DATA HIDING IN IMAGE BASED AUTHENTICATION USING COMBINATION OF ZERO-KNOWLEDGE PROTOCOL AND STEGANOGRAPHY

NURUL NADZIRAH BT ADNAN

Degree of Computer Science (Network Security) W

Faculty of Informatics and Computing

Universiti Sultan Zainal Abidin, Terengganu, Malaysia

DECLARATION

I would like to declare that this thesis is produced based on my own effort with the aid of obtaining information from the sources listed in the acknowledgement. I would also declare that this thesis is only been produced by my own effort and had never been produced and published by other students and also in other universities.

_____

(NURUL NADZIRAH BT ADNAN)

Date:

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful, all praise is only for Him, the King of the whole universe. May His blessing is upon his beloved Prophet Muhammad S.A.W and all his family. A very great hamdalah I served to Him for giving me enough health, time and maturity of mind to prepared this project and complete this thesis.

I would like to express my deepest appreciation to all who provided me the possibility to complete this thesis. A special thanks to my supervisor Prof Madya Dr Zarina Binti Mohamad for her guidance, ideas, help, criticsm and advice from the start until end that is helpful to me to complete this final year project.

Next, I was proud to thank my parents and my family for giving moral support and encouragement throughout my life whenever I feel like giving up. I also take this opportunity to give special thanks to all lecturers of Faculty of Informatics and Computing and my colleagues for their attentions, guidance and advice during my final year project. To all panel that involve in appraisal session and give useful comment and tips, I express my heartful gratefulness for their guide.

May Allah S.W.T bless all effort for completing this final year project. Thankyou.

ABSTRACT

One other most important aspects in information security nowadays is to understand when creating or improving the website's login procedure or known as user authentication. The concept that is useful to secure or authenticate the system is the simple text-based passwords. But, it is not secure enough and a burden on the user to remember. There is an alternative solution to these which is Graphical User Authentication (GUA) or imaged-based authentication. This is because humans are good at recognizing images rather than remembering password. This type of approach help user to create and memorize passwords easily. However, while applying the GUA, we might have attract the attacker that can capture the users mouse clicks and eavesdropping. In this project, the new strategy that combine the zero-knowledge protocol and steganography as the solution to these shoulder surfing attack to improve the security and usability in the system. In zero-knowledge protocol, user can prove that he know graphical passwords without sending it which means that user does not have to send the password to the verifier and reveal it to the other people. Meanwhile, in steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image. Hackers who trying to crack the password will eventually fail since the passwords were secure by

the encryption method along with the graphical based authentication and not be sent over the insecure channel anymore. Therefore, this is the secured approach to prevent the interception by the unwanted parties. My expectation in this project is to provide a better in network performance and secured authentication approach which is user-friendly.

ABSTRAK

Salah satu aspek yang paling penting dalam keselamatan maklumat pada masa sekarang adalah untuk memahami apabila membuat atau meningkatkan prosedur log masuk laman web atau dikenali sebagai pengesahan pengguna. Konsep yang berguna untuk menjamin atau mengesahkan sistem adalah kata laluan berasaskan teks mudah. Tetapi, ia tidak cukup selamat dan beban kepada pengguna untuk diingati. Terdapat penyelesaian alternatif untuk ini iaitu Pengesahan Pengguna Grafik (GUA) atau pengesahan berasaskan gambar. Ini kerana manusia pandai mengiktiraf imej dan bukan mengingati kata laluan. Pendekatan jenis ini membantu pengguna membuat dan menghafal kata laluan dengan mudah. Walau bagaimanapun, semasa menggunakan GUA, kami mungkin menarik penyerang yang dapat menangkap klik tetikus pengguna dan mengupingnya. Dalam projek ini, strategi baru yang menggabungkan protokol sifar pengetahuan dan steganografi sebagai penyelesaian kepada serangan melayari bahu ini untuk meningkatkan keselamatan dan kebolehgunaan dalam sistem. Dalam protokol sifar pengetahuan, pengguna boleh membuktikan bahawa dia tahu kata laluan grafis tanpa menghantarnya yang bermaksud pengguna tidak perlu menghantar kata laluan kepada pengesahkan dan mendedahkannya kepada orang lain. Sementara itu, dalam steganografi, pembawa penutup mungkin adalah pembawa cari yang tidak bersalah (imej, audio, video, teks, atau beberapa kod wakil digital yang lain) yang akan memegang maklumat tersembunyi. Mesej adalah maklumat yang tersembunyi dan mungkin plaintext, teks cipher, imej, atau apa-apa yang boleh dimasukkan ke dalam sedikit aliran. Bersama pembawa sampul dan mesej terbenam mencipta stego-carrier. Menyembunyikan maklumat mungkin memerlukan kunci stego yang merupakan maklumat rahsia tambahan, seperti kata laluan, yang diperlukan untuk

memasukkan maklumat tersebut. Sebagai contoh, apabila mesej rahsia tersembunyi di dalam imej sampul, produk yang dihasilkan adalah imej stego. Hacker yang cuba memecahkan kata laluan akhirnya akan gagal kerana kata laluan selamat dengan kaedah penyulitan bersama dengan pengesahan berasaskan grafik dan tidak akan dihantar ke saluran tidak selamat lagi. Oleh itu, ini adalah pendekatan yang selamat untuk mencegah pemintasan pihak-pihak yang tidak diingini. Harapan saya dalam projek ini adalah untuk menyediakan prestasi yang lebih baik dalam rangkaian dan memperoleh pendekatan pengesahan yang mesra pengguna.

Table of Contents

CHAPTER 1

INTRODUCTION

1.0 Project Background

Indeed, the internet and the usage of computer are rising up rapidly nowadays.

Computer security or common known as a cybersecurity is the protection of computer systems from the theft of or damage to their hardware, software or electronic data as well as from the disruption or misdirection of the services that they provide. Data or information will be protecting against harm that may come via network access and the code injection [1, 2]. To overcome this problem, many techniques will be considered and can be categorized as encipherments, routing protocols and data integrity authentication.

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server[].

Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID. Most users are most familiar with using a password, which, as a piece of information that should be known only to the user, is called a knowledge authentication

factor. Other authentication factors, and how they are used for two-factor or multifactor authentication (MFA).

Furthermore, authentication can be divided into two categories which is message authentication and entity authentication [1, 3]. Message authentication is the process to authenticate and verify the message to be sent by the sender and not modified or forged by the third parties. Meanwhile, entity authentication is the process of identifying a party to the other party can refer to a user, a process or a system. User authentication system is the most common entity authentication system implemented and used for decades [1]. And user authentication mechanisms are currently categorized into three main types:

1. Biometric authentication (something you are)
2. Token-based authentication (something you have)
3. Knowledge-based authentication (something you know).

Knowledge based techniques are the most well-known authentication techniques in this century and it include of text-based and graphic-based authentication method[]. Blonder was the first to introduce the concept of graphical various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords in 1996 [3]. Knowledge based authentication is generally classified into two categories: text based password authentication and graphical password authentication.

Based on some studies such as those in, humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a

result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically.

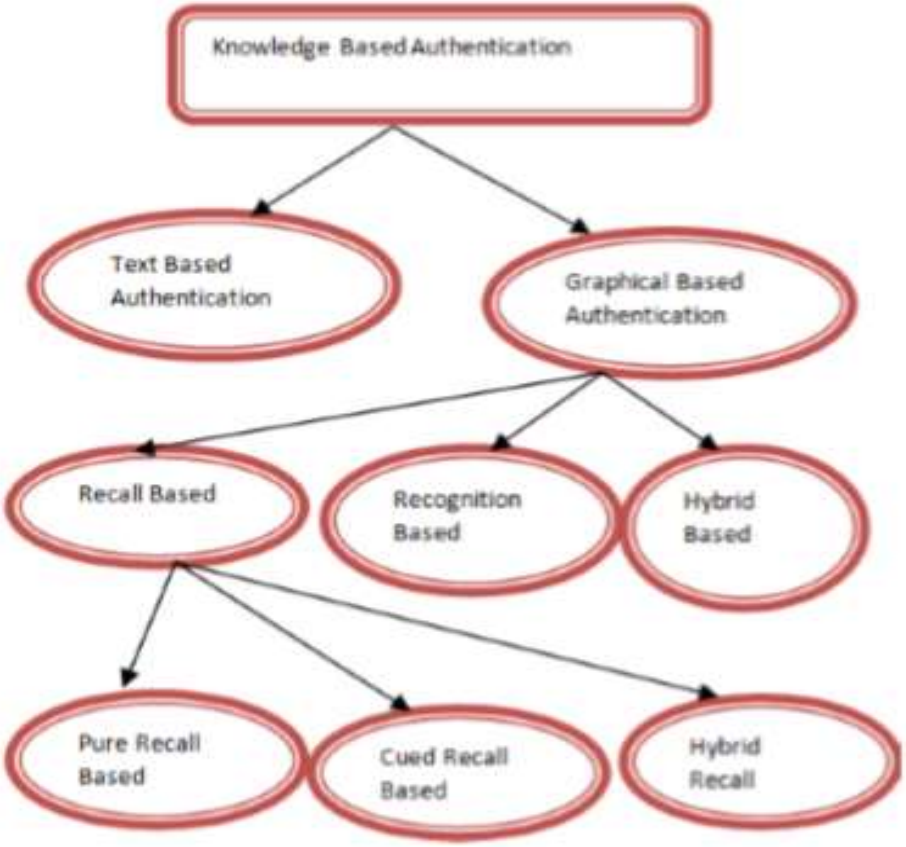


Figure 1 shows the diagram of knowledge based authentication

Graphical user authentication (GUA) is an authentication system that makes use of a graphical password which works by having the user select for images, in a specific order, presented in a graphical user interface (GUI).

Zero-knowledge protocol are one of the entity authentication which is widely used for verifying in authentication over the secure insecure channel. Zero-knowledge protocols were introduced by Goldwasser, Micali, and Rackoff (GMR) who have proven these protocols to be important models of computation in both complexity and

cryptography [3, 4]. User does not reveal anything endanger the confidentiality of his/her password in zero-knowledge protocol. The interactions are so designed that they cannot lead to revealing or guessing the password. Although after changes the message, the authentication system only knows that the user does or does not have the password, nothing more. The result is a Yes or No, just a single a bit of information.

Meanwhile, steganography is involving data hiding information in a seemingly innocuous cover message. In steganography we hide our secret information in some cover image such that one cannot track the message [2]. The original Image is called cover image and the image in which message is embedded is called Stego Image. Steganography can also be done with Text, video, audio and protocol steganography. There is a difference between cryptography and steganography. Cryptography helps us to keep message content in secret form while steganography helps to keep the existence of the message as a secret. If cryptography is forbidden to use then in that case steganography is very useful. Today there are many applications of steganography. It is used in user authentication so that data can be safely stored, it is used in smart identity cards where the information of the person is secretly stored in the image of the person itself. Some other applications are medical imaging, online voting system [3, 4].

COVER IMAGE: This image is used to hold the secret information.

STEGO IMAGE: Image holding the embedded message.

SECRET MESSAGE: This is the secret information which is to be embedded with the cover image.

Zero knowledge protocol are techniques for proving identity or ownership[]. Their combination is that possession of some information can be proved without

revealing that information. This is an interactive process whereby a prover convinces a verifier of a certain assertion. In this research, combination the concepts of steganography and zero-knowledge protocol in order to create a graphical based password in which no one gains enough information to falsely claim ownership.

1.1 Problem statement:

Current available authentication systems are suffered from many kinds of weaknesses and limitation. Computer security also involves safeguarding computing resources, ensuring data integrity, limiting access to authorized users and maintaining data confidentiality.

The security and usability problems associated with alphanumeric passwords as “the password problem” (Wiedenbeck, Waters, Birget, Broditskiy & Memon, 2005) [5]. The problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans [5, 6].

2) Passwords should be secure for example, they should look random and should be hard to guess, they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text [5].

The vulnerabilities, of the text-based password scheme have been well known. Users always tend to choose short-length passwords or passwords which are easy to memorize, hence, this situation makes the passwords susceptible to password crackers or hackers. Furthermore, text-based password in alphanumerical scheme is vulnerable to dictionary attack, brutal guessing, social engineering, key-loggers, hidden-camera, spyware attacks, shoulder surfing and etc.

Besides, the textual passwords have been the most widely used authentication method for decades. Combination of numbers and upper- and lower-case letters,

textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employee's passwords within 30 seconds [7]. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

1.2 **Objective**:

2.0 To propose the combination of the zero-knowledge protocol and steganography techniques in the graphical password to provide the authentication and confidentiality of the data [8].

3.0 To design an improved version of GUAS method with combination steganography and zero-knowledge protocol that able to achieve balance between the aspect of security, usability and reliability [9].

4.0 To implement an authentication approach based on graphical password using zero-knowledge. (To test the secure graphical password compared to text-based.)

1.3 Scope

The scopes for this project are identified to make the system development process easier. This project scope is more on how the system's password is make the system is more securely. For system's scope, system can view user's password and responsible to it. So, only system can verify or authorize the users by the password that user key-in.

For users' scope, users need to register and login before users can access the system. During register process, they need to choose ten images and they must click a point at anywhere on that images to embed the password into image or steganography. After that, they must login to the system and must select five images that they have selected during register process and also click a point that they have clicked during register. If the images selected are correct and in correct sequence plus the click point is accurate which is where the password was hidden, then the users will successfully login and can access the system.

If users select or click wrong password exceeds one minute, the system will automatically logout. This will prevent intruder from being able to repeatedly guess correct password or at least make it take a lot longer time to guess it.

1.4 Limitation:

To overcome the disadvantages of textual password we proposed the graphical password in a banking sector as a real time scenario. Graphical password and a virtual keyboard shuffling method is used to protect the traditional password attacks while we using textual password. Our proposal system overcomes the disadvantages of textual password attacks. Due to encryption of our data additional security will be provided

CHAPTER 2

LITERATURE REVIEW

2.0 Literature review:

This chapter provides an overview of previous research on the work of the graphical password authentication using combination of zero-knowledge protocol and steganography. It including a few articles and journals that related directly and indirectly to the secure graphical password. All those researches was described, summarized, evaluated and clarified.

2.1 Steganography

The word "Steganography" is a Greek word which means "covered or hidden writing". In other words Steganography is technique of hiding information behind the cover medium. Steganography can be done with Text, images, video, audio media and protocol steganography. In our work we are going to use digital image steganography because digital images have a large amount of redundant data and for this reason it is possible to hide message inside image file [1]. Image Steganography requires following elements to carry out the work:

- Cover medium: It is an image that holds secret message.
- The Secret message: it is message to be transmitted. It can be plain or encrypted text, images or any other data.

- The Stego-key: it is key used to hide the message (May or may not be used).

Data is hidden in such a way that nobody notices its presence in cover medium. The main motive of steganography is to hide the existence of communication [2].

The various types of steganography include:

a) Image Steganography: The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.
b) Audio Steganography: Steganography can be applied to audio files i.e., we can hide information in an audio file, it can be called Audio Steganography. The audio file should be undetectable.
c) Video Steganography: Steganography can be applied to video files also. If we hide information in a video file, it can be called Video Steganography. The video file should be undetectable by attacker.
d) Text files Steganography: Steganography can be applied to text files also. If we hide information in a text file, it is called Text Steganography.

2.1.1 LSB Image Steganography

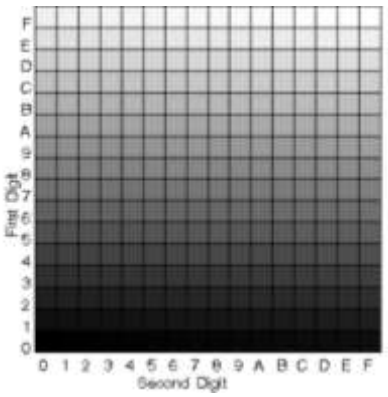
Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. Steganography is art and science of hiding the fact that communication is taking place. Secrets can be hidden in all types

of medium: text, audio, video and images. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image.

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by “1”. So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by “3”. This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied

to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

The following chart displays all 256 Gray-scale colors. [4] The gray-scale colour naming scheme uses a two digit hex value to define up to 256 shades of gray. In photography and computing, a grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black (also called bi-level or binary images). Grayscale images have many shades of gray in between. Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light, ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. Gray scale Shading Strengths (0=no color; 15=full color).

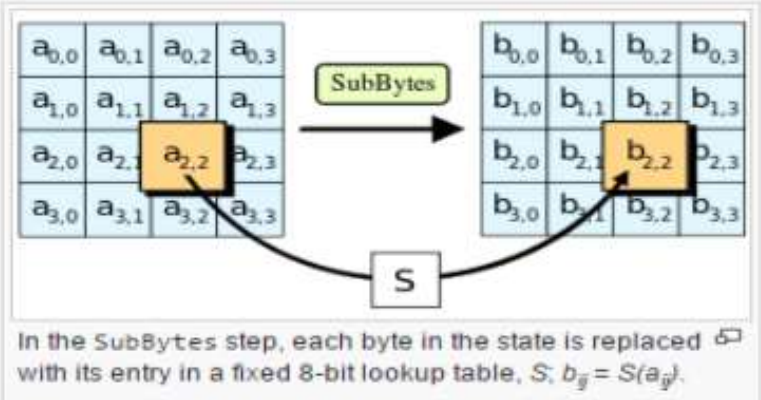


2.1.2 Advance Encryption Standard (AES-128 bits)

Advanced Encryption Standard (AES), also known as Rijindael is used for securing information[]. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. High security, mathematical soundness, resistance to all known attacks, high encryption speed, worldwide royalty free use, suitability across wide range of hardware and software are the characteristics of AES algorithm. Loopholes are there in DES and 3DES encryption algorithm but AES algorithm does not have such loopholes so far [3].

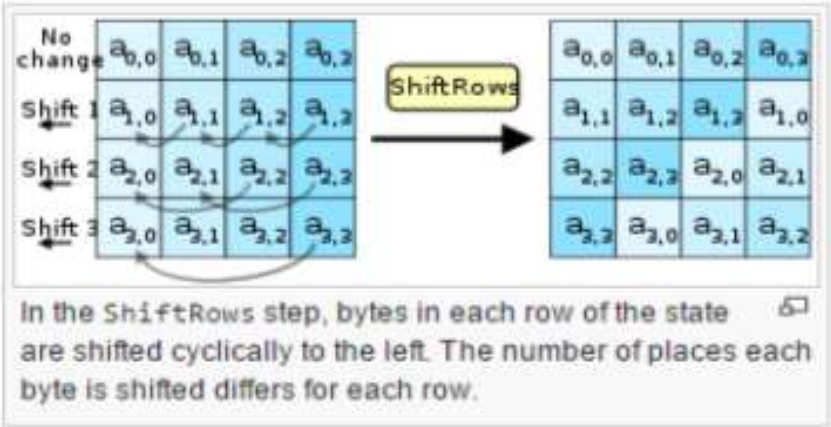
AES Algorithm consists of mainly four transformations, namely:

- SubBytes: In this transformation S-Box is used to perform byte by byte substitution of the block. Non-Linearity in cipher is achieved by this transformation. Multiplicative inverse over GF (28) is used to derive the S-Box.



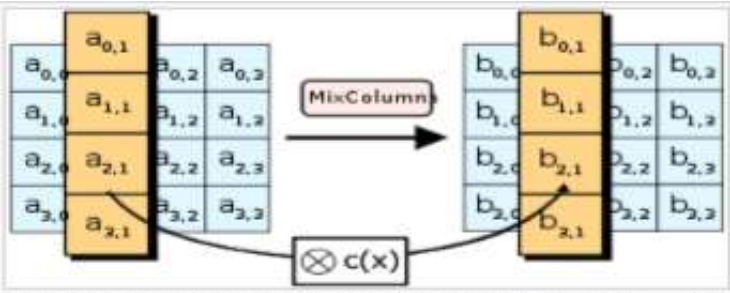
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

- ShiftRows: This transformation is performed on rows of the states. First row will remain unchanged but second, third and fourth row will be changed by cyclic one byte shift, two byte and three byte shift respectively. This operation makes columns linearly independent that's why AES degenerates four independent block ciphers.



In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

- MixColumns: This transformation is performed on every column in the state. Invertible linear transformation is used to combine the four bytes of the each column of the state. This transformation is used to achieve diffusion in the cipher.



In the MixColumns step, each column of the state is multiplied with a fixed polynomial c(x).

- AddRoundKey: Round key is combined with each byte of the state using bitwise XOR operation. 4X4 matrix is used to represent the original key consisting of 128 bits. This 4 word key is converted to a 43 words key.

2.1 GUA-Graphical User Authentication

The graphic-based scheme can be further divided into two groups: **recognition-based**, **pure recall-based, cued recall-based** and **hybrid recall-based** graphical techniques. Implement the recognition-based techniques, firstly, a user will be presented with a set of images and the user must get through the authentication by identifying and recognizing the images he or she pre-selected during the registration phase. However, recall-based techniques require a user to regenerate something that he or she created or previously chosen during the registration phase.

2.1.1 Recognition-based Techniques

Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

- D'ej'a Vu

Dhamija and Perrig developed a graphical authentication scheme based on hash visualization technique.

"We develop a prototype of D 'ej"a Vu and conduct a user study that compares it to traditional password and PIN authentication. Our user study shows that 90% of all participants succeeded in the authentication tests using D 'ej'a Vu while only about 70% succeeded using passwords and PINS. Our findings indicate that D 'ej'a Vu has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords). (R. DhamUa and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.)"

In the Deja Vu system, user will be asked to choose particular number of picture from a set of random images provided by a program. Later, user will be required to recognize the pre-selected pass-images in order to be authenticated. The results showed that almost 90% of all participants succeeded in the authentication session while using their technique, while only 70% successful accomplish using text-based passwords and Pins. However, the average time to complete the process is longer than the conventional approach, but has a much lesser failure rate. A drawback is that the server is required to store a huge amount of graphical material which may have to be transferred over the network, hence, delaying the authentication procedure. Another limitation of

this system is that the server also needs to store the seeds of the portfolio images of each user in plain text. In term of interface, the process of selecting a picture from picture database can be time consuming and tedious for the user.

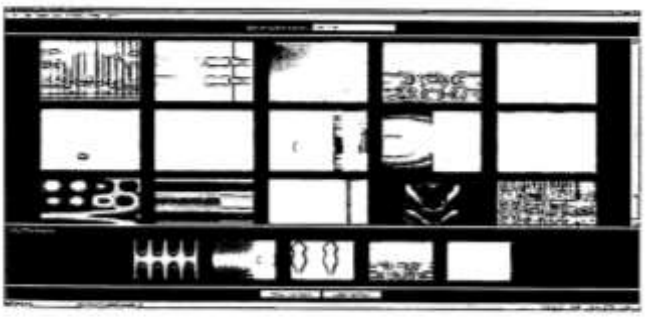


Figure 1: Example of random art images.

- Passface algorithm

In 2000 Brostoff and Sasse from Real User Corporation proposed a new graphical authentication scheme that is called Passface algorithm. To create a password the user will be asked to choose a certain number of images of human faces from the picture database. At authentication phase user will be required to identify previously chosen faces in order to be authenticated. The user recognizes and clicks on the known face, and then the procedure repeats several times. The majority of the users tend to choose faces of people based on the obvious behavioral pattern, which makes this authentication scheme kind of predictable and vulnerable to various attacks.

Fig 3. An example of Passface algorithm

2.1.2 Pure Recall-based graphical techniques

- Grid selection algorithm

In 2004, Thrope and van Oorschot further studied the impact of password length and stroke-count as a complexity property of the DAS scheme. In their study, they proofed that stroke-count posed significant effect on the DAS password space. The size of DAS password space decreases significantly with fewer strokes for a fixed password length. The length of a DAS password also has a significant impact but the impact is not as strong as the stroke-count. To improve the security, Thrope and van Oorschot proposed a “Grid Selection” technique. The selection grid is an initially large, fine grained grid from which the user selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password. This would significantly increase the DAS password space.

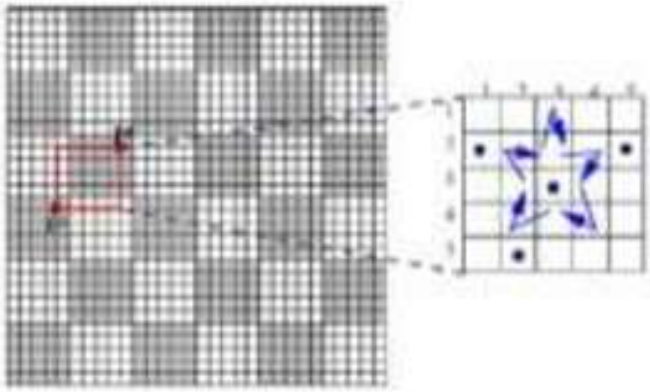


Fig 5. An example of Grid selection algorithm

- Draw-a-Secret (DAS) algorithm

In 1999 Jermyn, Mayer, Monrose, Reiter, and Rubin proposed a new graphical password scheme called Draw-a-Secret algorithm. This scheme allows user to draw a unique password on a 2D grid touches on a stylus sensitive touch screen. At registration phase the coordinates of the grids occupied by the drawn patterns are stored in order of the drawing. During authentication phase, the user is asked to redraw the picture by touching the same grids and in the same sequence . Unfortunately, most of the users over a certain period of time forget their drawing order. Another drawback is that the users tend to choose weak graphical passwords, which as a result makes this authentication scheme kind of predictable and vulnerable to various attacks .

- Pass doodle

Goldberg et al. proposed a technique called pass doodle [7]. In this technique, user has to draw hand written designs or text on a stylus sensitive touch screen. Some of the pass doodles drawn by the user as shown in the Fig4

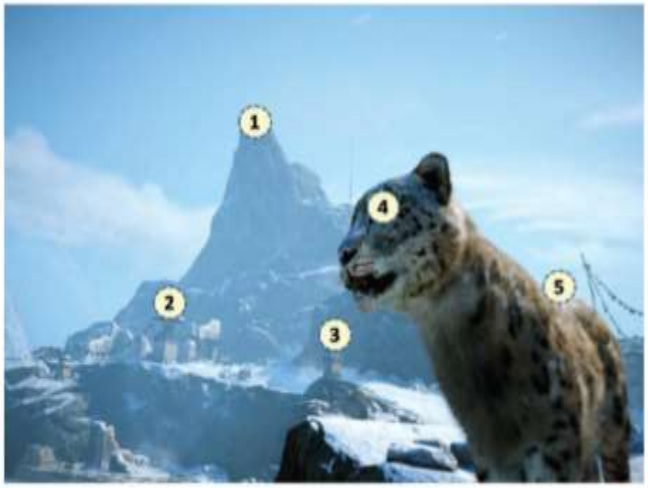
When login to the system, user has to draw the same pass doodle which was already drawn at the registration phase.

2.1.3 Cued Recall-Based Techniques

In cued recall based authentication system [6], the user has given some clues or hint implicitly to produce their passwords at the time of login stage. The widely used cued recall based techniques are Blonder, Pass points and cued click points are described in the following subsections.

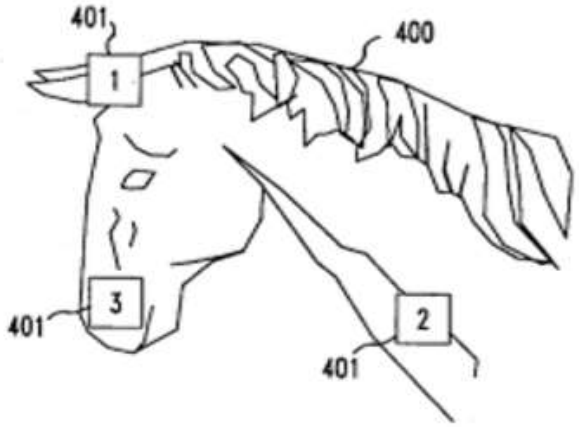
- PassPoint algorithm

  In 2000 Brostoff and Sasse from Real User Corporation proposed a new graphical authentication scheme that is called Passface algorithm. To create a password the user will be asked to choose a certain number of images of human faces from the picture database. At authentication phase user will be required to identify previously chosen faces in order to be authenticated. The user recognizes and clicks on the known face, and then the procedure repeats several times. The majority of the users tend to choose faces of people based on the obvious behavioral pattern, which makes this authentication scheme kind of predictable and vulnerable to various attacks.



- Blonder

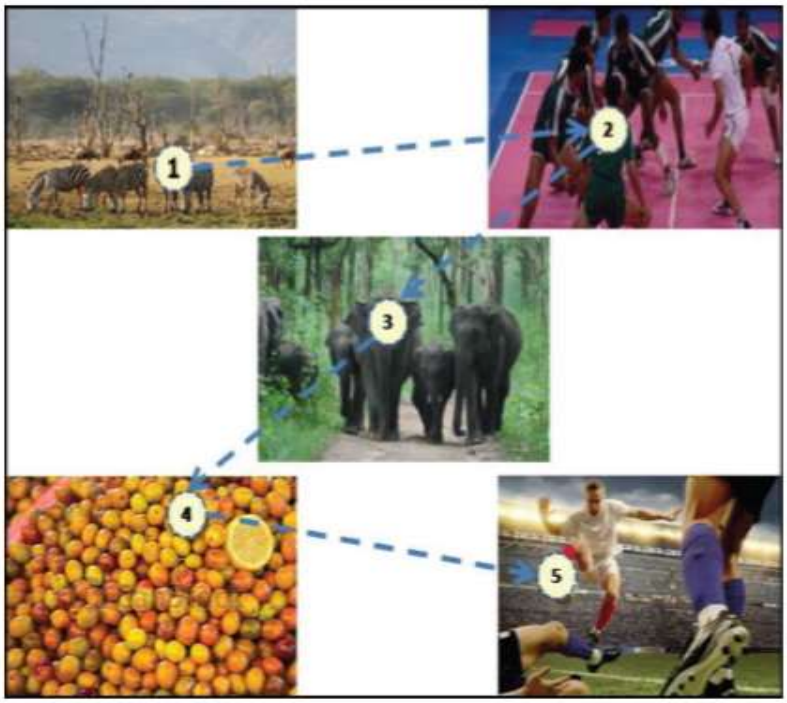
Blonder technique developed by Greg E [9]. Blonder in which a pre determined image shown to the user and user should locate or pointed to two or more regions on the predetermined image. In Fig 5, user selected tap regions in predetermined image.



The drawback of this technique is the number of clickable points position is relatively small, so the password becomes quite long to secure.

- Cued Click Points

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each of c = 8 images rather than on five points on one image. It offers cuedrecall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest clickpoint (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. As shown in Figure 1, each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.



2.1.4 Hybrid Recall Based Techniques

In this system, the combination of one or more schemes in pure recall based and also cued recall based techniques are used for hybrid recall based authentication.

- Click Draw based - Graphical Password Scheme (CD- GPS)

In this scheme, the combination of DAS in pure recall based technique and cued click points scheme in cued recall based technique is introduced. A set or collection of images in the database is called image pool. It consists of several themes of ten different images such as fruits, landscape, cartoon characters, food, sport, buildings, cars, animals, books and people. In this image pool, the user has to select only four images in a story sequence (i.e. the sequence of actions of images take part as per the selection of images chosen by the user and these actions of images easily memorized by the user) and the users may construct and remember their own stories as per the image selection. For example, out of ten images in the image pool, the user has to select only four images as shown with the number 6,3,4,7

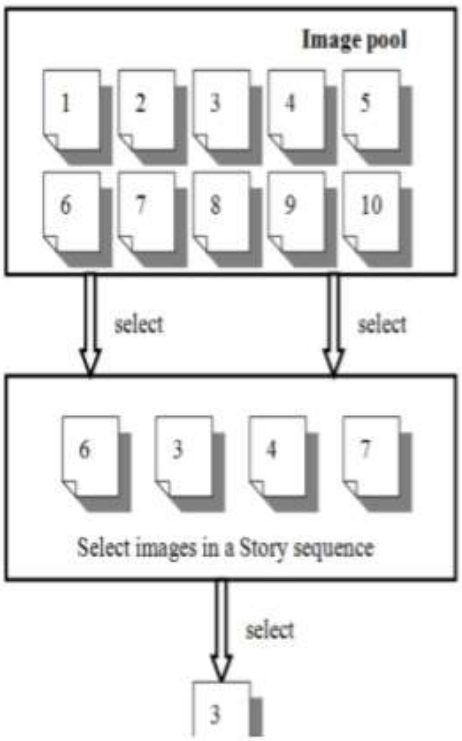


Fig 8: Image selection

Again, the user has to select only one image out of four images (6, 3, 4, 7) i.e. image 3 as shown in the Fig 8. User can draw the secret [5] on image during the final selection of the image. In Fig.9, the user click-drew a digital number of „T" as the secret, which consists of coordinates (13, 3), (13, 4), (13, 5), (14, 4), (15, 4) and (16, 4).

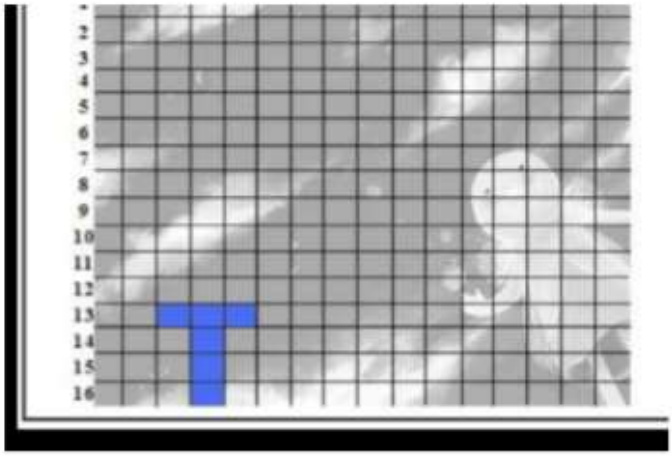


Fig 9: CD-GPS

Therefore, during the authentication, users should reproduce their secrets accurately in the correct coordinates on their selected images but without the need to consider and remember the click order [11].

Usability and Security The features of usability and security in recall based authentication systems could increase the user to select the better selection of passwords and also increase the effectiveness of password space.

2.2 Zero-knowledge protocol.

Zero-knowledge protocols also called as interactive protocols. The protocols are very promising for solving the problem related to verification of identity. They are protocols guranteed for proving your identity over an insecure medium without giving any information out to eavesdroppers that may enable them to identify themselves as you.

After the main theory introduced by Goldwasser, Micali and Rackoff(GMR) in 1985, A. Fiat and A. Shamir proposed a first practical solution in 1986 which is applicable to the computational power of that time[4]. The scheme of Fiat-Shamir is a trade-off between the number of authentication numbers stored in each security microprocessor and the number of witness number to be checked at each verifications[24].

- Sign-In Seal (fig.4):

A sign-in seal is a secret between the computer you set it up on and IBA. Therefore, when you sign in to IBA from this computer, your sign-in seal tells you that you are seeing a genuine IBA site, not a phishing site. Your sign-in seal is associated with your computer, not your ID. It is a convenient way to instantly recognize a genuine IBA sign-

in page and be sure that you are not on a page created by fraudsters attempting to steal your IBA ID and password. Because we associate your sign-in seal with your computer, after you create as seal, there are no additional steps to signing in. Even if a hacker knows or guesses your ID or other personal information, they cannot use it to discover your sign in seal. You can customize your seal either by creating a text seal or by uploading an image.

A user authentication mechanism's main goal and the most important requirement is security. Likewise many strategies that exist are primarily for attacking authentication to the system. Therefore schemes must be evaluated according to their vulnerabilities and susceptibility to different attacks because there are no systems that offer perfect security. Shoulder surfing attack refers to obtaining the password of a user when login by direct observation when user not adware or using external recording devices. Most of the graphical password schemes are vulnerable to shoulder surfing attacks. Only a

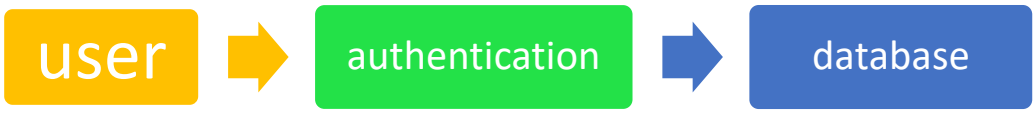
few of recognition-based technique are designed to resist shoulder surfing and none of the recall-based techniques are considered resistant to shoulder surfing. Therefore to overcome these problems, this project aim to research in combination of recognition based technique and zero-knowledge protocols.

CHAPTER 3

Methodology

3.0 Introduction

Methodology is a set of activities that done based on particular principles, rules, disciplines or procedure in the project. It is the important phases in the project development. In project development methodology is a framework that used to structure, plan, and control the process of development an information system. There are various model methodologies that can be used in developing the system or project such as use-case diagram, sequence diagram and flowchart as logical model. Each model has its own advantages and disadvantage. So, in the development methodology of this system or project, it explain about the approach used to develop the system, including the phases of development, justification for the choice of methodology and system requirements in terms of software and hardware.



3.1 Logical Model

In planning, analysis and design phases, usually this logical model will be used. Logical model used in imaged based to represent somethings from input relationships to activities and also output. The process of this graphical user authentication is divided into 3 phases, which are registration, login and authentication. This model will help or act as a tool to generate the effectiveness of the system known as logical framework.

3.1.1 Framework

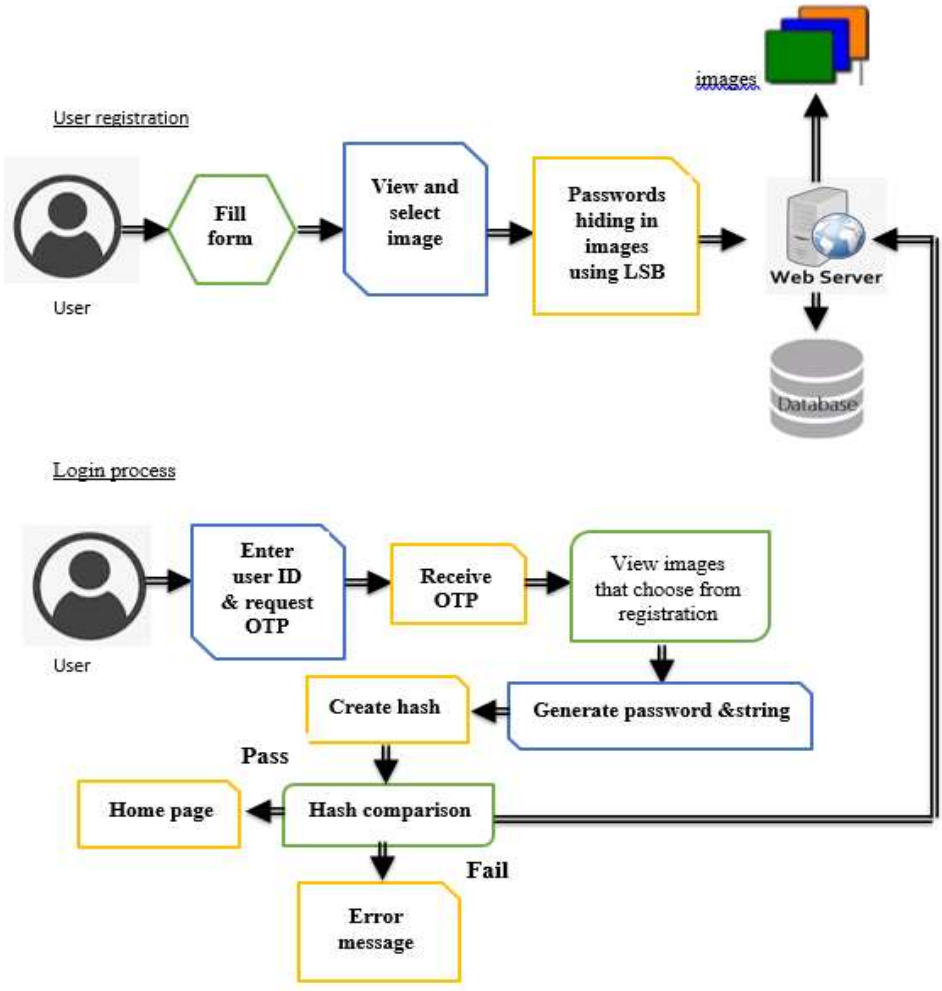


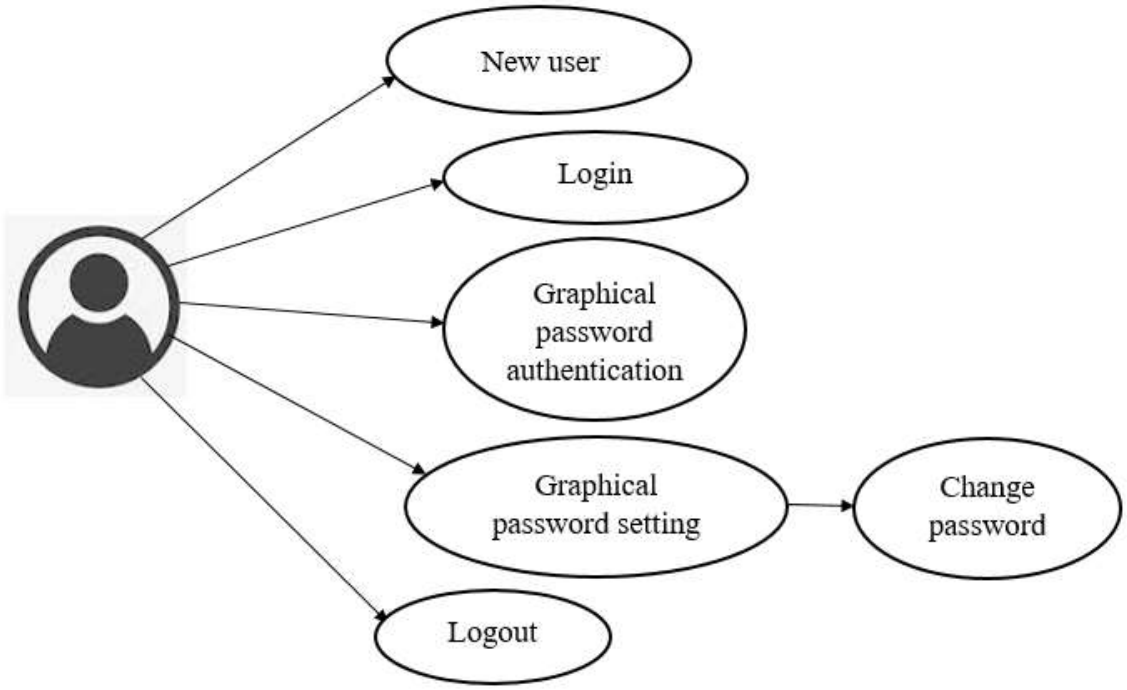
Figure 1: Framework of graphical authentication

Framework is a sketch of following process that shows how the system works and happen. System architecture or the framework is a conceptual model that defines the structure, behavior and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system.

Figure 1 shows that users can register to system by fill the form which is key in the first name, last name, username, email, phone number and it will view some images to be chosen. We need to select a few from that images. Then, users need to write the password so that it can embed to the image that chosen earlier. After that, the registration information include the images will be save in database. During login phase, users must enter the registration information again which is username and remember the selected images that include the password that in the picture. Then, system will compare with the information in database. If the result between registration and login information is same, so users will get the successful notification and can access the system, otherwise, users will get the error messages and need to enter the login phase once again.

3.1.2 Use Case Diagram

A use case diagram is a dynamic or behaviour diagram in UML. Use case diagrams model the functionality of a system using actors and use cases. Use cases are a set of actions, services, and functions that the system needs to perform. Use case diagram consists of four components includes boundary, the actor, the use cases and the relationship between actor and use case. Use case diagrams are used to gather the requirements of a system including internal and external influences. These requirements are mostly design requirements. Hence, when a system is analysed to gather its functionalities, use cases are prepared and actors are identified.

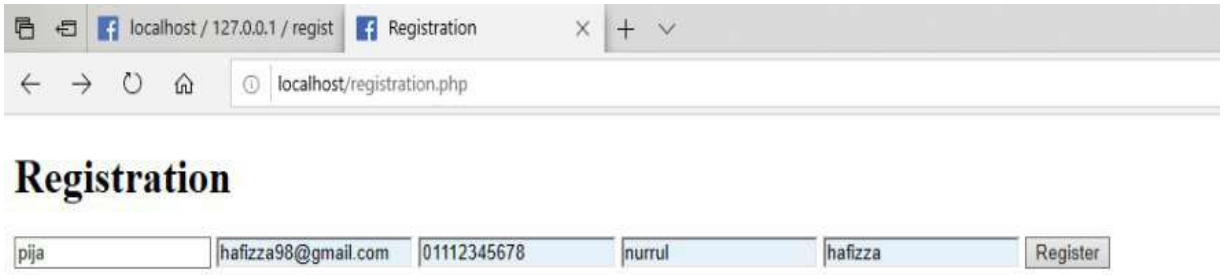


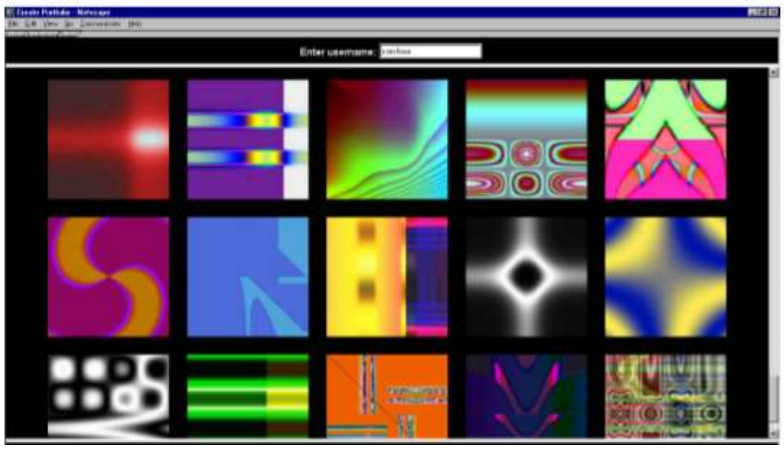
In the above Figure 2 use case diagram of user for graphical password

Actors can be defined as something that can interacts with the system. From this diagram, the new user will register as a new user and login. The user will choose the random art image from database. The user also can change the password in graphical password setting which that embed in the image.

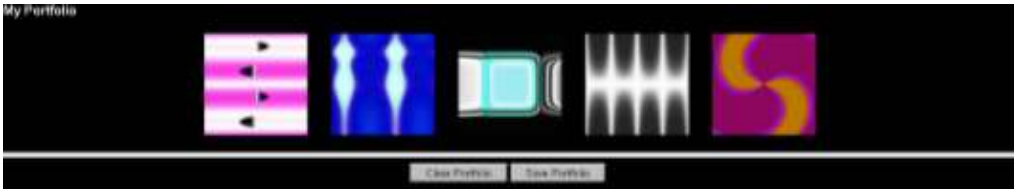
3.1.2.1 User registration

First, user starts by registers into the database so that they can login. User is prompted to choose a username and a few pictures password from database.





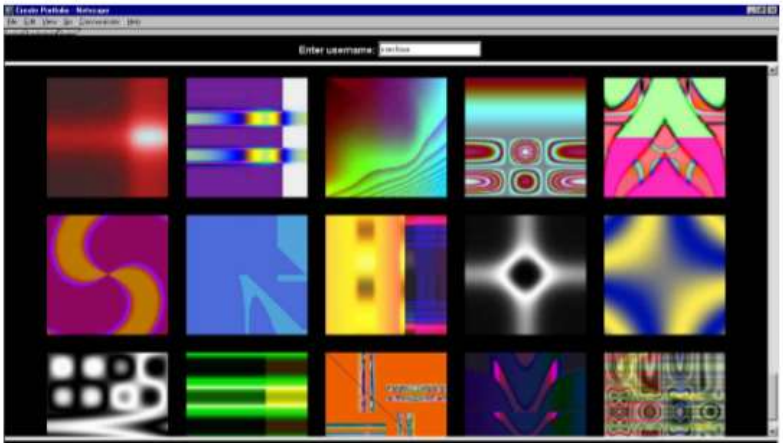
The user will have to choose 5 images from the database.



So, the user will use the username and password chosen when login phase.

3.1.2.2 User Login

User login by recognize his registered username earlier in registration phase. When login, the system will check whether the user is authorized user or not by comparing the username in the database by using mySQL query. After found the record of the username is registered, the system displays a set of random image by calling random image from image database. To continue, user has to recognize their password and answer whether his password is in the set or not. Below displays some of the random art images set generated by the system.



3.1.3 Embedding Process

There are several types of segmentation images, one of this type is segment image based on the bytes. In this paper, segmentation through the LSB algorithm is applied, and it is expected that the groups of bytes in the cover image submit mixture distributions. After obtaining the mixture distribution of bytes group for each original and secret image, the next step is to embed the secret image bytes into the original image bytes. The following steps describe how the proposed model works:

1. It used one of the popular methods of steganography (LSB algorithm) which is the simplest technique to embed the secret image data into the cover image by exchanging the least significant bit in odd bytes of the cover image to hide bits from the secret image.

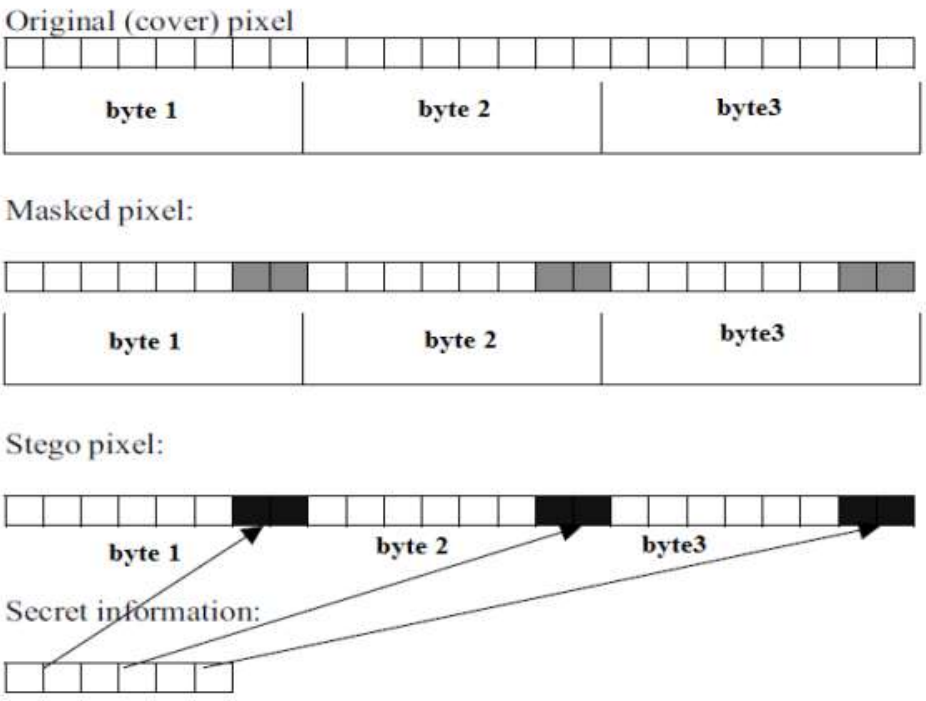


Figure 4: Process of Least Significant Bit

2. LSB algorithm is hidden more than one bit from secret image per one byte from cover image, so the cover size should larger than secret data size. In this paper, the size of cover image should be 16 times in compare with the secret image size, because one bit which is located in the right-most bit is used, and handling the bytes based on the odd and even position.

Original image.

Original Image in Binary Representation

byte1	byte2	byte3	byte4	byte5	byte6	byte7	byte8

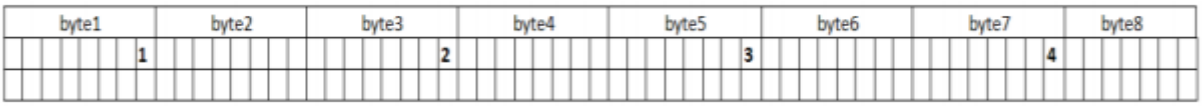
Secret Image

Secret Image in Binary Representation

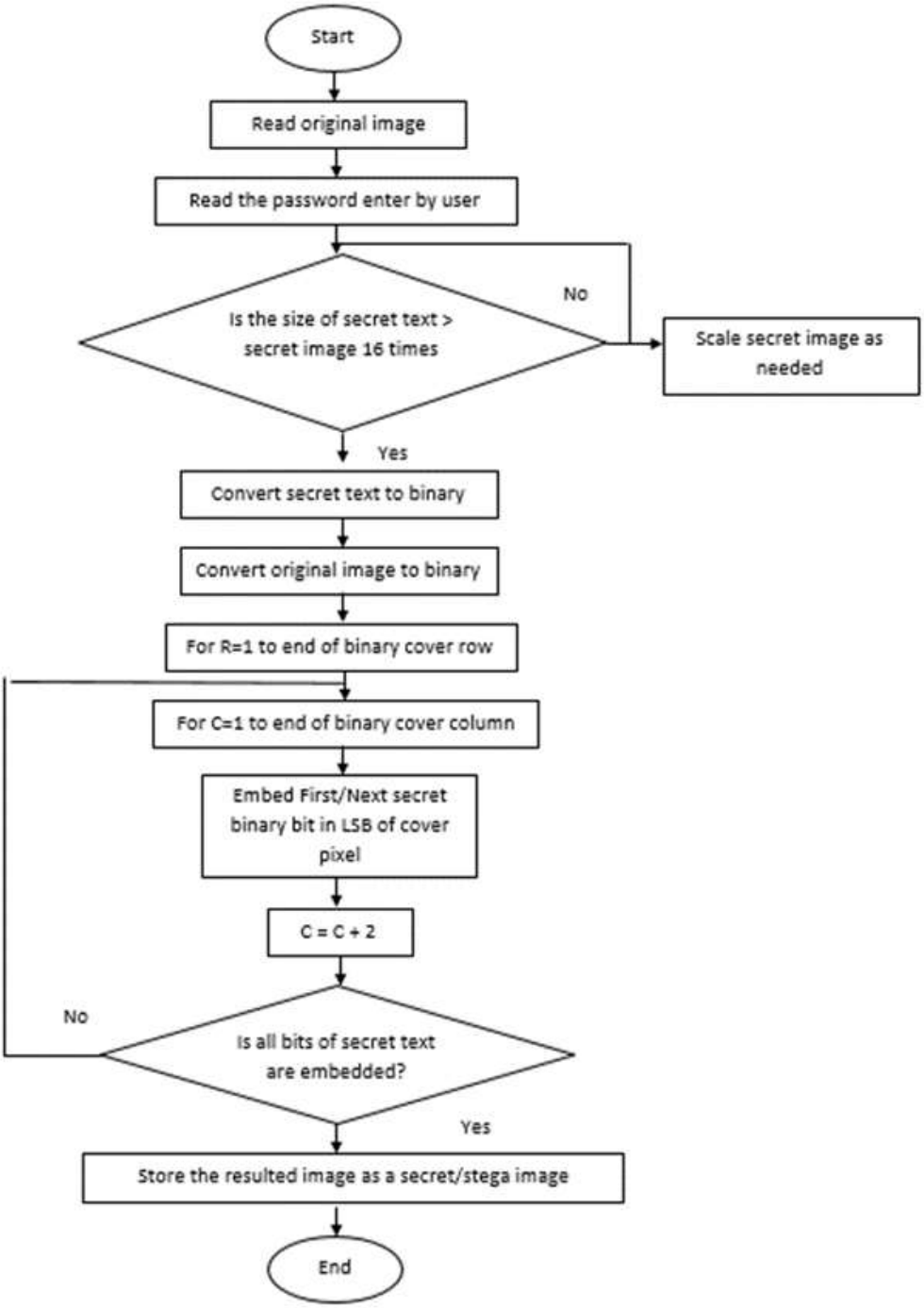
byte1	byte2	byte3	byte4	byte5	byte6	byte7	byte8
1 2 3 4 5 6 7 8							

Stego Image

Stego Image in Binary Representation



This model includes the following two procedures:- Sender procedure: the sender will hide the secret image in cover image through handling the cover image by using Least Significant Bit; the result for this step will produce stego image, then sent it to receiver party see the flowchart below.


Start
Read original image
Read the password enter by user
Is the size of secret text > secret image 16 times
No
Scale secret image as needed
Yes
Convert secret text to binary
Convert original image to binary
For R=1 to end of binary cover row
For C=1 to end of binary cover column
Embed First/Next secret binary bit in LSB of cover pixel
C = C + 2
Is all bits of secret text are embedded?
No
Yes
Store the resulted image as a secret/stega image
End

3.1.4 Authentication

The system will authenticate user whether his answer is correct about the existence of his password in the set displayed. System will set a token to the image set displayed contains user's registered password to verify that user recognize his password is in displayed image set or not. By using concept of Zero-knowledge protocol, this system only accept input of "yes" or "no" which is similar to 0 or 1 in other Zero-knowledge protocol. Every displayed set is considers a round as in Zero-knowledge. Similar to Zero-knowledge protocol, login is carry on with a few rounds to ensure the security of the user authentication system. If user's answers is correct in all round, then he will be authenticated. If his answer is incorrect in any round, he will not be authenticated.

In order to lie, the attacker must guess the value of i in advance, and give H =a(Gi) for some a. Since he has no way of doing it, then the authentication system will wrong with probability of ½ in each round. Since the choices are independent, the probability of getting the correct answers in all the rounds is 2^{-n}. For instance, let the round of authentication be 5 and each set of images contains 3 images.

Round of authentication, n =5,

Probability to guess correct in all round $= 2^{-5*3}$

$=2^{-15}$

=0.0000305(3 significant figure)

$=3.05 * 10^{-5}$

3.2 Summary

This chapter was detailed about the framework and diagrams which were use case and sequence diagram. The next chapter will discuss about the implementation and the result of the project. The algorithm designed in the design phase divided the operation of the system into 3 categories: registration, login and authentication.

3.3 References:

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,”ACMComput. Surveys, vol. 44, no. 4, 2012.

[2] H. Gao, X. Liu, S.Wang, and R. Dai, “A new graphical password scheme against spyware by using CAPTCHA,” in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.

[3] Indian Journal of Science and Technology, Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/86878, October 2016 by Ahmad M. Odat1 and Mohammed A. Otair2.

[4] Behrouz A. Forouzan, Cryptography and Network Security, 2008.

[5] A.H. Lashkari, F.T., Graphical User Authentication(GUA).2010: Lambert Academic Publisher.

[6] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi; “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”; IEEE Explore, 2008.

[7] Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy;” Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice”, Symposium On Usable Privacy and Security (SOUPS),Pittsburgh, PA, USA, 2005.

[8] Arash Habibi Lashkari, GPIP: A new Graphical Password Based on Image Portions.2014.

[9] Louis C. Guillou, Jean-Jacque Quisquater, C.G.Guethen(Ed): Advances in Cryptology – EUROCRYPT’ 88,LNCS 330.pp. 123-128,1988.