password:". Below the fields is a teal button labeled "Change".

Figure (4.8) changing Text password.

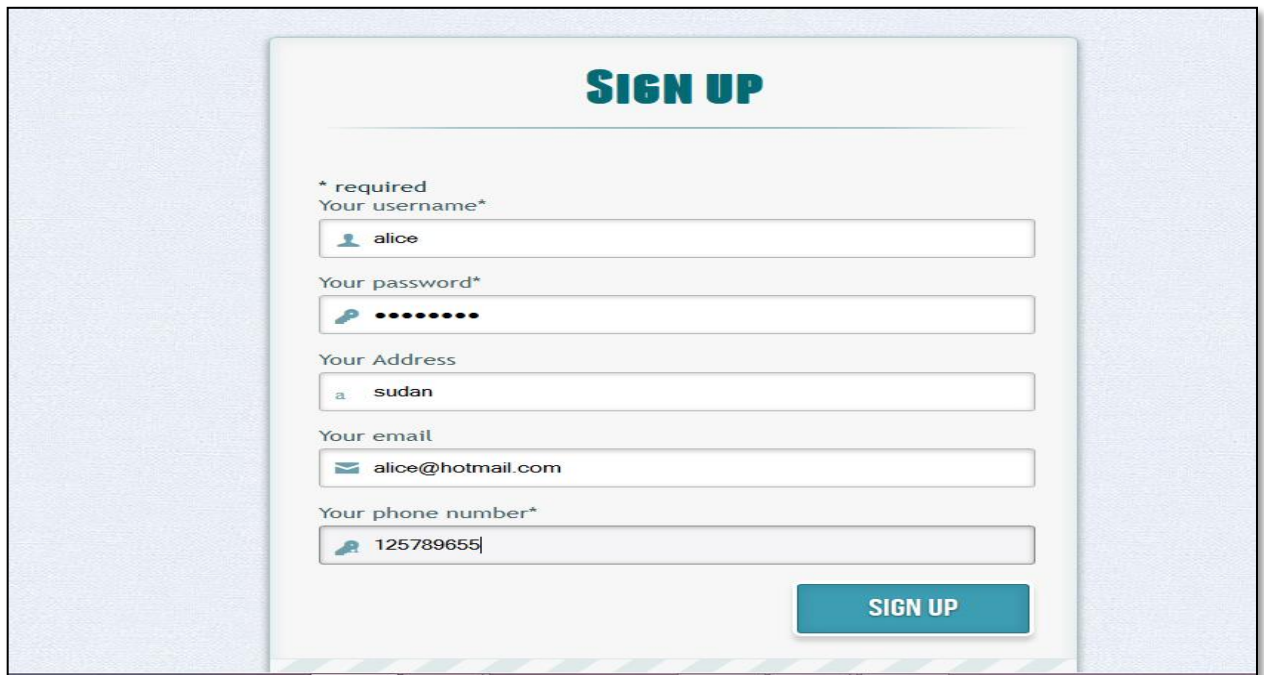


The screenshot shows a web form titled "Enter Your Email To Recover The Username Or Password". It contains a single input field for an email address and a teal button labeled "Enter".

Figure (4.9) Reset password

4.2.2 The Registration interface

This phase has two level, sign up for the text password and graphical password. Figure (4.10) shows sign up information, if the user not fill them, cannot completed successfully the text password login. Also the system checks if the username, email, phone number are existing in the database or not and force the user to enter at least 6 characters as password, press Sign up button to finish the first step in registration. Figure (4.11) shows the uploading images interface, the user can uploads any number of images to use some of them as graphical password. The user cannot upload images exceed 2MB size, also can upload only images with valid format (jpg, PNG, gif). To start upload the user press browse button and upload to complete uploading images, then the system displays the uploaded images as in figure (4.5). Figure (4.5) shows, system displays the uploaded images by the user, so the user can check images from the images group as password, and saves the checked images in the database as the user's graphical password, last the system redirects the user to the login page.



The image shows a registration form titled "SIGN UP" in bold teal letters. Below the title, there is a list of required fields, each with a small icon and a text input field. The fields are: "Your username*" with a person icon and the text "alice"; "Your password*" with a key icon and ten black dots; "Your Address" with a location pin icon and the text "sudan"; "Your email" with an envelope icon and the text "alice@hotmail.com"; and "Your phone number*" with a phone icon and the text "125789655". At the bottom right of the form is a teal button labeled "SIGN UP".

Figure (4.10) sign up.

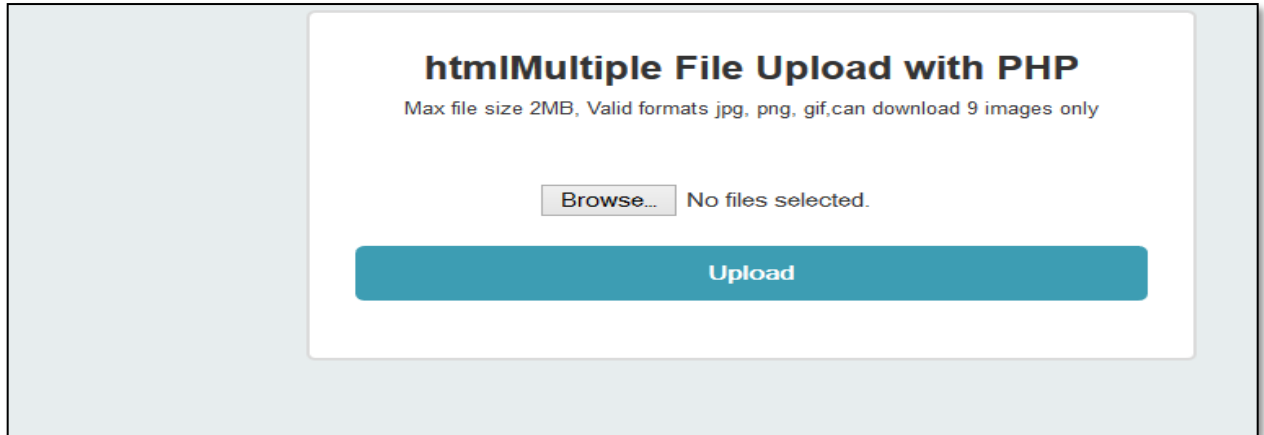


Figure (4.11) images upload.

4.3 Results

After system implementation and security analysis and how it resists for many security attacks below is the result of system implementation:

Can be used for all types of online systems and websites authentication, also decreases the unauthorized login by limit the login attempts to three times only and using RSA cipher to encrypt and decrypt password. It is user friendly, the system interface is easy and simple to use.

Easy to login, since the users remember images better. Resists for many graphical password attacks as shoulder surfing, because of using of OTP and recognition based technique. Not required any especial devices or software to implement therefore it is low cost for implementation.

4.4 The security analysis

The proposed system used many techniques to resist the security attacks as brute force and man in the middle and others password attacks, in the next session will explain how the system is resist for each attack and which feature function used in the system to resist the attack. Used recognition based graphical password in this project to increase the security and usability, proposed system using multiple authentication levels to provide more security.

This system is providing many techniques to resist the security attacks table (4.1) shows comparison between the password attacks resistance between the related works with proposed system, therefore it is resist for many security attacks as mentioned below.

Dictionary attack, since the recognition based graphical password involves mouse instead of keyboard therefore, it is useless against this type of graphical password.

Brute force attack, Whenever the password space increase, the password become more secure and vice versa, this system is flexible about the password space, it is gives the user option to upload as much as wants but also forces him to upload at least 5 images to make the password space secure, also forces the user to check at least 3 Images as graphical password. Also the system implemented password policy with length 6 character at least for password and other validations.

Surf shoulder attack, but this system provides a level of authentication to resist this attack by using the OTP, even if the attacker knows the graphical password, it is useless because the code only for one time use, therefore cannot access the system.

Guessing attack, the proposed system less the resist the guessing attack by making the user uploads the image as the user want, so the attacker will confuse about the user's favorites.

Spyware attack, the proposed system not use the keyboard to enter the graphical password, therefore it is useless to record the mouse or any input device movement or strikes of the keyboard.

Man in the middle, this system uses the RSA cipher to encrypt the password using the public key and private key to decrypt the password, only the authorize user can have the private key to decrypt the password. Assumption there is a third party between the two hosts has the public and the private key and distributes the key and generates the keys. Therefore, even the attacker somehow got an accesses to the data base cannot use it because the password is encrypted.

REFERENCES

5.1 Conclusion

Graphical password is using images as password, it was provided as alternative of text password because it's vulnerable for many security attacks. Graphical password has many different techniques to implement, it has three main categories the recall based graphical password, recognition based graphical password and hybrid scheme.

The security field provided many solutions to resolve the graphical password security issues. This research provided a system used recognition based technique and one time password to enhance the authentication process.

The designed system provided two levels of confirming user's identity, the first level is sign in using text password, decrypt and confirms the password using RSA cipher. The second level is identifying the graphical password correctly by selecting the correct images from the images set, then enter and the OTP verification code in the text box which is sends to user via SMS to the user's cell phone.

The analysis shows that the proposed system resists many security attacks such as dictionary attack, brute force attack and surf shouldering attack, also decrease the unauthorized login, the system is user friendly and easy to use.

5.2 Recommendation

To add another layer of security can use secure channel to transmit the data of the system. To provide more security and make the resistance of guessing attack more strong can add a feature to system the make the graphical password combination between user upload and system, also forces the user to choose from the system images as part of graphical

password. Uses different technique of graphical password like sykuri, because it is secure and easy to remember and it is user friendly

REFERENCES

1. Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle. "Comparison of Graphical Password Authentication Techniques". International Journal of Computer Applications. April 2015.
2. Delphin Raj K M ,Nancy Victor." A Novel Graphical Password Authentication Mechanism". International Journal of Advanced Research in Computer Science and Software Engineering. September 2014.
3. Nilesh Kawale and Shubhangi Patil." A Recognition Based Graphical Password System". International Journal of Current Engineering and Technology. April 2014.
4. saranya ramanam, bindhu js. "A Survey on different graphical password Authentication techniques". International Journal of Innvation Research in computer and communication Engineering. December 2014.
5. Jesudoss, Subramaniam . "A Survey On Authentication Attacks And Countermeasures In A Distributed Environment". Indian Journal of Computer and Engineering. May 2014.
6. Abuthaheer , Jeya Karthikka, T.M.Thiyagu." Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication". International Journal of Computer Applications. February 2014.
7. Nilesh Changune, Ganesh Shinde, Sagar Chaugule, Sandeep Helkar. "graphical password authentication using pccp with sound signature". IJRET: International Journal of Research in Engineering and Technology. Jan-2015.
8. Sarfraz Ahmed, S.Vivek." Recognition and Recall based Graphical Password Authentication". International Journal of Scientific & Engineering Research. July 2017.
9. Prashanthi Muddam, D.Raman. "Graphical Password Authentication for Secure Online Services". International Research Journal of Engineering and Technology. Aug-2016
10. Mohsen Gerami1, Satar Ghiasvand. "one time passwords via SMS". Bulletin de la Société Royale des Sciences de Liège. 2016.
11. [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem)), 31 oct-2018, 3:30pm

12. <https://en.wikipedia.org/wiki/Cryptography>, 14-11-2018, 4:30 pm.

13. Arash Habibi Lashkari, Azizah Abdul Manaf, Maslin Masrom. "A Secure Recognition Based Graphical Password by Watermarking". International Conference on Computer and Information Technology. 2011.

14. Veena Rathanavel1, Swati Mali." Graphical Password as an OTP ". International Journal Of Engineering And Computer Science. January 2017.

15. Aman Kumar, Naveen Bilandi."A Graphical password based authentication system based system for mobile devices". International Journal of Computer Science and Mobile Computing. April 2014.