AUTHENTICATION BY CUED RECALL ON IMAGE RECOGNITION

Kanthima Kongsathitsuwan

A Dissertation Submitted in Partial
Fulfillment of the Requirements for the Degree of
Doctor of Philosophy
(Computer Science and Information Systems)
School of Applied Statistics
National Institute of Development Administration
2015

AUTHENTICATION BY CUED RECALL ON IMAGE RECOGNITION

Kanthima Kongsathitsuwan

School of Applied Statistics

Associate Professor.....Major Advisor

(Vichit Lorchirachoonkul, Ph.D)

The Examining Committee Approved This Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy (Computer Science and Information Systems)

Professor.....Committee Chairperson

(Chidchanok Lursinsap, Ph.D)

Associate Professor.....Committee

(Waraporn Jirachiefpattana, Ph.D)

Assistant Professor.....Committee

(Pramote Kuacharoen, Ph.D)

Associate Professor.....Committee

(Vichit Lorchirachoonkul, Ph.D)

Instructor.....Dean

(Siwiga Dusadenoad, Ph.D)

May 2016

ABSTRACT

Title Dissertation	Authentication by Cued Recall on Image Recognition
Author	Miss Kanthima Kongsathitsuwan
Degree	Doctor of Philosophy (Computer Science and Information Systems)
Year	2015

Graphical passwords have been studied by a variety of methods. According to the psychological beliefs, human can remember an image better than text. Therefore, clicking on a graphical password is easier than typing a text password. Moreover, graphical password can avoid the limitation of text password. This research introduces a method for improving the security of authentication by using a blurred image with a cue as a graphical password that is an integration of recognition-based graphical password and cued-recall based graphical passwords together. The objective of this research was to compare the recall and guessing rates of the proposed scheme with the recall rate and the guessing rate of the Use Your Illusion (UYI) scheme. The proposed method randomly selects a new set of images every time from the user register database when a registered user logs ins. The aim was to reduce the chance of an attacker guessing the correct graphical password. Furthermore, this research utilized the Diffie-Hellman algorithm to compute the position of the secret image. The secret image was used to merge with the selected graphical password. The research also utilized a hash algorithm to create a graphic digest for resisting the message masquerade and reducing the transmission time. This proposed scheme utilized SSL/TLS to maintain security.

Based on the simulation study, the findings indicated that the recall rate of the proposed scheme was better than the recall rate of the UYI scheme and the system login time was lower with the proposed graphical passwords with UYI graphical passwords. However, the guessing rates of these schemes were very similar.

ACKNOWLEDGEMENTS

I would like to express my sincere thanks to my major advisor, Associate Professor Dr. Vichit Lorchirachoonkul, for his valuable advice, encouragement and guidance in making this dissertation a successful. I would also like to extend thanks and appreciation to all of the committee members, Professor Dr. Chidchanok Lursinsap, Associate Professor Dr.Waraporn Jirachiefpattana, and Associate Professor Dr. Pramote Kuacharoen, for their thoughtful comments and suggestions. I am indebted to all of the lecturers and staffs at the School of Applied Statistics, National Institute of Development Administration.

Gratitude is also dedicated to Dr. Chulakasem Chinnapha, the Rector of the Saint John's University for granting me a scholarship to study at the Nation Institute of Development Administration (NIDA), Dr. Suvichakorn Chinnapha who supported my scholarship, Ms. Chittri Kitpeanchareon who is a language editor, and Dr. Tana Kraikruan who is the green Cyber Advance Manager for valuable advices and the program tools for this research.

Special thanks are due to my beloved mother for her support taking care of my daughter and my family during my studying period.

Kanthima Kongsathitsuwan

May 2016

TABLE OF CONTENT

LIST OF TABLES

Tables **Page**

LIST OF FIGURES

Figures **Page**

ABBREVIATIONS

Abbreviations	Equivalence
BDAS	Background Draw-A-Secret
BPP	The Best Pre-secret Image's Position
c	Client's Secret Number
CCP	Cued Click Point
CHC	Convex Hull Click
DAS	Draw-A-Secret
g	Total Prime Number of the Graphical Password for Each User
GPI	Graphical Password With Icon
GPIS	Graphical Password With Icon Suggested by the System
MD5	Message Digest Algorithm 5
P	Prime Number
PCCP	Persuasive Cued Click-Point
PIN	Personal Identifier Number
PSP	Pre-secret Image's Position
s	Server's Secret Number
SSL/TLS	Secure Socket Layer/Transport Layer Security
t_1	the First Simulation Study
t_2	the Second Simulation Study
UYI	Use Your Illusion
YAGP	Yet Another Graphical Password
2D	Two Dimensions

CHAPTER 1

INTRODUCTION

1.1 Background

Security and privacy are vital requirements for information systems. Every information system needs an authentication process or method for identifying, to determine whether or not a particular user has permission to login into the information system. Basically, the identification method involves the use of a password. Passwords are currently divided into two types, namely, text passwords and graphical passwords.

Text passwords are widely used due to convenience and no requirement for special equipment. Nevertheless, text passwords are also easily breached because what is easy to remember is also easy to guess. Therefore, if users use a simple password such as 1234, the date of their important day or personal information an attacker will find it easier to compromise their password. Moreover, most users become even more vulnerable by using a duplicate password for all systems in which they are registered.

Graphical passwords have been studied for more than a decade. Previous research findings have revealed that graphical passwords continue to have the same weaknesses as text passwords. If a graphical password is easy to recall, it is also easy to guess.

1.2 Objectives of the Dissertation

The objective of this research was to improve authentication by using a cued graphical password. The proposed scheme extended the graphical password from Use Your Illusion (UYI) developed by Hayashi, Christin, Dhamja and Perrig (2008). The UYI scheme has been found to distort all images without a cue. However, distorted

image without a cue can make the recall rate lower than a cued graphical image and the user will take longer to login. The proposed scheme used a blurred image with a cue to compare the recall rate, the login time and the guessing rate with the UYI scheme.

1.3 Scopes of the Dissertation

The performances of the proposed scheme with a cued recall on image recognition was evaluated and compared with UYI scheme authentication. Three propositions were developed for performance comparisons at two different times: t_1, within one day after the user portfolio creation and t_2, approximately four weeks since t_1.

Proposition 1: User will be able to recall graphical passwords with cue better than UYI graphical password.

Two indices, the recall rates at time t_1 and t_2, were used to prove Proposition 1. The first index at time t_1, was intended to measure the recognition of the complex graphical password with minimum human ability of memorization. However, since the second index was evaluated after a time period of t_2-t_1 had elapsed, the human ability of memorization played a roles in the second index at the recognition of the password. Intuitively, the value of the second index at time t_2 should be less than the value of the first index.

Proposition 2: The system login time will be less with proposed graphical passwords than with UYI graphical password.

For security reason, one of the desirable properties of a good password is a short system login time. In the present study, the system login times were measured at times t_1 and t_2 in order to observe the impact on the system login time from the elapsed time after creating a graphical password.

Proposition 3: Against the educated guess attacks, the security of the proposed graphical password will be at the same level as the security of UYI graphical passwords.

In this study, an educated attacker is defined as an illegitimate user with some information about the legitimate user. The number of attempts before a successful attack and the login time of a successful attacker were used to compare the securities of the proposed graphical password with the securities of a UYI graphical password.

CHAPTER 2

LITERATURE REVIEW

Authentication is a process for proving that the identity of an object or subject is indeed the identity it claims to be.

Authentication methods can be classified into the following three types (Menkus, 1988):

1) Knowledge-based authentication or "what the user knows" based on private information supplied by the user such as a password, PIN, question and answer, etc.

2) Possession-based authentication or "what the user has" based on private objects the user possesses such as tokens, memory cards, smart cards, mobile phone, etc.

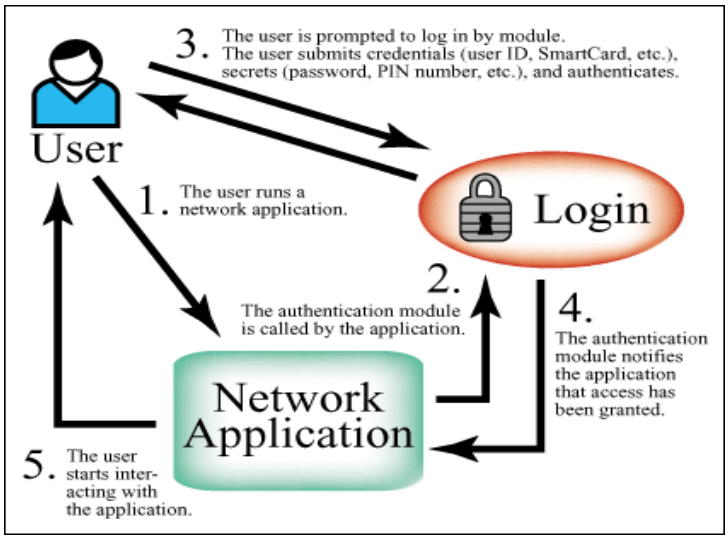

Figure 2.1 The Authentication Process.

Source: Micro Focus, 1999.

3) Biometric-based authentication or “what the user is” based on anatomical, physiological or behavioral characteristics such as fingerprints, iris scans, signature dynamics, etc.

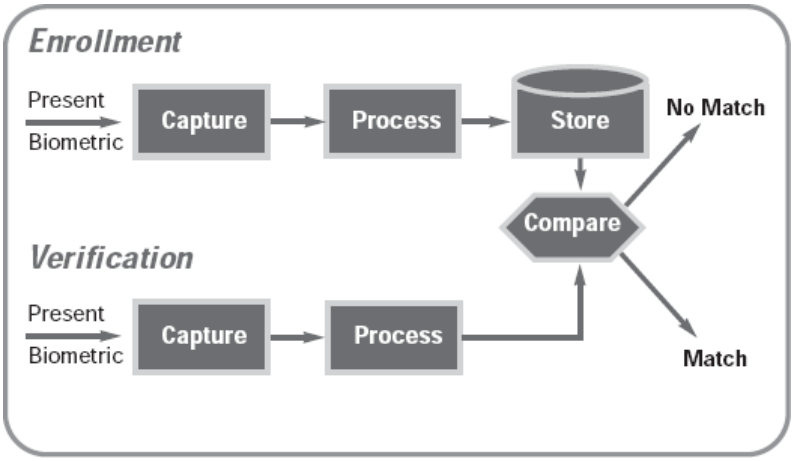

Figure 2.2 Biometric Authentication’s Steps.

Source: University of Birmingham. School of Computer Science, 2004.

Knowledge-based authentication is most widely used in information systems since no additional hardware is required and the implementation is simple. The password is the most widely used form of the knowledge-based authentication (Zviran and Haga, 1990). In practice, only the pair of a user ID and a password is used to authenticate a user in most systems in an organization in order to protect unauthorized users to access the system and block unauthorized access to any computer resources.

Smith (2002) suggests the following rules to improve text password security:

1) Non-dictionary and no-name passwords,
2) Passwords with at least eight characters with upper and lower case letters, numbers and special symbols,
3) Password aging and not reusing,
4) Complex yet easy to remember passwords,
5) Passwords should not be written.

From previous rules for text passwords, significant weaknesses are the difficulty of memorability without taking note and the easy-to-guess password by others. Furthermore, approximately 65.1 percent of users utilize repetitive passwords in various system (Brown, Bracken, Zoccoli and Doughlas, 2004). This leads to insecurity for text passwords.

Graphical password schemes have been studied to improve the weaknesses of text passwords because human ability finds it easier to recognize and recall images than the textual information (Standing, Conezio and Haber, 1970; Madigan, 1983; De Angeli, Coventry, Johnson and Renaud, 2005). Moreover, human being can recognize images in the form of pictograms and photographs better than drawings (Tao and Adam, 2008).

Graphical passwords are the same knowledge-based authentications as text passwords and can be classified into four categories as follows (Ray, 2012).

1) Recall-based graphical password system in which the user has to reproduce something that he creates during the registration phrase.

2) Recognition-based graphical password system in which the user can identify and recognize an image he/she has seen before without any hints.

3) Cued-recall based graphical password system in which the user is given a hint at the time of recall.

4) Hybrid systems which are a mixture of two or more schemes of the above schemes.

2.1 Recall-Based Graphical Password Systems

The recall-based graphical password system or pure recall technique is a drawmetric authentication that requires the user to draw a simple outline of the graphical password during registration and the user must draw the similar drawing to be authenticated (De Angeli et al., 2005). An example of the recall-based graphical password system is the Draw-a- Secret (DAS) (Jermyn, Mayer, Monrose, Reiter and Rubin,1999). In the DAS, after the user draws a secret 2D drawing on a grid, the system encodes the sequence of the coordinate grid in the drawing. The numbers of the coordinate pair and the position of the drawing line are the strong many-to-one

mapping authentication. The system verifies the drawing by checking the directions and the positions of the drawn strokes on the grid in order to authenticate a user.

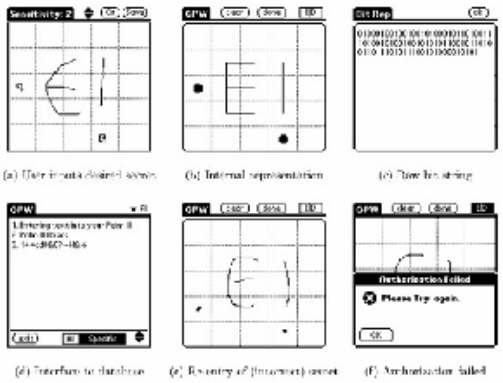

Figure 2.3 An Example of DAS Scheme.
Sources: Jermyn et al., 2013.

Moreover, Thrope and Van Oorshoct (2004) proposed a grid selection technique based on DAS. The grid selection adds an extra degree of complexity to the password by creating a secret within each original DAS scheme as shown in Figure 2.4. Although the grid selection cannot be concluded to be better than the DAS scheme, this technique offers more password space than the DAS scheme.

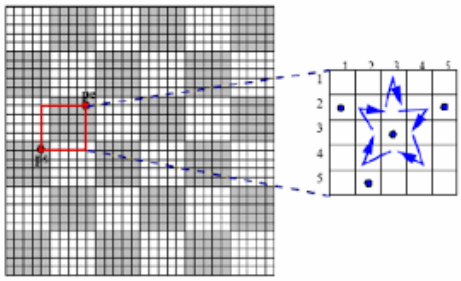

Figure 2.4 An Example of the Grid Selection Technique.
Sources: Thrope and Van Oorshoct, 2005.

Another interesting graphical password is the YAGP (Yet Another Graphical Password) scheme utilizing the Levenshtein distance to measure the similarity of two strings and trend quadrants to measure the drawing pen strokes (Gao, Guo, Chen, Wang and Liu, 2008). Therefore, a finer grid should be used for password comparison when there are no constraint on drawing positions. Improving the DAS, Goldberg, Hagman and Sazawal (2002) proposed a technique called "Passdoodle" which is a graphical password comprised of handwritten designs or text. Again, the user must be trained to construct a correct Passdoodle password.

Figure 2.5 An Example of Passdoodle Password.
Sources: Goldberg et al., 2004.

Weiss and De Luca (2008) develop the PassShapes algorithm to translate the key stroke direction as an alphanumeric character. The user is required to draw a simple geometric shapes constructed of an arbitrary combination of a number of different strokes to be authenticated. The depository of the password in the form of the alphanumeric character is exposed to risk similar to text passwords. Another improvement of the DAS is the Pass-Go algorithm (Tao and Adams, 2008) in which a user selects grid intersections as a means of entering the password instead of drawing through grid cells as in the DAS. The Pass-Go graphical password has theoretical password space that is larger than the DAS due to the requirement of a finer grid.

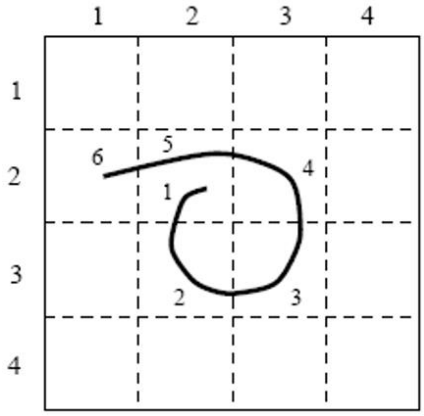

Figure 2.6 An Example of Pass-Go Password.
Sources: Tao and Adams, 2008.

The other drawmetric authentication is GrIDsure (2009). This method challenges users with a grid containing pseudo-randomly generated numbers. Users have to select numbers from a grid-square as their secret pattern. Jhawar, Inglesant, Courtois and Sasse (2011) concluded that the GrIDsure is more secure than the traditional PINs in cases requiring prevention of shoulder sniffing. However, Bond (2008) found the GrIDsure to be unable to resist phishing and cameras at the point-of-sale or ATM.

Figure 2.7 An Example of GrIDsure Authentication.
Sources: Jhawar et al., 2009.

All of the pure recall graphical passwords systems have been developed to help users memorize password more easily. However, the issues of login time, success rate, and strength against attack are generally not considered in details.

2.2 Recognition-Based Graphical Password Systems

Recognition-based graphical password systems require the user to select the correct image out of decoys. Phishing attacks and man-in-the-middle-attacks are more difficult with recognition-based systems (Biddle, Mannan, Oorchot and Whalen, 2011). One of the most extensively studied recognition-based graphical password systems is Passfaces (PASSFACES Corporation, 2009). In the Passfaces technology, a user selects a random set of human faces, typically 3 to 7 faces to serve as a secret authentication code. To authenticate, the user has to identify the face belonging to a pre-selected set among decoys. Several such rounds are repeated with different panels. The successive face identification causes a long login time. The greater the similarity of the decoy faces to the correct faces, the higher chance for a type II error.

Figure 2.8 An Example of Passface Authentication.
Sources: PASSFACES Corporation, 2009.

A more complex scheme is the Story scheme proposed by Davis, Monrose and Ritter (2004). In the Story scheme, a user has to select a sequence of images for his/her portfolio. The user is required to select images among decoys in the correct

order to be authenticated. It should be noted, however, that differences in the Story scheme are clearly observed in choices made by males and females.

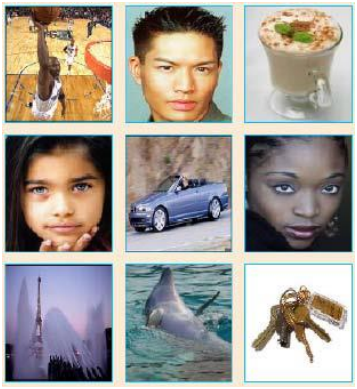

Figure 2.9 An Example of Story Scheme.
Sources: Davis et al., 2004.

Dhamija and Perrig (2000) presented a graphical authentication scheme, Déjà Vu, based on the Hash Visualization technique (Perrig and Song, 1999). In the Déjà Vu scheme, the user is asked to select a certain number of images from a set of abstract pictures randomly generated by the system. The abstract picture is difficult to write down and difficult to explain to others. The user is required to identify pre-selected images in order to be authenticated. In the Déjà Vu scheme, however, the order of identifying the correct images is irrelevant. It is known that many users may select the same set of images if the sample images are attractive. However, the images may be interpreted differently with different image explanations. If someone knows the user's favorite color or tone, images belonging to the legitimate user can easily be guessed.

Wienshall (2006) proposed a cognitive authentication scheme by keeping the path direction of identifying images by starting from the upper left corner. If the image is in the portfolio, the position of the next image will move to the image below.

The results of each round differ. Attacks by shoulder sniffing or spyware are difficult.

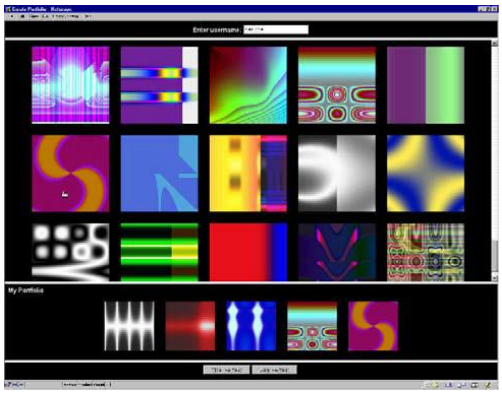

Figure 2.10 An Example of Déjà Vu Scheme.
Sources: Dhamija and Perrig, 2000.

The passface, Story, Déjà Vu, and cognitive authentication schemes are similar in a sense that the images are randomly selected with training of image recognition. Pering, Sundar, Light and Want (2003) suggested a different test of the recognition in which a photographic authentication system allows a user to select the user's image as a graphical password. For the authentication process, the user has to select the correct image from decoys, some of which are from other users' images. The system shows ten image groups and each group contains four images in one panel. This method takes a longer login time and an intimate acquaintance would be able to guess which image is legitimate.

Hayashi et al. (2008) propose the Use Your Illusion (UYI) scheme which allows a user to select personal images as suggested by Pering et al. (2003), but the UYI scheme distorts the selected image to prevent others from guessing.

Figure 2.11 An Example of Use Your Illusion (UYI) Scheme.
Sources: Hayashi et al., 2008.

Wiedenbeck, Waters, Birget, Brodskiy and Memon (2005) and Bicakci, Atalay, Yuceel, Gurbaslar and Erdenniz (2009) proposed several images shown in the form of the small images or icons in one name. In the Graphical Password with Icon (GPI) scheme, a user selects personal icons. In the Graphical Password with Icon suggested by the System (GPIS) scheme, however, the system randomly selects a number of icons for a user. Both GPI and GPIS schemes allow the user to select six icons from 150 decoys in one panel and use small icons as graphical passwords as suggested by Wiedenbeck, Waters, Sobrado and Birget (2006). But the Convex Hull Click (CHC) scheme randomly positions the selected small icons on the screen, and one panel contains at least three of the user's icons. A user has to click his graphical password at any position within the triangle. However, the disadvantage of this method is a lengthy login time. The percentage of memorizing graphical passwords is empirically shown to be in the same order as the percentage of memorizing text passwords.

Figure 2.12 An Example of Convex Hull Click (CHC) Scheme.
Sources: Wiedenbeck et al., 2006.

2.3 Cued-Recall Graphical Password Systems

Cued-recall graphical passwords are graphical passwords with a hint to remind the user to remember the user's own password. The first cued-recall graphical password is Blonder which was designed by Blonder (1996). The Blonder lets a user predetermine positions within a visual image displayed to the user and the user has to point to the correct order of the predetermined position in the process of authentication. However, the relatively small predefined point leads to inadequate security (Wiedenbeck et al., 2005).

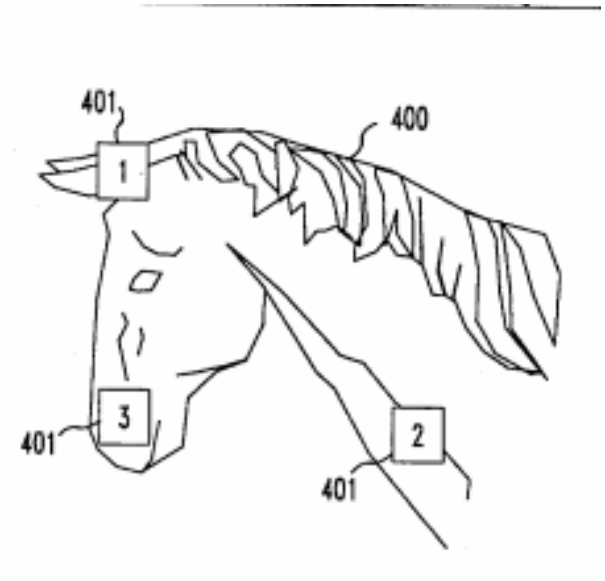

Figure 2.13 Graphical Password Scheme Suggested by Blonder.
Sources: Blonder, 1996.

Wiedenbeck et al. (2005) suggested the Passpoint scheme in which the system randomly selects an image for a user to click five points (pixels) within the image. For authentication, a user has to click the points in the correct sequence. Otherwise, the image is the user's cue for click-point selection. The sensitive issue of the Passpoint scheme is the determination of a small neighborhood of correct click points for acceptable human error. Based on the test conducted by Wiedenbeck et al. (2005), user were found to takes a login time ranging from 9-19 seconds with a login success rate of 55-90%. The login time and the login success rate are in the same order as other methods.

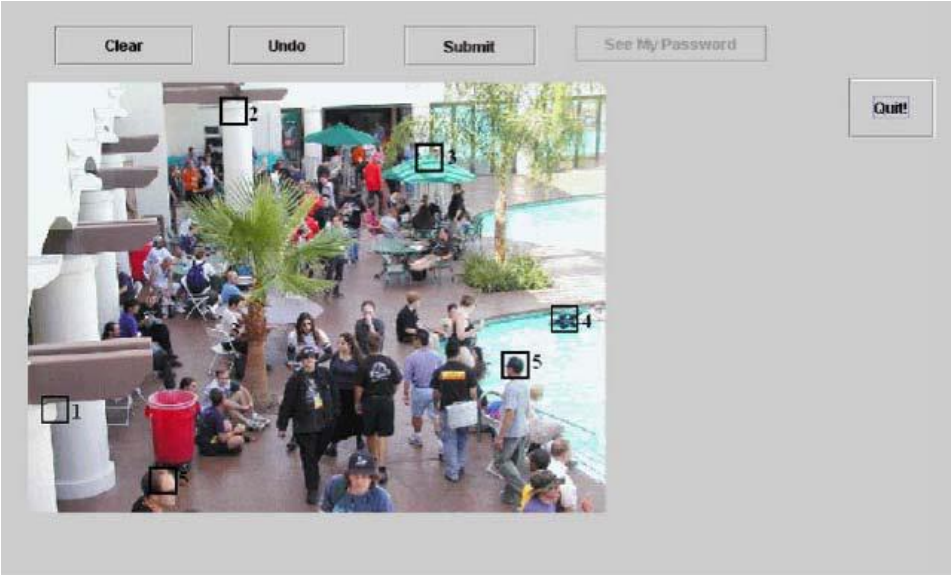

Figure 2.14 An Example of Passpoint Scheme.
Sources: Wiedenbeck et al., 2005.

Chiasson, Biddle and Oorschot (2007; 2008) proposed two variations of the Passpoint scheme Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP) respectively. The CCP scheme uses five images per one login and a user successively selects one click-point within each image as the one-to-one cue or one at time, not the one-to-many cues as in the Passpoint scheme. During the creation step of the PCCP scheme, the PCCP image is dimmed except for the viewport. The user selects the click-point inside a bright viewport. The PCCP concept is to reduce the dispersion of the hotspot guiding the user to click the position near the click-point. In addition, all three schemes, PassPoint, CCP, and PCCP, use a grid-based discretization algorithm in which an attacker can use grid identifiers to attack the positions kept in the server-side storage (Robert, Sonia and Van, 2012).

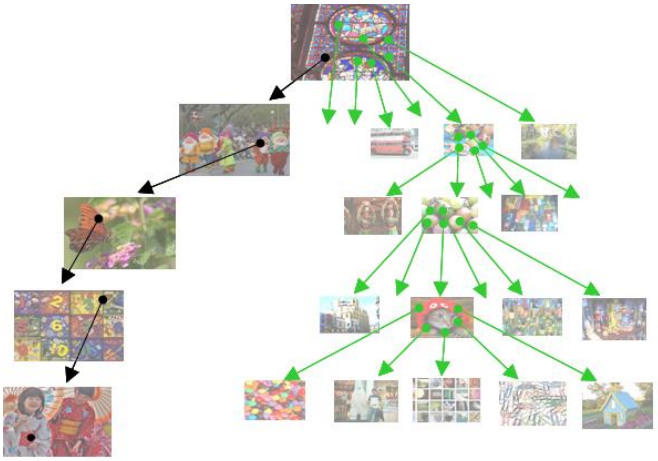

Figure 2.15 A CCP Password Creation.

Sources: Chiasson et al., 2007.

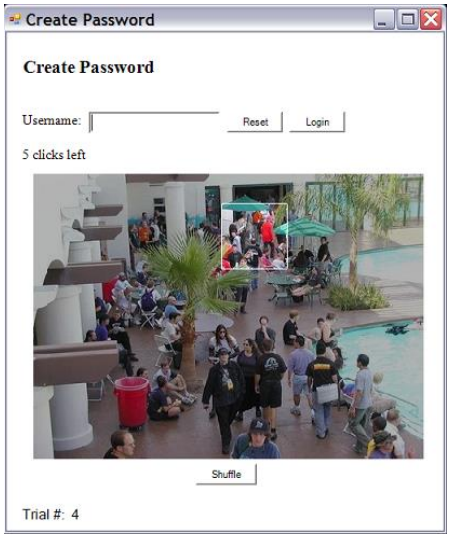

Figure 2.16 Bright Viewport in PCCP Scheme.

Sources: Chiasson et al., 2008.

Dunphy and Yan (2007) developped the Background Draw-a-Secret (BDAS) scheme based on the DAS scheme which adds a background to decrease the amount of symmetry of the image and to enhance memorability. However, the main obstacle to the BDAS is the training required before usage.

Figure 2.17 An Example of BDAS Scheme.
Sources: Dunphy and Yan, 2007.

Moreover, the VisKey (SFR, 2006) released by SFR and V-GO (PASSLOGIX, 2006) provided by Passlogix Inc. are both commercial softwares passwords categorized as cued-recall graphical passwords. The VisKey is specifically designed for mobile devices. The user has to select an image stored in the device as the background for the graphical password. The user also has to select a spot in the same order as the user defined in the register phrase. The weakness of the VisKey is the difficulty of touching the exact points. Tao (2006) suggests allowing a certain tolerance area around the exact point in the VisKey. In the Passlogix V-GO scheme, the user has to create a graphical password by navigating through an image and can click and/or drag on a series of items within that image to authenticate identification. The weaknesses of the Passlogix V-GO are that the user-chosen password may be easily guessable and the password space is small.

Figure 2.18 An Example of VisKey Scheme.
Sources: SFR, 2006.

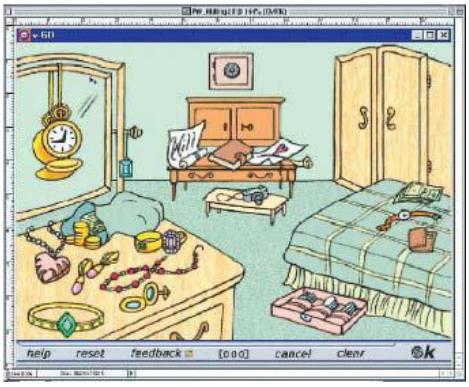

Figure 2.19 An Example of Passlogix V-GO Scheme.
Sources: PASSLOGIX, 2006.

In terms of security, the graphical passwords encoded in the canonical representation of their theoretical password space can be easily attacked by brute-force guessing and dictionary attacks in the same manner as text passwords in the case of small password space (Robert et al., 2012). Examples of small graphical password space are the DAS and Pass-GO schemes which are recall-based graphical passwords. Empirical studies have concluded that the graphical passwords chosen by legitimate users are in a symmetric subspace with respect to the central vertical and horizontal

axes. Graphical passwords in such symmetric subsequences are easily attacked by exponentially decreasing the reading space with populating dictionaries.

For recognition-based graphical passwords, attackers can exploit the knowledge of a user race or gender to guess a possible correct password such as in the Passface scheme. Users tend to select attractive faces of their own race. The automated image-processing tool can successfully attack exploited hotspots in cued-recall graphical passwords (Dirik, Menon and Birget, 2007). Cued-recall graphical password will help users memorize images better than pure recall graphical passwords. For cued-recall graphical passwords, the user has to remember only a specific part of images instead of the wholes images as in the pure recall graphical password.

CHAPTER 3

METHODOLOGY

The objective of this research was to improve authentication by using cued graphical password. The proposed scheme was motivated by the UYI scheme to develop a new scheme with a better recall rate and shorter login time than the original UYI scheme without sacrificing security. The three phrases involved in developing this scheme were registration, authentication and communication security.

Phrase I: Registration

A user creates a personal profile consisting of the user's name, text password, age, education level, and gender. Additionally, the user creates five graphical passwords by selecting images from the user's collection. The general selection guideline for a secure authentication is that the image has absolutely no direct or indirect relation to the user. The image cannot be used to identify the user, any person or any place possibly related to the user. Each selected image is divided into nine panels as shown in Figure 3.1. Next, the user selects one panel from the nine panels in the image that is the cue, and the system adds RGB color to blur the remaining eight panels as shown in Figure 3.2. The system creates a secure database to store the users' profiles including the selected graphical passwords.

Figure 3.1 An Example of the Partition of the Selected Image.

Figure 3.2 An Example of the Cued Graphical Password and the Remaining Blurred Panels in the Selected Image.

Phrase II: Authentication.

The user has to enter the user's name and text password as in the conventional text password system. If the validity of the user name and password is confirmed, the system randomly selects one graphical password from the user's profile and creates eleven decoys by randomly selecting from other selected images in the database of user profiles. The system shows all twelve images within one window as shown in Figure 3.3.

Figure 3.3 An Example of Displaying Twelve Images in One Window.

Phrase III: Communication security.

To maintain security, the selected graphical password is merged with the secret image by utilizing the Diffie-Hellman algorithm. In addition, the transposition process decreases the probability of successfully attacking the message masquerade to $^{1}/_{18!}$ or $1/6.4024*10^{15}$. Moreover, this proposed scheme utilizes the hash function to resist the message masquerade and reduce the transmission time.

The details of the process describe as follow. Each image is assigned to store in an array named P1 to P12 for convenience to identify the position of the secret image as shown in Figure 3.4.

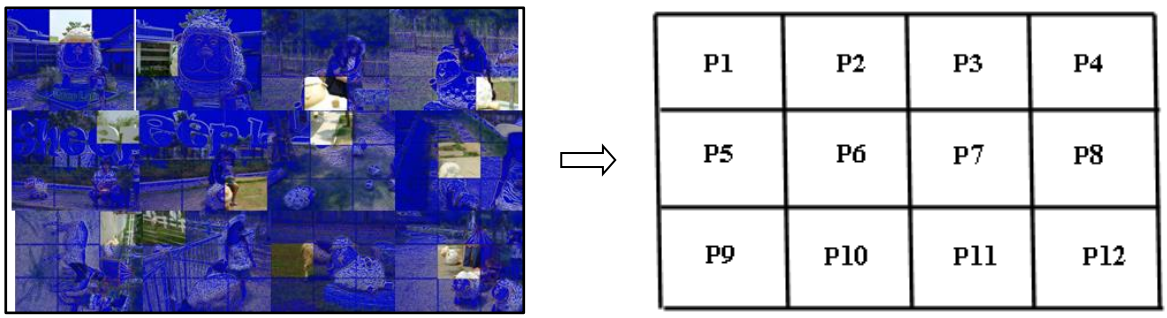

Figure 3.4 An Example of Named the Position of Each Image.

The process of merging the image using the Diffie-Hellman algorithm as is separated into two steps as follows:

1) Finding the position of the secret image

(1) Define “P” as a large prime number. The “P” shall be a random integer. The proposed scheme uses an example of “P” from Behrouz (2008), which is 7646242985634937659550305074763380967269497489235737728609252356666607554236374233096611800333381061947301309504147387009991780436548785807987581.

(2) Define “g” as the total number of graphical passwords for each user.

(3) Both the server and client know “P” and “g”.

(4) The client will random “c” and the server will random “s”. Both ”c” and “s” are the secret numbers that do not exchange between client and server

(5) The client will compute c': $c' = g^c \bmod P$.

(6) The server will compute s': $s' = g^s \bmod P$.

(7) Next, the client and the server will exchange c' and s'

(8) Then the client will compute the pre-secret image position(PSP) by $s'^c \bmod P$ and the server will compute the pre-secret image position(PSP) by $c'^s \bmod P$ or $g^{cs} \bmod P$.

(9) Finally, the secret image position will be PSP mod 13. The fraction is 0,1,2,3,4,5,6,7, 8,9,10,11,12. If the fraction is 0, which is out of the position in array or is to be the same as the position of the selected graphical password, the system will repeat the image selection.

2) Transposition of the selected image with the secret image.

To strengthen security, this proposed scheme will use the advantage of separating an image into nine panels by transposition of each panel in the selected image and the secret image. Similar to the position identification of the secret image, each panel of the selected image and the secret image is assigned storage in an array named A1 to A9 for the selected image and S1 to S9 for the secret image as shown in Figure 3.6. The transposition process uses the PSP from the first step to identify the beginning panel position of the selected image and the secret image. To reduce the probability that the fraction is the same position as the position in the computation, this proposed system uses the congruential method. In cases where the fraction is an

even number, the number 1 will be added to translate it into an odd number. The formulation for computing the beginning panel is $X_{i+1} = KX_i \bmod 2^n$ (K is PSP).

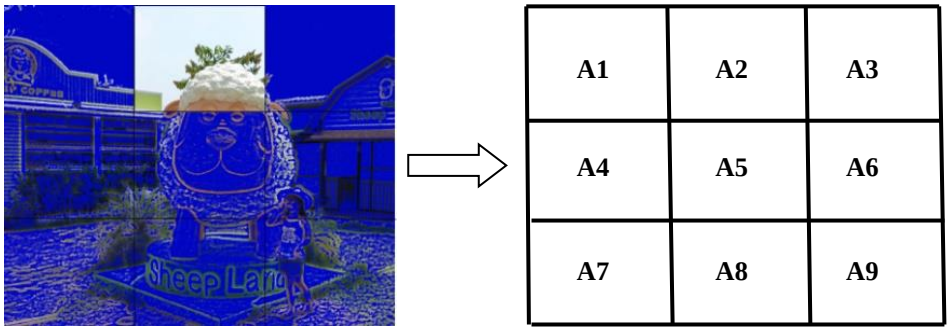

Figure 3.5 The Left-Hand Side Image is the Selected Image and the Right-Hand Side Image is a Demonstration Position of Each Panel.

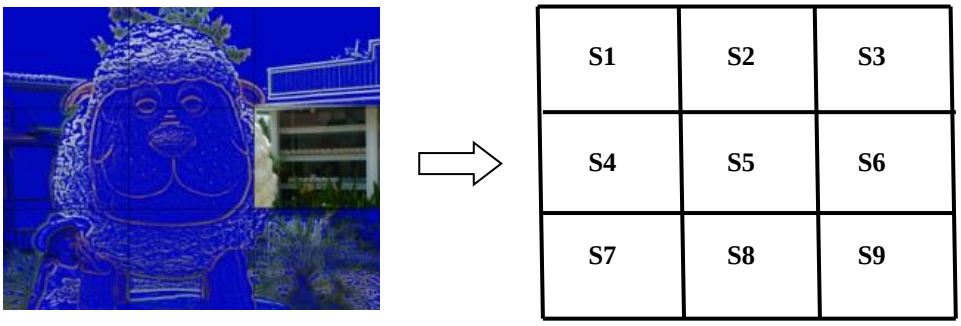

Figure 3.6 The Left-Hand Side Image is the Secret Image and the Right-Hand Side Image is a Demonstration Position of Each Panel.

For example, if the fraction is 6. The output of this process is presented as follow:

A6	**S6**	**A7**	**S7**
A8	**S8**	**A9**	**S9**
A1	**S1**	**A2**	**S2**
A3	**S3**	**A4**	**S4**
A5		**S5**	

Figure 3.7 The Output of Transposition Process.

When the transposition or merging process is finished, the system will hash the merged image by an MD5 algorithm. The hashed graphical password is called "graphic digest". The server will then merge the correct graphical password sent to the client with the secret image and hashes them.

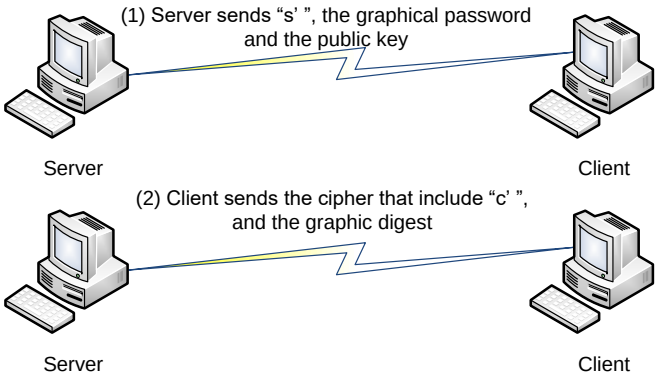

Figure 3.8 The s', c' and Graphic Digest's Transmission.

Finally, the server will compare the received graphic digest with the graphic digest in the server. If they coincide, the authentication is successfully.

CHAPTER 4

RESULTS OF SIMULATION STUDY

Twenty-five pairs of known participants in the experiment were randomly selected from a group of undergraduate students in information technology who had been studying together for at least three years at a well-known university in Bangkok. Each pair communicated with each other at least through Facebook, Instagram or Line social media account. The participants consisted of 16 males and 34 females with basic knowledge of information technology at similar levels. The participants were aged between 20-22 years. The pairs of participants were randomly separated into two groups. No members in one group belonged to the same pair.

The experiment consisted of two sub-simulation studies. The first one was designed to measure the ability of recalling personal graphical passwords and the second was designed to measure the security of graphical password against educated attackers.

4.1 Simulation Study's Procedure

The first sub-simulation study was conducted at two different times. The first time was conducted on the same day users created portfolios and the second time was conducted at approximately 4 weeks after the creation of the user's portfolio.

The first sub-simulation study can be described as follows:

1) The participant in each group logged into the system with their respective user names and text passwords to create five graphical passwords as described in Chapter 3.

2) The system randomly selected one of the user's five graphical passwords without replacement and eleven decoys from the database of users' graphical passwords. The selected graphical password and eleven decoys were shown in one window.

3) If the participants selected one of the twelve displayed graphical password within a specific period of time, the system would verify the validity of the selected graphical password. Otherwise, the system would return to step 2.

4) If the selected graphical password was valid, the system would record the time taken for one successful login which was also the time taken in one attempt at graphical password selection. The number of attempts was then recorded.

5) The participants were allowed a maximum of three attempts at logging into the system. Otherwise, the system would record the login as unsuccessful.

The second sub-simulation study was conducted only once at any time after the evaluation of the graphical password. In the second sub-simulation study, the participants in one group became the educated attacker of the participant in the same pair in the other group. The educated attackers were allowed a maximum of three attempts to log into the system in the same environment as in the first sub-simulation study. If the graphical passwords selected by the educated attacker were accepted by the system as valid graphical password within three attempts and within the specific time for one selection, the system would record the login as a successful attack including the total login time and the number of attempts. Otherwise, the system would record the login as an unsuccessful attack.

In comparison, the same two groups of participants are asked to perform the second sub-simulation study twice, one with the proposed scheme and another time with the UYI scheme.

The tools used in testing the proposed graphical password with cue are available at www.thecuegp.com and the tool for testing the UYI graphical password used the software available at http://arima.okoze.net/illusion/demo/index2.html which is the web demo for using Use Your Illusion research (UYI) by Hayashi et al. (2008).

4.2 Numerical Results

4.2.1 Recall Rate

The data collected from the first sub-simulation study by using the proposed scheme and the UYI scheme were analyzed and used to prove the three propositions developed in the scope of this dissertation. The simulation studies were conducted at t_1, within one day after creating the user's portfolio and t_2, approximately 4 weeks after t_1, in order to test human memorability.

In the first sub-simulation study using the proposed scheme, successful login at the first attempt was 96% for the experiment conducted at time t_1 and dropped slightly to 92% at time t_2. The remaining 4% and 8% were the successful logins on the second attempt at times t_1 and t_2 respectively.

The sub-simulation study was repeated under the same conditions but used the UYI scheme. Successful logins at the first attempt were only 36% at time t_1, and 0% at time t_2. Successful logins at the second and third attempts at t_1 were both equal to 32% and the second and third attempts at t_2 were 40% and 52% respectively. Unsuccessful logins using the UYI scheme at t_2 were 8%. It can be empirically concluded, therefore, that a user can recall graphical passwords with cue better than UYI graphical password as stated in Proposition 1.

The recall rates from the simulation study using the proposed scheme are summarized in Table 4.1.

Table 4.1 Comparisons of the Recall Rates at t_1 and t_2 From the Simulation Study Using the Proposed Graphical Password With Cue and the UYI Scheme

Successful login at	Recall rate at			
	Proposed graphical password with cue		UYI scheme	
	t_1	t_2	t_1	t_2
1st attempt	96.0	92.0	36.0	-
2nd attempt	4.0	8.0	32.0	40.0
3rd attempt	-	-	32.0	52.0
Unsuccessful Login	-	-	-	8.0

4.2.2 Login Time

The simulation study using the proposed graphical password with cue sets the login session time-out equal to one minute. If the participants were unable to log in successfully within the time limit, the time taken at the attempt was equal to the time-out; otherwise, the login time is equal to the time taken in each attempt. The login time was defined as the total time taken from the first login to a successful login. In the simulation study using the proposed graphical password with cue, all login attempts at t_1 and t_2 took less time than the specified time-out. The average login time were 8.0 seconds with a standard deviation of 3.5 seconds at t_1 and 8.1 seconds with a standard deviation of 7.1 seconds at t_2 when the login was successful at the first attempt and increased to 32.0 seconds with a standard deviation of 0.0 seconds at t_1 and 38.0 seconds with a standard deviation of 0.0 seconds at t_2 when the login was successful at the second attempt. The frequency distributions of the login times at t_1 and t_2 are shown in Figures 4.1 and 4.2 respectively.

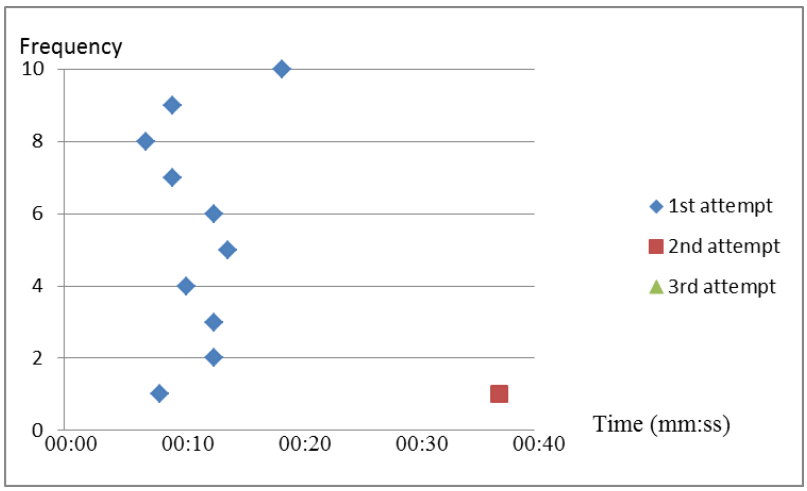

Figure 4.1 Frequency Distribution of Login Time at t_1 Using the Proposed Graphical Password With Cue.

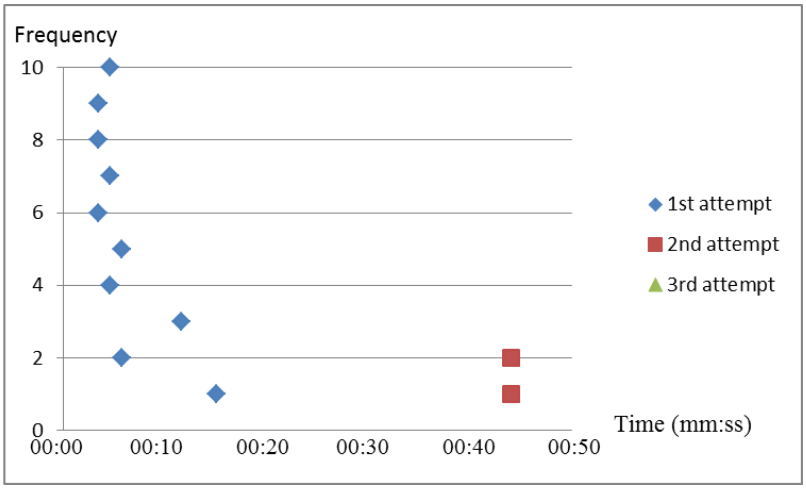

Figure 4.2 Frequency Distribution of Login Times at t_2 Using the Proposed Graphical Password With Cue.

The average login times were much longer in the first sub-simulation study using the UYI scheme than in the proposed graphical password with cue. At t_1, the average login time using the UYI scheme was 38.9 seconds with a standard deviation of 21.5 seconds increasing to 80.1 seconds with a standard deviation of 36.6 seconds and 147.2 seconds with a standard deviation of 76.0 seconds when the login was successful at the first, second and third attempts respectively. At t_2, none of the

participants were successful at the first attempt. The average login time was 158.2 seconds with a standard deviation of 98.1 seconds increasing to 193.4 seconds with a standard deviation of 56.0 seconds when the login was successful at the second and third attempts respectively. The frequency distributions for the login times at t_1 and t_2, are shown in Figure 4.3 and 4.4 respectively.

The results are summarized in Table 4.2. Any login requiring more than three attempts was defined as an unsuccessful login. Empirically, it can be concluded that login to the system using the proposed scheme required less time than logins to the system using the UYI scheme. Thus, proposition 2 is supported.

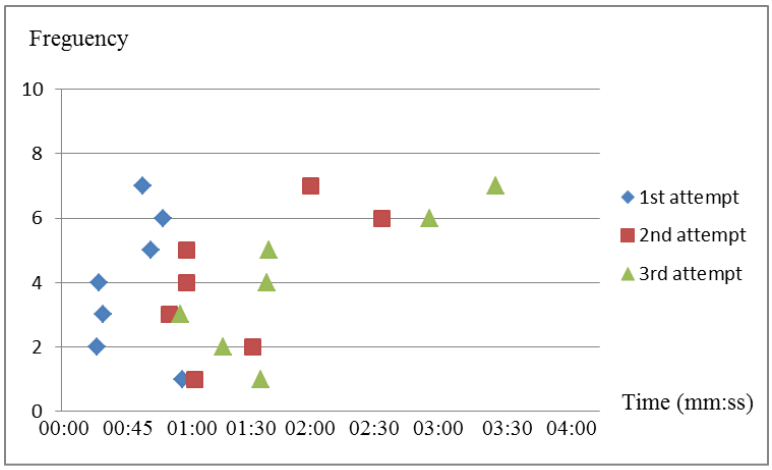

Figure 4.3 Frequency Distribution of Login Time at t_1 Using the UYI Graphical Password.

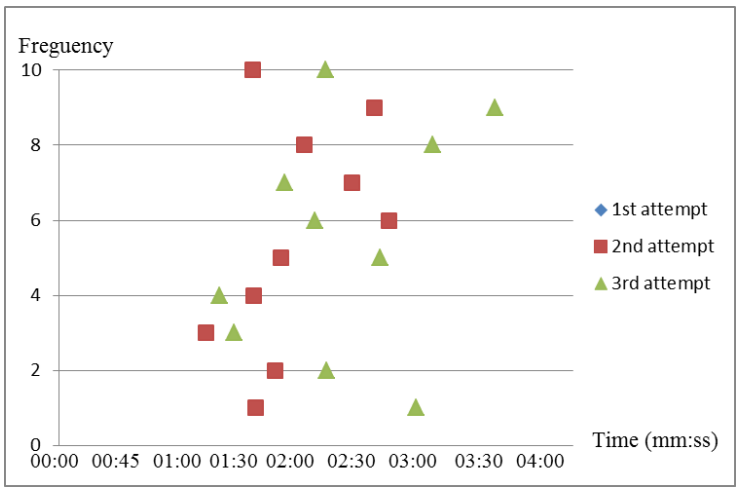

Figure 4.4 Frequency Distribution of Login Times at t_2 Using the UYI Graphical Password.

Table 4.2 Comparison of Login Times in the Simulation Study Using the Proposed Graphical Password With Cue and the UYI Graphical Password.

i^k attempt	Simulation study at t_1			Simulation study at t_2		
	No*	Login Time		No*	Login Time	
		Mean	SD		Mean	SD
Proposed graphical password with cue						
1	96	00:08	00:03	92	00:08	00:07
2	4	00:32	00:00	8	00:38	00:00
3	0	-	-	0	-	-
Total	100			100		
UYI scheme						
1	36	00:39	00:21	0	-	-
2	32	01:20	00:37	40	02:38	00:38
3	32	02:27	01:16	52	03:13	00:56
>3				8		
Total	100			100		

* No. means Number of successful login

4.2.3 Educated Attack

In the second sub-simulation study, the educated attack was simulated by letting the users in Group1 be the illegitimate users attacking the graphical passwords of the users in the same pairs in Group 2 and vice versa because the users in Groups1 and 2 were classmates at the same university.

None of the participants were able to login successfully at the first attempt of the educated attack in the simulation study using either the propose scheme or the UYI scheme. However, the successful logins at the second and third attempts were 16% and 20% when using the proposed scheme and 4% and 48% when using the UYI scheme respectively. The unsuccessful logins by educated attackers using the proposed graphical password with cue were 64%, which is higher than the unsuccessful login at 48% by using the UYI scheme. However, it should be noted that the average login time by the educated attackers using the proposed scheme was much less than the corresponding login time using the UYI scheme as shown in Table 4.3. This weak point may be able to improve with better techniques for blurring the remaining panels in the selected image.

The numerical results cannot support a convincing conclusion about the security comparison of the proposed scheme and the UYI scheme. This leads to a conclusion that the securities of both schemes against the educated attacker are at the same level as stated in Proposition 3.

Table 4.3 Comparison of Login Times by the Educated Guessing in the Simulation Study Using the Proposed Graphical Password With Cue and Using the UYI Scheme.

i^k attempts	**Proposed graphical password with Cue**			**UYI scheme**		
	No	Login Time		No	Login Time	
		Mean	SD		Mean	SD
1	0			0		
2	16	00:47	00:14	4	04:10	00:00
3	20	01:08	00:03	48	04:41	01:32
>3	64*	>3.00		48*	>3.00	
Total	100			100		

*Unsuccessful login.

CHAPTER 5

CONCLUSION

In this dissertation, a graphical password with cue was proposed to achieve better recall rates and shorter login times than the well-known UYI scheme. Three propositions were developed to support the proposed graphical password with cue. The simulation study designed to prove the three propositions was conducted at two different times. t_1, within 1 day after the creation of the graphical passwords, and t_2, at approximately 4 weeks after t_1. The participants in the simulation study were undergraduates and students majoring in information technology.

Three propositions were developed to assert that the proposed graphical password with cue would have better recall rate and shorter login times than the UYI scheme without sacrificing security against educated attackers. The numerical results from the experiment confirmed all three propositions.

Moreover, utilizing the Diffie-Hellman algorithm and the transposition process decreased the probability of successful attacking the message masquerade to $1/6.4024*10^{15}$.

5.1 Limitations of the Current Study

In the simulation study using UYI graphical password, the software was the standard software downloaded from http://arima.okoze.net/illusion/demo/index2.html. In the standard software, the timeout in the login session could not be specified. However, the software in the experiment using the proposed graphical password with cue was developed to allow timeout specification in the login session. The interpretation of the numerical results should include awareness of the differences in the software used in the experiments. Moreover, using only five images to be

graphical passwords cannot prevent a shoulder-sniffing. An attacker can capture possible graphical passwords within five times that a user logs into a system.

5.2 Future Work

In the simulation study, blurring the remaining unselected eight panels by the RGB color was the only technique used to create the cues for the graphical passwords. Variations of the proposed graphical passwords should be widely investigated with other techniques for creating cues, such as slightly distorting the remaining unselected eight panels, finer panels in the image; other images such as an abstract image instead of a clear image as used in the experiment. Moreover, the amount of registered graphical passwords should be more than five images. Furthermore, the memorability and security of the proposed graphical password with cue should be compared with other recognition-based graphical passwords.

BIBIOGRAPHY

Alan, Brown, S.; Bracken, E.; Zoccoli, S. and Doughlas, K. 2004. Generating and Remembering Passwords. **Applied Cognitive Psychology**. 18(June): 641-651.

Behrouz, A. 2008. **Cryptography and Network Security**. New Delhi. McGraw-Hill.

Bicakci, K.; Atalay, N.B.; Yuceel, M.; Gurbaslar, H. and Erdeniz, B. 2009. Towards Usable Solutions to Graphical Password Hotspot Problem. **In Computer Software and Applications Conference COMPSAC'09 33rd Annual IEEE International.** Seattle: IEEE. 2: Pp. 318-323.

Biddle, R.; Mannan, M.; Van Oorschot, P.C. and Whalen, T. 2011. User Study, Analysis and Usable Security of Passwords Based on Digital Objects. **Information Forensics and Security.** 17(February): 970-979.

Blonder, Greg E.1996. **Graphical Password**. U.S.: Lucent Technologies Inc.

Bond, M. 2008. **Comments on GrIDsure Authentication.** Retrieved March 15, 2014. from https://www.cl.cam.ac.uk/~mkb23/research/GridsureComments.pdf

Chiasson, S.; Biddle, R. and Van Oorschot, P.C. 2007. A Second Look at the Usability of Click-Based Graphical Passwords. **In Proceedings of ACM Symposium on Usable Privacy and Security (SOUPS'07)**. New York: ACM. Pp.1-12.

Chiasson, S.; Biddle, R. and Van Oorschot, P.C. 2008. Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. **In BCS-HCI'08 Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction**. Swinton: British Computer Society. Pp. 121-130.

Chiasson, S.; Biddle, R. and Van Oorschot, P.C,. 2009. Multiple Password Interference in Text Passwords and Click-Based Graphical Password. **In CCS'09 Proceedings of the 16th ACM Conference on Computer and Communication Security.** New York: ACM. Pp. 500-511.

Davis, D.; Monrose, F. and Ritter, M. 2004. On User Choice in Graphical Password Schemes. **In Proceedings of the 13th USENIX Security Symposium**. Berkeley: USENIX Association. Pp. 11-11.

De Angeli, A.; Coventry, L.; Johnson, G. and Renaud K. 2005. Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems. **International Journal of Human-Computer Studies**. 63(July): 128-152.

Dhamija, R. and Perrig A. 2000. Déjà vu: A User Study Using Images for Authentication. **In SSYM'00 Proceedings of the 9th USENIX Security Symposium**. Berkeley: USENIX Association. Pp. 4-4.

Dirik, A.; Menon, N. and Birget, J. 2007. Modeling User Choice in the Passpoints Graphical Password Scheme**. In Proceedings of ACM Symposium on Usable Privacy and Security (SOUPS'07)**. New York: ACM. Pp. 20-28.

Dunphy, P. and Yan, J. 2007. Do Background Images Improve "Draw a Secret" Graphical Passwords?. **In CCS'07 Proceedings of the 14th ACM Conference on Computer and Communication Security**. New York: ACM. Pp. 36-47.

Gao, H.; Guo, X.; Chen, X.; Wang, L. and Liu, X. 2008. YAGP: Yet Another Graphical Password Strategy. **In ACSAC '08 Proceedings of the 2008 Annual Computer Security Applications Conference**. Anaheim: IEEE. Pp. 121-129.

GrIDsure. 2009. Retrieved March 15, 2014. From http://www.gridsure.com

Goldberg, J.; Hagman, J. and Sazawal, V. 2002. Doodling Our Way to Better Authentication. **In Proceedings of Human Factors in Computing Systems (CHI'2002)**. New York: ACM. Pp. 868-869.

Hayashi, E.; Christin, N.; Dhamja, R. and Perrig, A. 2008. Use Your Illusion: Secure Authentication Usable Anywhere. **In SOUP'08 Proceedings of the 4th ACM Symposium on Usable Privacy and Security**. New York: ACM. Pp. 35-45.

Hayashi, E.; Christin, N. and Hong, J. 2011. Security Through a Different Kind of Obscurity: Evaluating Distortion in Graphical Authentication Schemes. In **CHI'11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems**. New York: ACM. Pp. 2055-2064.

Jermyn, I.; Mayer, A.; Monrose, F.; Reiter, M.K. and Rubin, A.D. 1999. The Design and Analysis of Graphical Passwords. **In Proceedings of the 8th USENIX Security Symposium**. Berkeley: USENIX Association. Pp. 1-1.

Jhawar, R.; Inglesant, P.; Courtois, N. and M. Angela Sasse. 2011. Make Mine a Quadruple: Strengthening the Security of Graphical One-Time PIN Authentication. In **Network and System Security (NSS), 2011 5th International Conference**. Milan: IEEE. Pp. 81-88.

Madigan, S. 1983. **Picture Memory. In J. C. Yuille (Ed.), Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio Hillsdale**. Lawrence: Erlbaum Associates, Inc.

Menkus, B. 1988. Understand the Use of Password. **Computers and Security**. 7 (April): 132-136.

PASSFACES Corporation. 2009. **The Science Behind Passfaces**. Retrieved May 15, 2013 from http://www.passfaces.com/enterprise/resources/white_papers.htm.

PASSLOGIX. 2006. Retrieved Jan 29, 2014 from www.passlogix.com.

Pering, T.; Sundar, M.; Light, J. and Want, R. 2003. Photographic Authentication Through Untrusted Terminals. **IEEE Pervasive Computing**. 7(April): 30-36.

Perrig, A. and Song, D. 1999. Hash Visualization: A New Technique to Improve Real-World Security. **In Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce**. Kanazawa: Citeseerx. Pp. 1-2.

Ray, P.P. 2012. Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices. **Journal of Information Engineering and Applications**. 3(February): 230-236.

Robert, B.; Sonia, C. and Van, P.C. 2012. Graphical Passwords: Learning from the First Twelve Years. **ACM Computing Surveys (CSUR).** 44(August): 1-23.

SFR. 2006. Retrieved Jan 29, 2014 from www.viskey.com/tech.html .

Smith, R.E. 2002. **Handbook of Authentication: From Passwords to Public Keys**. New York: Addison-Wesley.

Standing, L.; Conezio, J. and Haber, R. 1970. Perception and Memory for Pictures: Single- Trial Learning of 2500 Visual Stimuli. **Psychologic Science.** 19(August): 73-74.

Tao, H. 2006. **Pass-Go, A New Graphical Password Scheme**. Master's thesis, University of Ottawa.

Tao, H. and Adams, C. 2008. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. **International Journal of Network Security**. 7(September): 273-292.

Thorpe, J. and Van Oorchot, P.C. Towards Secure Design Choices for Implementing Graphical Password. **In Proceedings of the 20th Annual Computer Security Application Conferences**. Ottawa: IEEE. Pp. 50-60.

Weinshall, D. 2006. Cognitive Authentication Schemes Safe Against Spyware (short paper). **IEEE Symposium on Security and Privacy**. 1 (May): 300-306.

Weiss, R. and De Luca, A. 2008. PassShapes-Utilizing Stroke Based Authentication To Increase Password Memorability. **In Proceedings of the 5th Nordic Conference on Human-Computer Interactions: Building Bridge**. New York: ACM. Pp. 383-392.

Wiedenbeck, S.; Waters, J.; Birget, J.; Brodskiy, A. and Memon, N. 2005. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. **In SOUP'05 Proceedings of the 2005 Symposium on Usable Privacy and Security**. New York: ACM. Pp. 1-12.

Wiedenbeck, S.; Waters, J.; Sobrado, L. and Birget, J. 2006. Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. **In AVI'06 Proceeding of the Working Conference on Advanced Visual Interfaces**. New York: ACM. Pp. 177-184.

Zvrian, M. and Haga, W.J. 1990. User Authentication by Cognitive Passwords: An Empirical Assessment. **In JCIT Proceedings of the Fifth Jerusalem Conference on Information Technology**. Jerusalem: IEEE. Pp. 137-144.

APPENDICES

APPENDIX A

THE PROPOSED METHOD'S LOGIN TIME AND THE NUMBER OF ATTEMPTS

APPENDIX A

THE PROPOSED METHOD'S LOGIN TIME AND THE NUMBER OF ATTEMPTS

Table a.1

No. of the legitimate user	1 Day (t_1)		4 Weeks (t_2)	
	login time	attempt	login time	attempt
1	0:00:07	1	0:00:13	1
2	0:00:32	2	0:00:05	1
3	0:00:11	1	0:00:10	1
4	0:00:11	1	0:00:04	1
5	0:00:09	1	0:00:38	2
6	0:00:12	1	0:00:05	1
7	0:00:11	1	0:00:03	1
8	0:00:08	1	0:00:04	1
9	0:00:06	1	0:00:03	1
10	0:00:08	1	0:00:03	1
11	0:00:16	1	0:00:04	1
12	0:00:06	1	0:00:08	1
13	0:00:05	1	0:00:36	1
14	0:00:05	1	0:00:38	2
15	0:00:05	1	0:00:04	1
16	0:00:04	1	0:00:03	1
17	0:00:05	1	0:00:11	1
18	0:00:15	1	0:00:16	1
19	0:00:06	1	0:00:06	1
20	0:00:05	1	0:00:07	1

Table a.1 (Continued)

No. of the legitimate user	1 Day (t_1)		4 Weeks (t_2)	
	login time	attempt	login time	attempt
21	0:00:09	1	0:00:04	1
22	0:00:15	1	0:00:16	1
23	0:00:06	1	0:00:06	1
24	0:00:05	1	0:00:07	1
25	0:00:09	1	0:00:04	1

APPENDIX B

THE USE YOUR ILLUSION (UYI) METHOD'S LOGIN TIME AND THE NUMBER OF ATTEMPTS

APPENDIX B

THE USE YOUR ILLUSION (UYI) METHOD'S LOGIN TIME AND THE NUMBER OF ATTEMPTS

Table b.1

No. of the legitimate user	1 Day (t_1)		4 Weeks (t_2)	
	login time	attempt	login time	attempt
1	0:00:58	1	0:04:00	3
2	0:01:04	2	0:02:12	2
3	0:01:32	2	0:02:25	2
4	0:00:52	2	0:03:00	3
5	0:01:00	2	0:01:58	3
6	0:00:17	1	0:01:39	2
7	0:01:36	3	0:02:38	0
8	0:00:20	1	0:01:48	3
9	0:01:00	2	0:03:36	3
10	0:01:18	3	0:02:52	3
11	0:00:57	3	0:02:32	3
12	0:00:18	1	0:02:11	2
13	0:02:34	2	0:04:11	3
14	0:02:00	2	0:04:53	3
15	0:00:39	2	0:02:29	2
16	0:00:43	1	0:03:42	2
17	0:00:49	1	0:02:59	3
18	0:00:39	1	0:03:17	2
19	0:01:39	3	0:02:45	2
20	0:01:28	1	0:03:06	0
21	0:01:40	3	0:03:32	2

Table b.1 (Continued)

No. of the legitimate user	1 Day (t_1)		4 Weeks (t_2)	
	login time	attempt	login time	attempt
22	0:02:57	3	0:03:24	3
23	0:03:29	3	0:02:13	3
24	0:05:00	3	0:04:28	3
25	0:00:39	1	0:02:10	2

APPENDIX C

THE ILLEGITIMATE USSER'S LOGIN TIME AND THE NUMBER OF ATTEMPTS

APPENDIX C

THE ILLEGITIMATE USER'S LOGIN TIME AND THE NUMBER OF ATTEMPTS

Table c.1

No. of the illegitimate user	Proposed method		UYI method	
	login time	attempt	login time	attempt
1	0:00:40	1	0:04:25	3
2	0:00:13	1	0:03:54	3
3	0:00:30	1	0:02:50	2
4	0:00:05	1	0:03:08	3
5	0:00:30	1	0:02:48	2
6	0:00:39	2	0:02:15	3
7	0:00:04	1	0:05:22	3
8	0:00:03	1	0:03:19	3
9	0:00:04	1	0:04:55	3
10	0:00:03	1	0:06:10	0
11	0:00:04	1	0:03:14	3
12	0:00:04	1	0:01:49	3
13	0:00:03	1	0:05:27	0
14	0:00:03	1	0:08:56	3
15	0:00:51	2	0:04:17	3
16	0:00:03	1	0:05:34	3
17	0:00:02	1	0:04:13	0
18	0:00:04	1	0:02:41	3
19	0:00:04	1	0:05:12	0

Table c.1 (Continued)

No. of the illegitimate user	Proposed method		UYI method	
	login time	attempt	login time	attempt
20	0:00:05	1	0:03:21	3
21	0:00:06	1	0:02:28	3
22	0:00:04	1	0:06:05	3
23	0:00:04	1	0:04:03	3
24	0:00:05	1	0:05:14	0
25	0:00:06	1	0:03:18	2

APPENDIX D

THE FLOWCHART OF CALCULATION THE SECRET AND THE SELECTION IMAGE'S POSITION

APPENDIX D

THE FLOWCHART OF CALCULATION THE SECRET AND THE SELECTION IMAGE'S POSITION

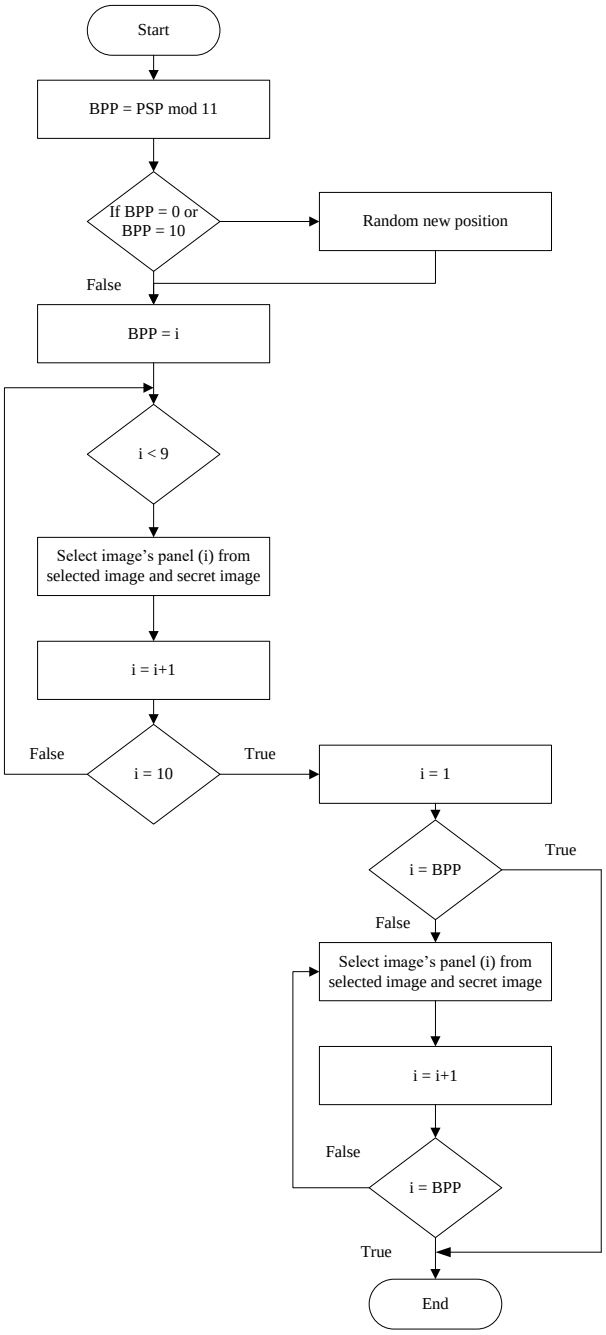

Figure d.1 Transposition's Steps

BIOGRAPHY

NAME	Miss Kanthima Kongsathitsuwan
ACADEMIC BACKGROUND	Bachelor's Degree with a major in Computer Information Management from Saint John's University, Bangkok, Thailand in 1994 and a Master's Degree in Computer Information System at Assumption University, Bangkok, Thailand in 1997
PRESENT POSITION	Lecturer, Information Technology in Business Faculty of Business Administration Saint John's University, Bangkok, Thailand
EXPERIENCES	Received a Scholarship from Saint John's University for Study Master and Doctoral Degree