UDC 004.738.5, DOI:10.2298/CSIS081223028L

A Tabular Steganography Scheme for Graphical Password Authentication

Tsung-Hung Lin[1], Cheng-Chi Lee[2,4], Chwei-Shyong Tsai[3],
and Shin-Dong Guo[4]

[1]Department of Computer Science and Information Engineering,
National Chin-Yi University of Technology, TaichungTaiwan, R.O.C.
duke@ncut.edu.tw
[2]Department of Library and Information Science,
Fu Jen Catholic University, Taipei, Taiwan, R.O.C.
Correspondence: cclee@mail.fju.edu.tw
[3]Department of Management Information Systems,
National Chung Hsing University, Taichung, Taiwan, R.O.C.
tsaics@nchu.edu.tw
[4]Department of Photonics & Communication Engineering,
Asia University, Taichung, Taiwan, R.O.C.

Abstract. Authentication, authorization and auditing are the most important issues of security on data communication. In particular, authentication is the life of every individual essential closest friend. The user authentication security is dependent on the strength of user password. A secure password is usually random, strange, very long and difficult to remember. For most users, remember these irregular passwords are very difficult. To easily remember and security are two sides of one coin. In this paper, we propose a new graphical password authentication protocol to solve this problem. Graphical password authentication technology is the use of click on the image to replace input some characters. The graphical user interface can help user easy to create and remember their secure passwords. However, in the graphical password system based on images can provide an alternative password, but too many images will be a large database to store issue. All the information can be steganography to achieve our scheme to solve the problem of database storage. Furthermore, tabular steganography technique can achieve our scheme to solve the information eavesdropping problem during data transmission. Our modified graphical password system can help user easily and friendly to memorize their password and without loss of any security of authentication. User's chosen input will be hidden into image using steganography technology, and will be transferred to server security without any hacker problem. And then, our authentication server only needs to store only a secret key for decryption instead of large password database.

Keywords: graphical password authentication; security; teganography; protocol.

1. Introduction

Today's network environment is full of dangerous attackers, hackers, crackers, and spammers. Authentication, authorization and auditing are the most important issues of security on data communication. In particular, the user authentication is indispensable to every person living closest friends, but also a key area of security research. Authentication system is based on the passwords which use the alphanumeric for authentication and identifier. Many authentication techniques including biometrics and smart card are the possible and useable applications. The authentication security can be increased, but sometime the passwords seem to remain dominant due to the drawbacks of reliability, security, or cost of other techniques [3][11][13][15]. Biometric techniques make use of physiological or behavioral characteristics to be their identities. Authentication may be secure, but it still needs to resolve the security usability and balance for general usage [13]. And, smart card also needs to type passwords for user authentication. In this paper, we propose a new graphical password authentication protocol to solve this problem. Graphical password technique is one of methods which may provide more secure and more efficiency system for authentication. A set of secure passwords needs to be long enough and random [4], but that will be a problem for human to remember. Everyone will forget their settings everyday if they didn't use again [12]. The research results showed that, when users forget their password, they can only remember part of the correctness [8]. Usable and easy memorization is the main research issues of graphical password authentication. In this paper, we modify and redesign the Passpoints scheme to improve the efficiency of password authentication. Passpoints is a new, more secure and more flexible graphical password that proposed by Wiedenbeck et al. [23]. In addition, the stored passwords database is another common problem for graphical password systems. In our system, we use steganography technique to hide the user graphical password points on the image. Then we transfer the encryption key to server. Server only needs to store a secret key to the database. Server can use the secret key to decrypt user graphical password points from any images which store in the database. By the way, our tabular steganography technique can not only provide more security and also reduce the storage of database information. Furthermore, tabular steganography technique can achieve our scheme to solve the information eavesdropping problem during data transmission.

2. Related Works

Graphical password authentication protocol is first described in Blonder [7]. Blonder proposes a new idea, he lets users use mouse or stylus by themselves to click the picture on presetting correct regions for replacing the traditional text input password. After that, graphical password systems are popular and several different issues are developed [2][9][10][14][20][23].

Graphical password authentication is an image-based authentication technique which can be divided into two categories [2][27]. We describe these two categories, recognition-based authentication technique and recall-based authentication technique as follows.

2.1. Recognition Based

Recognition-based technique is a kind of graphical password authentication techniques which need to choose those correct pictures from many pictures. Dhamija and Perrig [18] propose a scheme which can use Hash Visualization technique [1] to support recognition-based graphical password authentication. Kotadia [16] proposes a new recognition-based graphical password authentication that is a multi-image technique with one step for authentication. In Dhamija and Perrig's system, the system shows some random generated images and the users are asked to select a certain number of images for the authentication in the graphical interface [18], as shown in Fig. 1. Before use, the user needs to set in advance through the authentication sever to identify images. However, the average log-in time is longer than input alphanumeric password, but the result showed that 90% of all participants succeeded and the text-based password with PINS only 70% in the result [27]. The scheme proposed by Dhamija and Perrig was not really secure because the passwords need to store in database and that is easy to see.

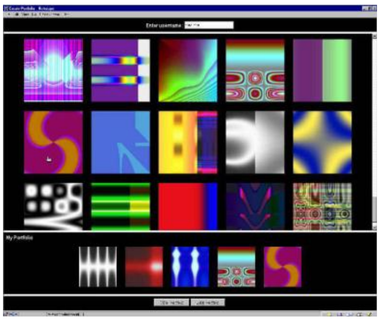
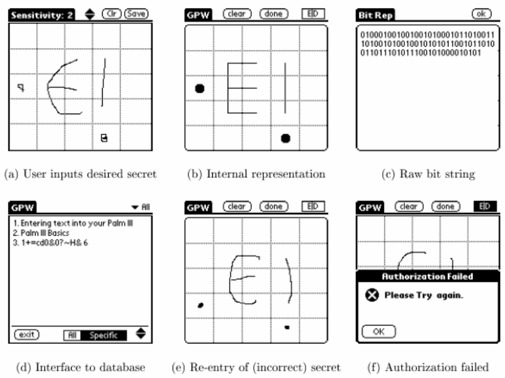


Fig. 1. Random images select used by Dhamija and Perrig [18]

After that, Akula and Devisetty's proposed algorithm [20] is similar to Dhamija and Perrig's, the different is that it uses hash function SHA-1 rather than Hash Visualization technique. Their scheme can be more secure and require less memory than Dhamija and Perrig's [18]. "Passface" is still a multi-image technique developed by Real User Corporation [19]. Users will be asked to choose four face images to be the password. In authentication step, the users see a grid of nine faces, as illustrated in Fig. 2, and only one face was correct image.

Fig. 2. An example of Passface which shows nine faces in a grid (source: www.realuser.com)

User should choose the correct one from these nine faces and this step will repeat four times. "Passface" is based on assumption that people can recognize human faces easier than other pictures. Nevertheless, Valentine [25][26] has shown that "Passface" protocol is very memorable over long interruption. This is easier to remember, but not secure, users click four times in a nine grid has only equal third of the login failure rate of alphanumeric-based password [21].



010001001001001010001011010011
101001010010010101011001011010
0110111010111001010000010101

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

Authorization Failed

Please Try again.

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

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

Fig. 3. Draw-a-Secret (DAS) graphical password system

2.2. Recall Based

Another image-based authentication technique is recall-based authentication technique. "Draw-a-Secret" (DAS) is a famous recall based technique which proposed by Jermyn, et al. [11]. DAS technique allows users to draw their passwords on the interface, as shown in Fig. 3. A user will be asked to draw a simple picture and the picture will be store for authentication. During authentication, the user is asked to draw their unique password. User should draw the same grids in the same sequence, and then the authentication will be success. DAS technique can let users draw by themselves, but need more time then alphanumeric-based password [6], and if the users draw in the middle of two sequences, the system will be error. It is difficult that users should draw their password correct and always be same with the first time. Passlogix [17] has developed a graphical password system which is based on a designated image. In this scheme, user should click different items on an image in order to be authenticated, as illustrated in Fig. 4. User should recall the various items that combined their password and choose these correct items. This scheme is not flexible, but certainty provides more security. Passpoints [23] is a kind of single-images based graphical password scheme and this scheme provide more password space to support more security than textual passwords technique. Passpoints scheme also needs one picture to be the interface and allows users to click anywhere in this designated picture to be the user password. Passpoints provide large password space [10] to ensure the secure and provide more flexible interface for user. In addition, Birget et al. [10] proposed a new scheme that is based on the discretization method. Passpoints is our main subject and we will introduce and improve in next subsection.

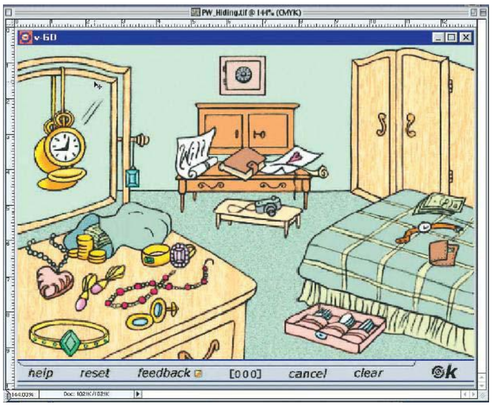


Fig. 4. A recall-based graphical password system

2.3. Passpoints

Passpoints [23] is a graphical password scheme similar to Blonder’s scheme [7]. Passpoints allows any images to be used and users can click on this designated image to complete their password authentication. A rich and colorful image can be divided into hundreds or more squares. The system of Passpoints includes both graphical and alphanumeric interfaces, but we only discussed the graphical interface. The graphical interface includes a rich picture and several buttons, as shown in Fig. 5. The size of the picture is 451 x 331 pixels and the grid square around a click point is set to 20 x 20 pixels. The special buttons of graphical interface is the “See My Password” button, and it allows users to view their password when they are clicking for ensuring the correct password. Users choose sequence of these memorable points to be the password and it can be hashed that means more security of this graphical password system.

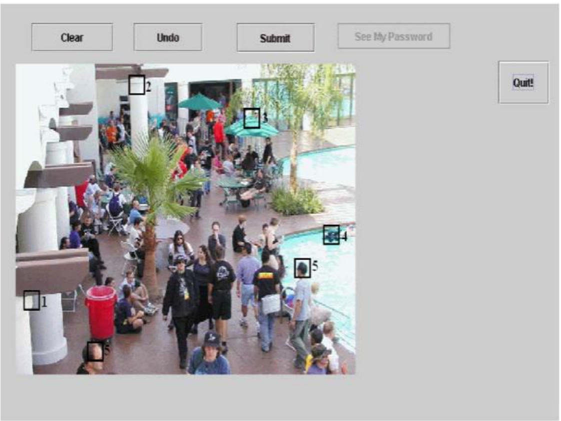


Fig.5. An example of Passpoints graphical password input interface

2.4. Security of Passpoints

The graphical password authentication security is based on the “password space”. We carefully compared the Passpoints graphical password with the alphanumeric password. In Table 1, we show that the password space between graphical password and alphanumeric password. For example, a 64 character alphabet which includes 10 digits, 26 lower-case letters, 26 upper-case letters, underscore, and dot. If a user chooses alphanumeric password length eight over 64 character alphabets, then the entire number of guessing possible password is $64^8 = 2.8 \times 10^{14}$. In graphical password system, there is an image size 451 x 331 = 149,281 and grid square size 20 x 20 = 400, there are about 149281 / 400 = 373 grid squares. If a user chooses 5 click points for the password and the entire number of possible is $373^5 = 7.2 \times 10^{12}$. The image size 451 x 331 is a small password space, but with a big image and more click points will increase the password space, we show the comparison in Table 1. “Passpoints” is secure and have enough password space, but needs to save more pictures for user to use. It will make a huge burden for database storage. In our modify scheme, we will use the “Steganography” technique to reduce the burden of database storage and get our final goal－**without any password table**.

Table 1. Comparison of password space between graphical and alphanumeric password by Susan, et al. [22]

	Image size	Grid square size (pixels)	Alphabet size/ No. squares	Length/No. click points	Password space size
Alphanumeric	N/A	N/A	64	8	2.8 x10^{14}
Alphanumeric	N/A	N/A	72	8	7.2 x10^{14}
Alphanumeric	N/A	N/A	96	8	7.2 x10^{15}
Graphical	451x331	20x20	373	5	7.2 x10^{12}
Graphical	1024x752	20x20	1925	5	2.6 x10^{16}
Graphical	1024x752	14x14	3928	5	9.3 x10^{17}
Graphical(1/2 screen used)	1024x752	14x14	1964	5	2.9x10^{16}

3. Our Graphical Password Authentication Scheme

3.1. Our Scheme

In general authentication process, the password will be hashed and stored for mapping to the correct identifier. It means the authentication database needs to store entire hashed security password. The more the users have registered to the system, the more databases will be stored for huge data. To reduce the amount of data storage is one of our main objectives. We hope that the database be able to more space to do a lot more things. We also hope that the number of users regardless of the size of the database remains the same efficiency.

The notations used in proposed scheme are summarized as follows:

A denotes the user A.
ID denotes the user identity of user A.
GPW denotes the encoded graphical password of user A.
S denotes the server identity.
N denotes a sequence number starting from 1 in the first register.
x denotes the secret key of S used to encrypt and generating a unique storage unique key storage key for each user.
ISN denotes the image serial number which user chosen to be the click image.

|| denotes the concatenation operation.
$\oplus$denotes the bitwise XOR operation.
h() represents a cryptographic hash function.

3.2. Registration Phase

In the registration phase, user will go through a security channel to register this system. We need users to set their *ID*s, login images and graphical password points, then server will use the secret key x to encrypt the graphical password and hide in the image which users choose. When users want to register this system, system will show the images for users to choose, and then compute the hiding values. In our scheme, we use the steganography technique to hide the encryption value in the images which are chosen by users. The encryption scheme can use AES or DES schemes. The steganography technique can also use any present scheme like vector quantization [24] scheme or others. The registration phase is processed in security environment, and the workflow is described as follows.

Step R1. $A \rightarrow S$: User A sends registration request, *ID* and *ISN* to server S.

Step R2. Server shows the registration interface to user *A*. User *A* sets the necessary registration information, *ID*, *ISN*, and *GPW* then computes the verifier $V = h^2(S||GPW||ISN||N)$.

Step R3. $A \rightarrow S$: V

Step R4. Server computes the key $K_A = h\ (ID||h(x||ISN))$, and computes the hiding verifier $hv^{(a)} = V \oplus K_A$.

Step R5. Server will request user to practice about five times for user who can remember his or her graphical password.

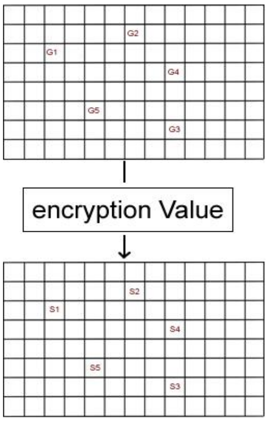


Fig. 6. Our mapping scheme use steganography technique

For example, an image will divide into many grids and we use information hiding technology to store secret key *x* and password in this image, as illustrated in Fig. 6. In Fig. 6, we also show the grids to explain the information hiding. We set a key *x* for secret key and use click five points which definition to G1, G2, G3, G4 and G5, respectively. We use secret key *x* and the graphical password points to do steganography, then hide the encryption value in five secret points S1, S2, S3, S4 and S5 in the image which is chosen by user. The hiding points are embedded in the same place as the graphical password points.

3.3. Login Phase

When a user wants to login the system, the user needs to input his or her *ID* and choose the correct image and click correct graphical password points. Then server will take the hiding value to authenticate user. In the login phase we have two symbols are *ra* and *rs*, *ra* is the random number which is decided by the arrangement of nine grids and *rs* is the random number chosen by server. If the users forget their chosen graphic points (locations) or images they uses, then they should bring up their petition and process the system's identity verification procedure. If the users have passed the identity verification, then they will redo the registration phase to set their new passwords. The flow is similarly to the processing of currently password forgotten processing phase. No one can help you to get your forgetting password. Because of everyone should carefully keep their passwords by themselves.

The workflows of login phase are described as follows.

Step L1. $A \rightarrow S$: *ID*, *ra*

Step L2. Server computes $K_A = h\ (ID||h(x||ISN))$, and then reduces the $hv^{(a)}$ from the image.

Server computes $V=hv^{(a)} \oplus K_A$ and $h(\ V \oplus ra)$.

Step L3. $S \rightarrow A$: *rs*, $h(\ V \oplus ra)$

Step L4. *A* computes $V = h^2(S||GPW||ISN||N)$, then computes $\mathrm{h}(V \oplus ra)$.

If $\mathrm{h}(V \oplus\ ra)$ equals to the received one, then the user *A* authenticates server *S*.

Then *A* computes

$\mathrm{d}_1 = \mathrm{V} \oplus \mathrm{h(S||GPW||ISN||N)}$,

$\mathrm{d}_2 = \mathrm{h(S||GPW||ISN||N)} \oplus \mathrm{h}^2\mathrm{(S||GPW||ISN||N+1)}$,

$\mathrm{d}_3\mathrm{=h(h}^2\mathrm{(S||GPW||ISN||N+1)||rs)}$.

Step L5. $A \rightarrow S$: d_1, d_2,d_3

Step L6. Server *S* uses the hiding verifier to compute $u_1=d_1 \oplus V$, then computes h(*u*1). Then *S* verifies it whether equal to *V*, or terminates this session.

S computes $u_2=d_2 \oplus u_1$ and will get $h^2(S||GPW||ISN||N+1)$.
Finally, if $h(u_2||rs)$ equals to d_3 then the server authenticates A.

The “Passpoints” system needs to store user ID, images and password table in the database. In our scheme, we use steganography technique to hide the user graphical password points in the image and our server only needs to store a secret key *x*. Server can use the secret key *x* to decrypt users’ graphical password points from any images which are stored in the database.

3.4. Analysis of Our Scheme

The Security of Our Scheme

We will discuss some attacks that may occur on our scheme and describe how to resist these attacks and analyze the guessing attack. Although the graphical password scheme can resist the guessing attack, but our scheme can improve it and spare larger password space. The graphical password system assigns one user with an image and that will let the database store too much information. In our scheme, an image is chosen from a group and many users can share the same image because the secret key *x* is the same and the recognition scheme can provide more security for our system.

Resistance to Replay Attack

Suppose that N = *n* and the hacker or adversary has captured all the past authentication messages of user A which $\{d_1(i), d_2(i), d_3(i)\}$ for i = 1, 2, 3…., and *n*-1. The correct hiding verifier of *A* is $h^2(S||GPW||ISN||n)$, and the hacker or the adversary cannot login into the system by using $\{ d_1(i), d_2(i), d_3(i)\}$, where $1 < i < n-1$. The each value is as follows:

$d_1(i)= h^2(S||GPW||ISN||i) \oplus h(S||GPW||ISN||i)$
$d_2(i)= h(S||GPW||ISN||i) \oplus h^2(S||GPW||ISN||i+1)$
$d_3(i)= h(h^2(S||GPW||ISN||i+1)||rs)$

If the hacker or adversary replaces the $d_2(n)$ and $d_3(n)$ with $d_2(i)$ and $d_3(i)$,where i = 1,2,3…, and *n*-1 during *A* login phase. Server will be aware of this crafty attack, because $h((d_2(i) \oplus (d_1(n) \oplus h^2(S||GPW||ISN||n)))||rs(n))$ will be not equal to $d_3(i)$ which is $h(h^2(S||GPW||ISN||n+1)||r(i))$. Another case is that the hack or adversary could cheated and fooled into the server *S* to replace the verifier $h^2(S||GPW||ISN||n)$ with $h^2(S||GPW||ISN||i)$ of *A*, where $1 < i < n-1$. But the hacker cannot impersonate user *A* to login *S* because $rs(n)$

$\neq rs$(i), and h((d_2(i)$\oplus$(d_1(n)$\oplus$h^2(S||GPW||ISN||n)))$\oplus$$rs$($n$)) is not equal to d_3(i). On the other hand, the hacker or adversary do not know the h^2(S||GPW||ISN||n), and certainly he cannot generate it. It is impossible to send correct $h(h^2(S||GPW||ISN||n) \oplus ra)$ to user A in the step L3 when finish receiving the *ra* sent from user A in step L1. Therefore, the hack or adversary cannot be successful to emulate server to cheat user A by such replay attacks we had decried before. Our scheme can certainly resist the replay attack.

Resistance to Guessing Attack and Improve Password Space

In the input phase, we show nine images for the user to choose and each image size 451 x 331 has 7.2 x 1012 numbers possibility to guess [5], and now the numbers of possibility were 9 x 7.2 x 1012. We just discuss about the guessing attack and the security is based on the password space. The password space in our scheme can be increased and our scheme can provide more security and efficiency in graphical password system. Although the graphical password system can resist the guessing attack but in our scheme, we can provide larger password space than Passpoints and the nine grids scheme also can help us to resist more attacks.

Resistance to Forge Attack

We use the nine grids arrangement to be the random number *ra* for user and server *S* selects random number *rs* to user. These random numbers will be different from every login processes. If a hacker can obtain all the information which is sent on the internet, the hacker did not know the graphical password. Hacker cannot compute the correct authentication data which is $h(S||GPW||ISN||n)$ and also cannot to produce the correct keys {d_1, d_2, d_3}. The *ra* used by user to authenticate the server and the *rs* used by server to authenticate user, only the legal user and server can get the correct values.

Resistance to Password-File Compromise Attack

Usually, the authentication server saves the keys *N* and *ISN* in the password-file. In our scheme, we need not to save password table, because the keys *N* and *ISN* are small and we use them to hide the h$v^{(a)}$ into the image. We suppose the password file of server has been compromised by hacker or adversary. If hacker has obtain the *ISN*, *N* and the hv(a) of user A. The h$v^{(a)}$ is the hiding verifier of user A and the value is $h^2(S||GPW||ISN||n) \oplus K_A$, the *ISN* and *N* are not secret. But the hacker cannot compute correct $h^2(S||GPW||ISN||n)$ because he do not know the K_A which is $h(A||h(x||ISN))$. The secret key x can resist the password-file attack. Only server *S* can use secret key x to take out the hiding value from images. And, only server *S* can contrast them when the hiding value has been changed. If the secret key x

has been not secret anymore, the server should change another secret key and all the users should choose their new graphical passwords and register to *S* again.

Table 2. The attacks and security features on graphical password

Graphical Password Scheme	Techniques		Possible Attack Methods						Security Features on Graphical Password					
	Recognition	Recall	Brute force	Dictionary	Guessing	Spyware	Shoulder surfing	Social	Large password space	Randomly assign	Hash function	Image variation	Decoy images	Repeat verification
Jansen et al.	V		V	X	V	X	V	X	X	V	V		V	
Passfaces	V		V	V	V	X	V	X	X	V			V	
Triagle	V		V	X	V	X	X	X	V	V			V	
Movable Frame	V		V	X	V	X	X	X	V	V			V	
Intersection	V		V	X	V	X	X	X	V	V			V	
Pict-O-Lock	V		V	X	X	V	X	X	V	V		V	V	V
Déjà Vu	V		V	X	V	X	V	X	X	V	V		V	
Blonder		V	V	X	V	X	V	X	V					
VisKey SFR		V	V	X	V	X	V	X	X					
Passlogix v-Go		V	V	X	V	X	V	X	X					
PassPoints		V	V	X	V	X	V	X	V		V			
DAS		V	X	V	V	X	V	X	V		V			
V=Yes X=No Blank=not mentioned														

Resistance to Insider Attack

The insider attack is named that user A uses the same graphical password to access several servers for convenience. If the insider hacker of server has obtained the graphical password *GPW*, then he can impersonate user A to access other servers. Actually, it is not easy and the insider of server cannot directly obtain the *GPW*, because the user cannot reveal *GPW* from server in the registration and login phases. The insider server also cannot know the value of *GPW* from user A. Another supposing that is the server wants to impersonate user A to log into another servers. If a vicious server knows the hiding verifier $h^2(S||GPW||ISN||n)$, and then try to impersonate A to log into another server, say S^*. Then, the $h^2(S||GPW||ISN||n)$ will not be equal to $h^2(S^*||GPW^*||ISN^*||n^*)$ even if $GPW^* = GPW$, $ISN^* = ISN$ and $n^* = n$. The insider server cannot successfully impersonate user A to login S^*. Our scheme can certainly resist the insider attack.

Resistance to Denial-of-Service Attack

Recently, denial-of-service (DOS) attack becomes the important issue on data communication security. To achieve prevention from the denial-of-server attack, server S has to make sure that u_2 computes correctly. The d_3 can protect the integrity of d_1 and d_2. And, the d_3 can be used to calculate the u_2, and any unauthorized changes of d1, d_2 and d_3 will be found in the server. The hacker or adversary cannot disable any user’s account and the proposed scheme can really resist the denial-of-server attack. Our scheme can resist many kinds of attacks and improve the password space of the Passpoints system. In Table 2, Hafiz et al. [28] show the features and possible attacks of graphical password systems, we use this table to prove our improvement and our features. The Passpoints will be attacked by guessing but the large password space can resist it. We use nine grids to decrease password space and will be more effective to resist attacks.

Improve Database Storage

Recognition based graphical password techniques has a big problem that is to store many images for users. The password database needs to store ID, password table, images and other information which server need. In the premise, server needs enough space to store many sorts of information, especially the images. It will cause equipment burden. In our scheme, we successfully overcome this problem that database does not have to store the large data instead the secret key x. No matter how many users use the system, server just needs to pass the secret key x and key x is only for server using. Although in our scheme also need to store some images but when the user member increases, our scheme will still be a very effectual scheme.

3.5. Security Policy

In graphical password system, shoulder-surfing is a big problem but many researches can solve this problem. Shoulder-surfing means a person who stands on the back of user and wants to see the password when user inputs their passwords. We introduce some schemes and our policy to prevent shoulder-surfing problem. First scheme is developed by Sobrado and Birget [14] and which system displays a number of pass-objects among many different objects. User needs to recognize pass-objects to be authenticated. Second scheme is developed by Man, et al. [22], user needs to select a number of pictures as pass-object, but each pass-object has several variants and each variant is unique code. Third scheme is developed by Hong, et al. [5], and this scheme still uses pass-object, but allows user to assign their own codes to pass-object variant. Shoulder-surfing is a problem, but we propose a simple scheme to prevent this problem. In traditional authentication phase, User uses mouse to click their correct passwords on the interface which uses the left-button of mouse. Our improved scheme is that we can use the right-button of mouse to confuse the person who wants to see the password input. Any person wants to see the password but will not know which clicks are correct. We can set our system to accept only left-button, but let right-button of mouse to click and display. User can use left-button or right-button of mouse, but only the designated-button will be accept and authenticated.

3.6. Usability of Graphical Password

The usability is very important of graphical password and number of existing graphical password schemes available on the internet. We discuss about the usability and explain why the “Passpoints” can really use in the future. In Table 3, we show the usability features of graphical password which is made by Hafiz, et al. [28] and there are 12 schemes in the table to compare with their usability. The Passpoints scheme is the best of these 12 schemes in compare with each usability feature.

The Passpoints scheme is the only scheme that can be considered as an efficient scheme. The input reliability and accuracy are one of the features which can provide the usability and users can easily remember their graphical password. Even we use nine grids but do not spend many times and we believe that our modified Passpoints still can keep efficient. For user to use our system, user clicking one of nine pictures is just like to choose one of the correct points in Passpoints. Although this is easy but can really improve the security and also can keep efficient. If the users forget their setting points or images, they can redo the setting phase by the certified phase that same as the traditional alphanumeric password certified phase.

Table 3. The usability of graphical password

Graphical Password Scheme	Techniques		Usability Features on Graphical Password												
	Recognition	Recall	Memorability								Efficiency	Input reliability &	Easy and fun to use	Grid based	Drawing password
			Meaningfulness	Human faces	Organized by theme	User assign image	Leon based	Abstract image	Navigating image	Freedom of choice					
Jansen et al.	V		V		V						X		V	V	
Passfaces	V			V		V					X	V	V	V	
Triagle	V						V				X		V		
Movable Frame	V						V				X		V		
Intersection	V						V				X		V		
Pict-O-Lock	V						V				X	V		V	
Déjà Vu	V							V			X		V	V	
Blonder		V	V			V				V	X				
VisKey SFR		V	V			V				V	X	V			
Passlogix v-Go		V	V		V				V		X		V		
PassPoints		V	V			V				V	V	V	V	V	
DAS		V	V									X		V	V
V=Yes X=No Blank=not mentioned															

4. Conclusion

In the graphical password systems, we need the image big enough to ensure the security. Because of the large enough images can be cut into many enough sub-blocks to meet the users to set their passwords. In a small screen device, the problem is how to provide a large enough password space on a small image. The research of Passpoints suggested that user might be handled by magnification of any area of the chosen image [23]. Our research suggests that user can move the image in small screen by mouse. In the screen, the system will show the given area and when user hold the left button of mouse then user can move the image in this area that means we can put a big image in a small screen device like PDA. The limitation of graphical password system has some important issues. First, the image should be colorful and rich enough, the image should be a big enough to provide large enough password space to keep the security. And when input password may click in the middle of two grids, the fault tolerance can be set to solve this problem. Second issue is efficiency; users to use the mouse to enter a password may be slower than the keyboard. However, graphical password still has value and possibility instead of alphanumeric password. The most important issue is the human memory. People should spend more time learning and practice the graphical password but user's thinking and feeling this kind of graphical password will be much easier than alphanumeric password [23]. Finally, this paper reports a new scheme of graphical password and combines with another technology to improve database of server. In cryptography, security is based on the strength of password. Most passwords belong to alphanumeric password which is developed from symmetric cryptographic algorithm to asymmetric cryptographic algorithm. That shows the importance that saving password is in password-table. We provide a new scheme of graphical password and prove that our scheme can solve the problem of database storage. All information can be steganography to achieve our scheme and can solve the problem of database storage. Furthermore, the information eavesdropping problem during data transmission can be overcome by our tabular steganography technique. Overall, our modified graphical password system can help user easy and friendly to memory their password and without loss of any security of authentication. User's chosen input will hide into image using steganography technology, and transfer to server security without any hacker problem. And then, our authentication server only needs to store a secret key *X* for decryption instead of large password database.

Acknowledgment. The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 99-2221-E-030-022.

References

1. A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce. (1999)
2. A. Paivio, T. B. Rogers, P. C. Smythe, “Why are pictures easier to recall then words?”, Psychonomic Science, Vol.11, No.4, pp.137–138. (1999)
3. C. C. Lee, M. S. Hwang, W. P. Yang, “A Flexible Remote User Authentication Scheme Using Smart Cards”, ACM Operating Systems Review, Vol. 36, No. 3, PP. 46-52. (2002)
4. C. S. Tsai, C. C. Lee, M. S. Hwang, “Password Authentication Scheme: Current Status and Key Issues”, International Journal of Network Security, Vol.3, No.2, pp.101-115. (2006)
5. D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware", Proceedings of International conference on security and management. Las Vergas, NV. (2004)
6. D. Weinshall, S. Kirkpatrick, “Passwords you’ll never forget, but can’t recall”, Proceedings of CHI 2004 ACM Press, New York, pp. 1399-1402. (2004)
7. G. E. Blonder, “Graphical password”, United States Patent 5559961. (1996)
8. H. P. Bahrick, “Semantic memory content in permastore: fifty years of memory for Spanish learned in school”, Journal of Verbal Learning and Verbal Behavior, Vol. 14, pp. 1-24. (1984)
9. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords", Proceedings of the 8th USENIX Security Symposium. (1999)
10. J.C. Birget, D. Hong, and N. Memon. "Robust Discretization, with an Application to Graphical Passwords". IEEE Transactions on Information Forensics and Security, Vol. 1, pp. 395-399. (2006)
11. J. Scholtz, J. Johnson, “Interacting with identification technology: can it make us more secure?”, Proceedings of the CHI 2002 Extended Abstracts, ACM Press New York, pp. 564–565. (2002)
12. J. T. Wixted, “The psychology and neuroscience of forgetting”, Annual Review of Psychology, Vol.55, pp. 235–269. (2004)
13. L. Coventry, A. De Angeli, G. I. Johnson, “Usability and biometric verification”, ATM interface, CHI 2003 Proceedings, pp. 153–160. (2003)
14. L. Sobrado and J. C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4. (2002)
15. M. A. Sasse, S. Brostoff, D. Weirich, “Transforming the ‘weakest link’-a human/computer interaction approach to usable and effective security”, BT Technical Journal Vol.19, pp.122–131. (2001)
16. M. Kotadia, "Microsoft: Write down your passwords", ZDNet Australia, May 23. (2005)
17. Passlogix, "www.passlogix.com", last accessed in June. (2005)

18. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication", Proceedings of 9th USENIX Security Symposium. (2000)
19. RealUser, "www.realuser.com", last accessed in June. (2005)
20. S. Akula, V. Devisetty, "Image Based Registration and Authentication System", Proceedings of Midwest Instruction and Computing Symposium. (2004)
21. S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation", People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag. (2000)
22. S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme - WIW", Proceedings of International conference on security and management, Las Vegas, pp. 105-111. (2003)
23. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a grapgical password system”, International Journal of Human-Computer Studies, Vol.63, pp.102-127. (2005)
24. T. -S. Chen, C. -C. Chang, and M. -S. Hwang, “Virtual image cryptosystem based upon vector quantization” , IEEE Transactions on Image Processing, Vol. 7, No. 10, pp. 1485-1488. (1998)
25. T. Valentine, "An evaluation of the Passface: personal authentication system", Technical Report, Goldsmiths College, University of London. (1998)
26. T. Valentine, "Memory for Passfaces after a Long Delay", Technical Report, Goldsmiths College, University of London. (1999)
27. X. Suo, Y. Zhu, G. Scott. Owen, “Graphical Password: A Survey”, Proceedings of the 21th ACSAC IEEE COMPUTER SOCIETY. (2005)
28. M. D. Hafiz, A. H. Abdullah, N. Ithnin, H. K. Mammi, “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”, Proceedings of second Asia International Conference on Modelling & Simulation, IEEE Computer Society. (2008)

Tsung-Hung Lin received the B.S. degree in computer science from Tamkang University, Taiwan, Republic of China, in June 1988 and the M.S. and Ph.D. degrees in Computer Science and Information Engineering from the National Chung Cheng University, Taiwan, Republic of China. He joined the faculty of Department of Information Management, Hsing Wu College, Taiwan, Republic of China, as an associate professor in August 2005. Since 2007, he has been an associate professor at the Department of Computer Science and Information Engineering at National Chin-Yi University of Technology, Taiwan, Republic of China. His research interests include wireless communication and mobile computing, the next-generation mobile network and system, wireless personal area network, wireless sensor network, Steganography, and multimedia security.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he was an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. From 2010, he is now an assistant professor of Library and Information Science, Fu Jen Catholic University. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 60+ articles on the above research fields in international journals.

Chwei-Shyong Tsai was born in Changhua, Taiwan, Republic of China, on September 3, 1962. He received the B.S. degree in Applied Mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received the M.S. degree in Computer Science and Electronic Engineering in 1986 from National Center University, Chungli, Taiwan. He received the Ph.D. degree in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From August 2002, he was an associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. Since August 2004, he has been an associate professor of the Department of Management Information Systems at National Chung Hsing University, Taichung, Taiwan. Since August 2007, he has been an professor of the Department of Management Information Systems at National Chung Hsing University, Taichung, Taiwan. His research interests include image watermarking, image authentication, information hiding, bio-information and computer networks.

Shin-Dong Guo received the B.S. and M.S. in Photonics and Communication Engineering, Asia University, in 2006 and 2008. His current research interests include information security, cryptography, and mobile communications.

Received: December 23, 2008; Accepted: August 20, 2010.