IJCSN International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015
ISSN (Online): 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Graphical Password Scheme Using Discretized Centralization

[1] Zarqa Rehmani, [2] Siddhi Keluskar, [3] Karishma Shaikh, [4] Vaishali Baviskar

[1,2,3,4] G. H. Raisoni Institute Of Engineering And Technology

Abstract - Conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. This paper presents an integrated evaluation of the Persuasive Cued Click-Points graphical password scheme, including usability and security evaluations, and implementation considerations. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points.

Keywords - *Graphical passwords, Security, Discretized centralization, Dead zone (of image), Serialization d/b, Shoulder surfing, Encryption/Decryption.*

1. Introduction

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users towards stronger passwords. In our system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password.

There has been a great deal of hype for graphical passwords since two decade due to the fact that primitives methods suffered from an innumerable number of attacks which could be imposed easily. Here we will progress down the taxonomy of authentication methods. To start with we focus on the most common computer authentication method that makes use of text passwords. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks.

Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The idea of graphical passwords first described by Greg Blonder (1996). For Blonder, graphical passwords have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

2. Related Works

In 2002, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. However, both the Movable Frame scheme and the Intersection scheme have high failure rate. In the Triangle scheme, the user has to choose and memorize several pass-icons as his password. To login the system, the user has to correctly pass the predetermined number of challenges. In each challenge, the user has to find three pass-icons among a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons. In 2006, Wiedenbeck proposed the Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme with superior security and usability. To login the system, the user has to correctly respond several challenges. In each challenge, the user has to find any three pass-icons displayed on the login screen, and then

click inside the invisible convex hull formed by all the displayed pass-icons. However, the login time of Convex-Hull Click scheme may be too long. In 2009, Gao proposed a shoulder surfing resistant graphical password scheme, ColorLogin, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of ColorLogin is too high and the password space is too small. In 2009, Yamamoto proposed a shoulder surfing resistant graphical password scheme, TI-IBA, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for the user to find his pass-icons. Unfortunately, TI-IBA's resistance to accidental login is not strong. And, it may be difficult for some users to find his pass-icons temporally displayed on the login screen. Graphical passwords were first described by Blonder. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based scheme.

3. Existing Systems

3.1 Recall Based Techniques

Types of click based graphical password techniques:
1. Pass Points (PP)
2. Cued Click Points (CCP)
3. Persuasive Cued Click- Points (PCCP)

3.3.1 Pass Point (PP)

Based on Blonder's original idea, Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown in Figure. To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.

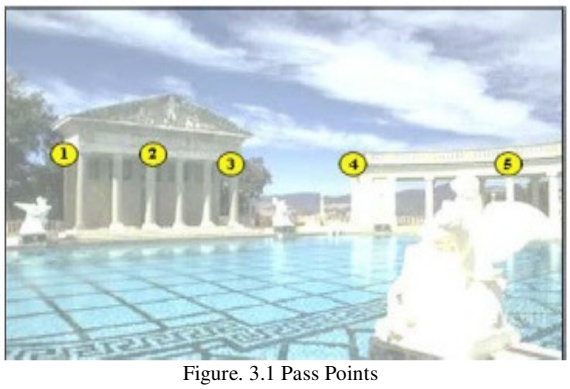

Figure. 3.1 Pass Points

3.3.2 Cued Click Points (CCP)

CCP was developed as an alternative click based graphical password scheme where users select one point per image for five images Figure: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

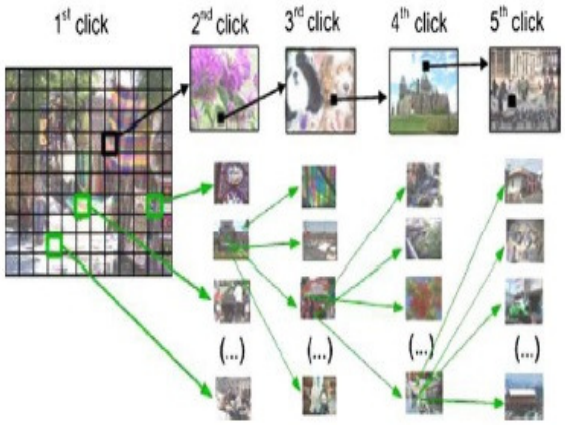

Figure 3.2 Cued Click Points

3.3.3 Persuasive Cued Click- Points (PCCP)

To address the issue of hotspots, PCCP was proposed. As with CCP, a password consists of five clickpoints, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious.

Figure 3.3 PCCP

4. Discussion

Some of the possible techniques for breaking graphical passwords are described and compared with text based passwords.

• Dictionary attacks
Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based
graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

• Guessing
Unfortunately, it seems that graphical passwords are often predictable,serious problem typically associated with text-based passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

• Shoulder Surfing
Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition based techniques are designed to resist shoulder-surfing.

• Spy ware
Except for a few exceptions, key logging or key listening spy ware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spy ware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

• Social engineering
Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phasing web site to obtain Graphical passwords would be more time consuming.

5. System Architecture

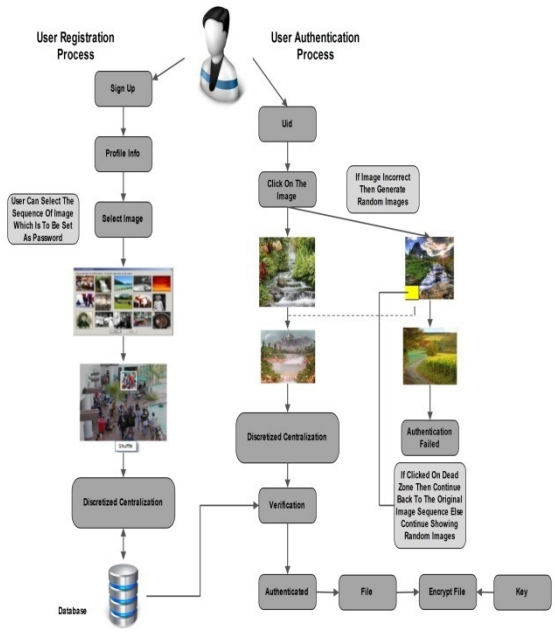

Figure 5. Architecture

6. Algorithm

6.1 Image Processing Algorithm

- Pixels are stored as Integers.
- The integers can be 8-bit, 24-bit or 32-bit depending on the image type.
- Most popular are 24 bit color images where 8 bits each for Red, Green And Blue color values are used to represent a 24-bit pixel value.
- 8 bit images are grayscale images where as 32 bit images have an additional transparency channel.

6.1.1 RGB Separation

RGB Color Example
Sample PIXEL value in HEX = 0EDEB5
In programming the hex numbers are represented as 0x0EDEB5. 0x prefix is for hex notation.

Then individual color channels:
0E (red) - DE (green)- B5 (blue)
00001110 – 11011110 – 10110101

Actual Color Composed Will Be :
Traverse Through Entire Image
for(y=0;y<height;y++) {
for(x=0;x<width;x++) {
pix = input[y][x];

Extract 8-bit R, G and B values from
24-bit Color Value

b = pix & 0xff;
g = (pix >> 8) & 0xff;
r = (pix >> 16) & 0xff;

E.g. Assume PIXEL value is 0x435A56 where 0x43 is red, 0x5A is green and 0x56 is blue component. Now to separate blue we can use the LOGICAL AND operator to mask or filter the blue component from the rest. Since AND'ing with 1 makes no difference where as AND'ing with 0 will force the bit to 0.

435A56
AND 0000FF

0x000056 - blue separated

For Green we shall first right shift the pixel value by 8 bits so that green component is now at LSB position. And then repeat the masking process.
435A56 >> 8 = 435A

0x435A
AND 0x00FF

0x005A - green separated

Similarly we shall right shift by 16 bits so that red component will be at the LSB position and then do the masking.

6.1.2 RGB to Grayscale Conversion

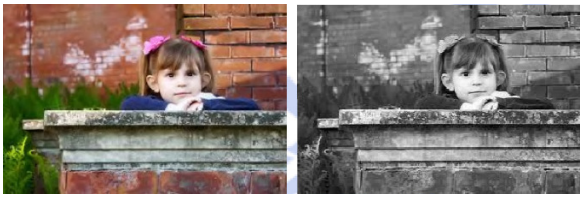

Figure 6.1COLOR-GRAYSCALE-BLACK&WHITE

Steps / Algorithm

- Traverse through entire input image array.
- Read individual pixel color value (24-bit).
- Split the color value into individual R, G and B 8- bit values.
- Calculate the grayscale component (8-bit) for given R, G and B pixels using a conversion formula.
- Compose a 24-bit pixel value from 8-bit grayscale value.
- Store the new value at same location in output image.

Traverse Through Entire Image
for(y=0;y<height;y++) {

for(x=0;x<width;x++) {
pix = input[y][x];

Read individual pixel color value (24-bit).
Split the color value into individual R, G and B 8-bit values,

B=RGBColor & 0xff
G=(RGBColor>>8) & 0xff
R=(RGBColor>>16) & 0xff

Calculate the grayscale component (8-bit) for given R, G and B pixels using a conversion formula,
GS= (R+G+B)/3;
Compose a 24-bit pixel value from 8-bit grayscale value,
R = G = B = GS;
output[y][x]=(R<<16)|(G<<8)|B; } }
Store the new value at same location in output image.

6.3.3 Discretized Centralization

Discretization is used in click-based graphical passwords so that approximately correct entries can be accepted by the system. Method that eliminates false accepts and false rejects. It also allows for smaller tolerance regions without impacting the usability of the system.

FALSE ACCEPT AND FALSE REJECT

With Centered Discretization, the rate of false accepts and false rejects is zero by definition since centered tolerance implies that the system will only accept clickpoints that are within r from the original point. With Robust Discretization, false positives occur when a clickpoint is accepted by the system but falls outside of the centered-tolerance grid square of the original point. Conversely, false negatives occur when a click-point falls within the centered-tolerance grid square of the original point but is rejected by the system.

6.3.4 SHA1 (Secure Hash Algorithm)

The SHA1 encryption algorithm specifies a Secure Hash Algorithm (SHA1), which can be used to generate a condensed representation of a message called a message digest. The SHA1 is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required. Both the transmitter and intended receiver of a message in computing and verifying a digital signature uses the SHA1. SHA1 is used for computing a condensed representation of a message or a data file. When a message of any length < 2 64 bits is input, the SHA1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature The SHA1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

6.3.5 RSA (Rivest Shamir & Adleman)

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption.

RSA Key Generation Steps:

1. choose 2 primes call them p, q
2. multiply them call product n
3. multiply their predecessors
(p-1,q-1) call product Φ
4. pick some integer call it e
   – between 1 and Φ (exclusive)
   – sharing no prime factor with Φ
5. find the integer (there's only one) that call it d
   – times e divided by Φ leaves 1

then your keys are:
– public: e together with n (e is for "encryption")
– private: d together with n (d is for "decryption")

7. Mathematical Model

7.1 Problem Description

Let S be the system such that,

S= {U,P,P',I,Uid,R}

where,

U={U1,U2,U3,…..,Un}

U is the number of users that will be participating in registration process.

P={P1,P2,P3,…,Pn}

P is the set of passwords that the user is going to set.

P'={P1',P2',P3',…,Pn'}

P' is the set of hash value for every password (hash value could be a combination of (x,y) co-ordinates)

I={I1,I2,I3,….,In}

I is the set of images which is to be set as password.

Uid=Set of user ids created in registration phase

R= Set of random images to be displayed after a wrong login attempt.

7.2 Activities

Activity 1:

"n" number of users sign up on one system for registration process.

Let f(s) be a function of system.

Thus, f(s)->{U1,U2,..,Un} Є U

Activity 2:

A user selects a sequence of image which is to be set as password.

If f(i) is function for images then,

f(i)->U

Activity 3:

Every Pn password has a hash value Pn' corresponding for every (x,y) co-ordinates.

Activity 4:

Authentication-For every user id (Uid) an image is generated.

Let f(uid) be afunction for user ids.

Then, f(uid)<- I

Activity 5:

For 1 bad click point random images are generated.

Thus, f(u)->{R1,R2,…,Rn} Є R

7.3 VENN Diagrams

Activity 1- "n" users sign up on a system

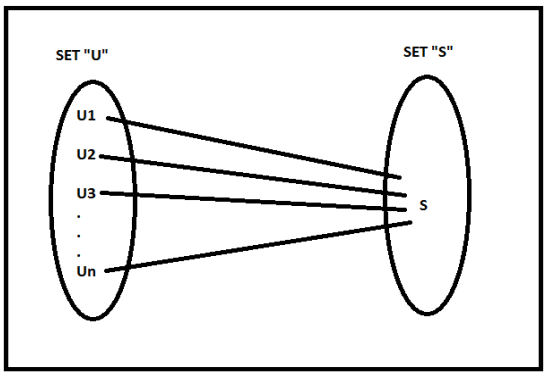

Figure 7

Activity 2- User selects sequence of images

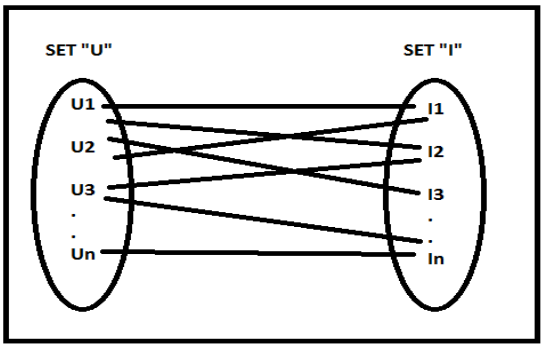

Figure 8

Activity 3- Every Pn password has a hash value Pn'

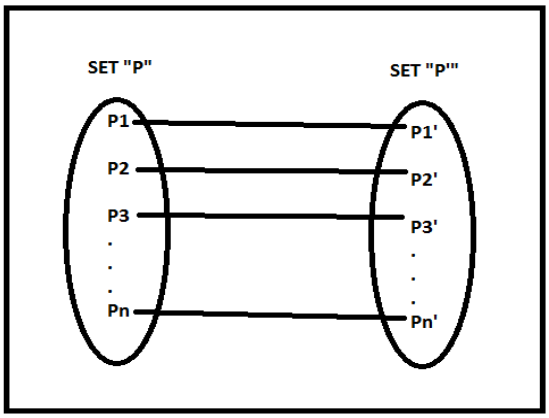

Figure 9

Activity 4- For every user id an image is generated

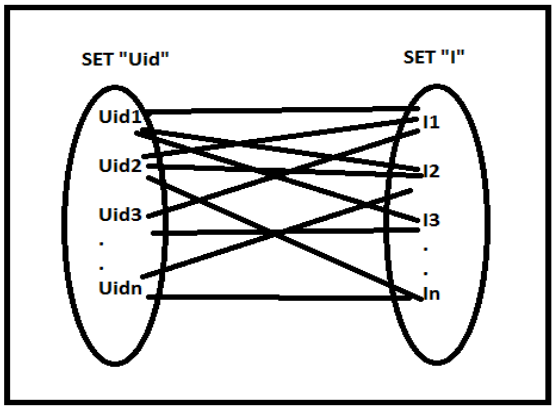

Figure 10

Activity 5- For 1 bad click random images are displayed

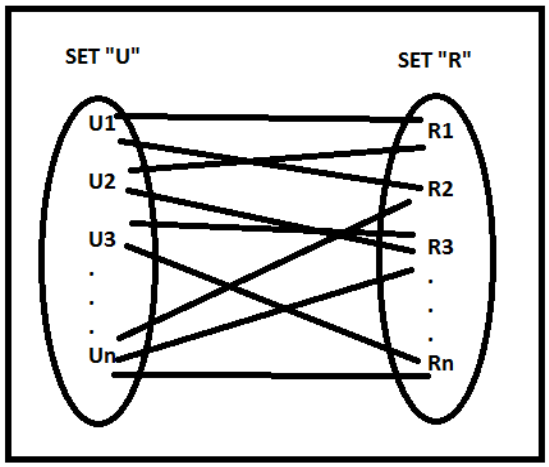

Figure 11

8. UML Diagrams

8.1 Use Cse Diagram

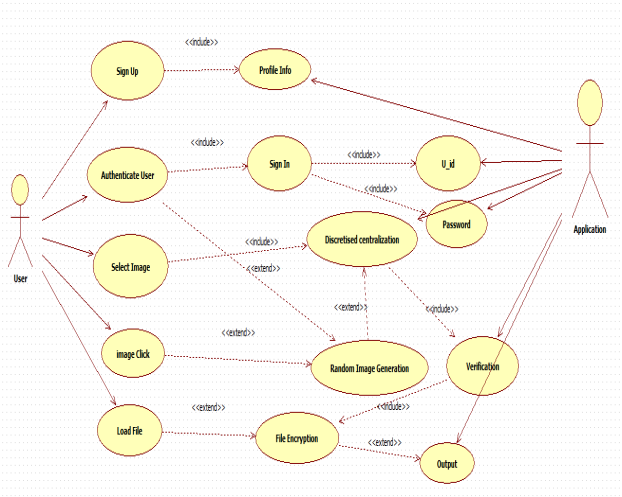

Figure 12 CSE Diagram

8.2 Class Diagram

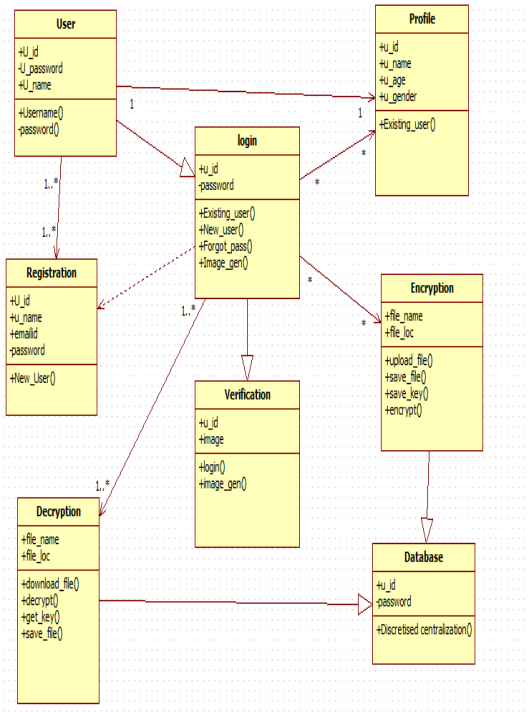

Figure 13 Class Diagram

8.3 Sequence Diagram

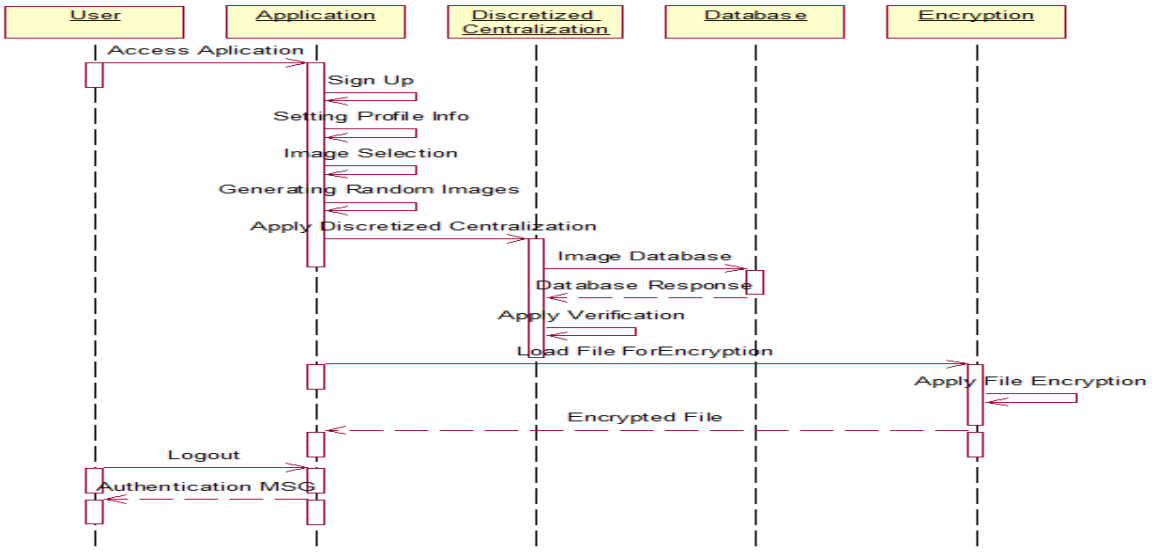

Figure 14 Sequence Diagram

8.4 Collaboration Diagram

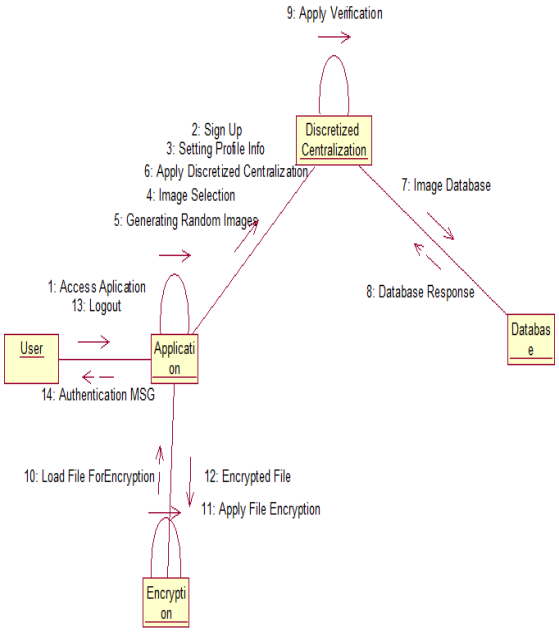

Figure 15 Collaboration diagram

8.5 Component Diagram

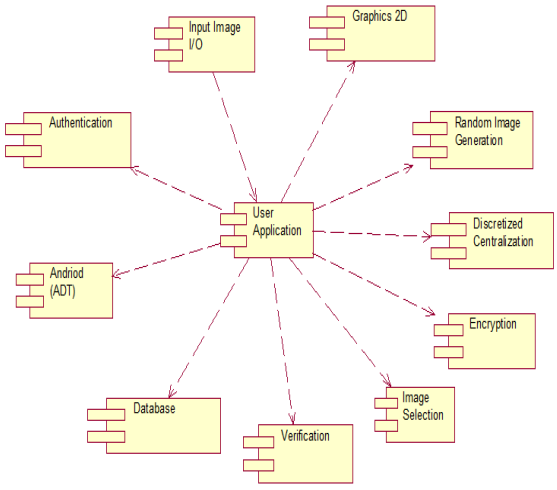

Figure 16 Component Diagram

9. Conclusion

A simple text-based shoulder surfing resistant graphical password, in which the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks has been proposed. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. Finally, the resistances of the proposed scheme to shoulder surfing and accidental login are analyzed and evidence of the usability and security by analyzing data collected from a large user study of Pass Points are provided.

References

[1] Defences Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points, International Journal of Communications and Engineering, March 2012.

[2] Persuasive Cued Click-Points :Design, implementation, and evaluation of a knowledge based authentication mechanism, IEEE 2012 paper.

[3] M. K. Rao and S. Yalamanchili. “Novel shoulder-surfing resistant authentication schemes using text-graphical passwords,” International Journal of Information & Network Security,Aug. 2012.

[4] Z. Imran and R. Nizami, “Advance secure login,” International Journal of Scientific and Research Publications,Dec. 2011.

[5] "A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", Huanyu Zhao and Xiaolin Li Scalable Software Systems Laboratory Department of Computer Science Oklahoma State University.