Information Technology Journal 8 (8): 1170-1179, 2009
ISSN 1812-5638

The Security Analysis and Enhancement of Photographic Authentication

Hsien-Chou Liao, Cheng-Hsiung Hsieh, Ching-Wen Chen and Wei-Chiang Chen
Department of Computer Science and Information Engineering, Chaoyang University of Technology,
168 Jifong E. Rd., Wufong Township Taichung County, 41349, Taiwan, Republic of China

Abstract: The aims of this project were to analyze the security of photographic authentication (PA) systematically, show that PA is vulnerable under the polling attack, and give some suggestions to enhance its security. To achieve the above goals, an automatic attack tool is designed to analysis the security of PA systematically. The tool captures the displayed photos, matches with historical ones to accumulate their counts. It selects the photo with highest count and repeats the process until successful login. In order to interfere with the photo match of the attack tool, a noise displacement method is also used to add noises into the original photos. Correspondingly, two noise reduction techniques are implemented in the attack tool for security analysis of PA with noise displacement methods. Furthermore, a simulation tool is designed to analysis the security of PA under a large number of photo sets. The security of PA is analyzed clearly from the experimental and simulation studies and enhancement ways of PA are also summarized in this study.

Key Words: user authentication, cognition authentication, feature-based image matching, network security, pervasive computing.

INTRODUCTION

In the ubiquitous computing environment, services can be accessed at anywhere, anytime, and using any devices or untrusted terminals. User authentication is the key mechanism for authorizing these services. Current popular authentication mechansim is still based on alphanumeric password or personal identification number (PIN). There are two criteria on its usability and security. One is the password should be simple and easy to remember to increase its usability. The other is the password should be random and difficult to be guessed in order to increase its security. Obviously, the two criteria are conflict since a simple password is not safe and easily guessed. Oppositely, a complex password is safe but difficult to remember. A password is also easily forgotten if it is seldom used. Besdies, the same password is usually used to access several systems or services and thus increases the security risk. Such risk also arises if passwords are written on a notebook or stored in the computer.

Therefore, some studies attempt to propose alternative ways for authentication. Previous experiments related to cognitive psychology have proven that peoples have excellent capability on remembering images, pictures, or photos. It is called pictorial superiority effect. Graphical password is initially proposed by Blonder (1996). A user clicks a series of meaningful square areas on a picture. The authentication is successful if the order and locations are the same as pre-defined sequence. Some related authentication techniques include Passfaces (Brostoff and Sasse, 2000), PassPoints (Wiedenbeck et al., 2005) or cued click points (Chiasson et al., 2007), PassShapes (Weiss and Luca, 2008), and Photographic authentication (PA) (Pering et al., 2003). For Passfaces, a user selects four faces as a password from either male or female datasets. A login procedure is used to verify their selection. Then, a user must select these four faces from four different nine faces in turns. For PassPoints or cued click points, a user must click a series of pre-defined points on an image for successful authentication. For PassShapes, its ideal is from users on memorizing a numeric password by the shape formed by the order of digits on ATM (Automatic Teller Machine) keyboard. A user is authenticated by drawing his pre-defined shapes. For the PA, a user uploads a set of photos to authentication server. When he request for login, the server displays four photos containing one of the user for ten times. That is, the user must select his photo among four ones for ten times to authenticate successfully. Besides, the usability of various graphical authentication techniques is also examined (Eljetlawi and Ithnin, 2008). Some features, such as easy of use and creation, the ease to memory, are suggested to enable the graphical authentication to be more usable for the users. These techniques are

Corresponding Author: Hsien-Chou Liao, Department of Computer Science and Information Engineering,
Chaoyang University of Technology, 168 Jifong E. Road, Wufong Township Taichung County, 41349,
Taiwan, Republic of China Tel: +886-4-23323000/4211 Fax: +886-4-23742375

presented in detail in next section.

Among these techniques based on cognitive psychology, the security of PA is studies further in this paper. PA conforms to the popularity of digital photos. Although authors state that PA is a secure authentication technique for untrusted public terminals, the evolution of hardware computing power and image processing techniques enable that an attack tool can be designed for matching the displayed photos and break PA systematically. Therefore, three tools, including authentication, attack, and simulation, are designed to analyze the security of PA in this paper. According to the experimental and simulation results, the methods for enhancing the security of PA are also summarized.

Graphical password firstly described by Blonder (1996) is based on the principle of pictorial superiority effect. According to the classification of Suo et al. (2006), the graphical password can be classified into two categories. One is recall-based technique. A user is asked to reproduce something created or selected earlier during the registration stage. For example, Passfaces, PassPoints, cued click points, PassShapes belong to this category. The other is recognition-based technique. A user is presented with a set of images. He recognizes and identifies the images selected during the registration stage for passing the authentication. For example, the photographic authentication (PA) belongs to this category. For the recall-based techniques, the password setting in the registration stage is easily influenced by prospective psychological factors, such as sex, skin color, *etc*. For example, a white man prefers to select a good-looking white female as graphical password. A young lady prefers to select images related to food or animal as password. A man prefers to select images related to sports or nature as password. Such prospective psychological factor may cause security issues of the authentication technique. Some authentication techniques are presented in details below:

For the Passfaces proposed by Brostoff and Sasse (2000), a user selects four faces as login password from either male or female datasets firstly. A login procedure is used to verify their selection. The user must select these four faces from different nine faces for four times. Experimental results show that users correctly recalled their Passfaces in 99.98 percent of logins. Passfaces have also proved to be memorable over long periods without use.

For the PassPoints (Wiedenbeck et al., 2005), a user has to select five distinct points on a given image. The image is colorful with many elements that could serve as memorable click points. The password space of PassPoints is determined by the image size and tolerable grid size. For example, if the image size is 1024×752 pixels and the tolerable grid size is 20×20 pixels, the password space of five points equals $(1024\times 762/20\times 20)^5 \approx 2.6\times 10^{16}$. It is larger than a alphanumeric password of length eight over a 64-character alphabet, i.e., $64^8 \approx 2.8\times 10^{14}$. Dirik et al. proposed a model to evaluate whether a given image is well suited for PassPoints system (2007). The model can be also used to analyze possible dictionary attacks against the system. However, it is still troublesome for a user to remember different PassPoints for various servers. The cued click points (Chiasson et al., 2007) is similar to PassPoints except every point is clicked on a different image. The next image is based on the previous click-point. The number of images used in cued click points is huge compared with the single image used in PassPoints. Although the password space of the cued click points is larger than PassPoints, it is time consuming for setting the relationship among the images for different click points at different stages.

Weiss and Luca (2008) proposed an authentication technique called PassShapes. Its ideal is from users on memorizing a numeric password by the shape formed by the order of digits on ATM keyboard. For example, the password “9-2-7-9” is a triangle shape. Authentication is to draw simple geometric shapes constructed of an arbitrary combination of eight different strokes. Some simple shapes are not allowed, e.g., circle or ellipse. The system transforms the shapes into a password string. However, PassShapes are easily remembered by users and attackers.

Besides, Renaud and Angeli (2005) discussed two types of graphical authentication techniques: recognition-based and location-based, also called visuo-spatial mechanisms. The authors also proposed a set of metrics which can be used to measure the quality of Web authentication mechanisms.

For the photographic authentication (PA) studied in this paper, the basic principle is quite simple. A photo set that belongs to a user is used as a login password. Authentication is successful if the user can select a photo in the set from four ones for ten turns. PA is easily to fulfill for three reasons. Firstly, digital photos are easily available currently. Secondly, the upload of photos to the authentication server is similar the upload to Web log (Blog) or Web album. Thirdly, the implementation of PA is very easy. Therefore, the security of PA is analyzed clearly in this paper in order to increase its feasibility in the practical environment.

ANALYSIS AND ENHANCEMENT OF PA

For the PA, a user selects the photo belongs to him among four ones and repeats for ten times. Therefore, one forth of the displayed photos belongs to the user. If the times of every displayed photos are counted, those photos belong to the user are expected to have higher counts than the others not belong to him. In order to analyze the security of PA, three tools, authentication, attack, and simulation tools, are designed as shown in Fig. 1.

Authentication tool is used to provide the same process of PA for users. When a user inputs his identifier (ID), four photos that one is selected randomly from user's photos and three are selected from the other users' photos, are displayed. The authentication is successful when the correct photo is selected for ten turns.

An attack tool is designed to emulate the user's operation automatically. The tool enables the setting of an ID to be attacked and captured the displayed photos of the authentication tool. The photos are matched with historical ones to accumulate their counts. The attack tool selects the photo with highest count and repeats the process until successful authentication.

The attack tool is operated in the real scenario. It is time-consuming and only suitable for small number of users. Therefore, a simulation tool is designed to analyze the security of PA under large number of IDs. All the parameters for the PA process are defined and the login count for the successful authentication is recorded to realize the influence of these parameters on the login count.

According to the previous description, the PA technique can be attacked by accumulating the times of displayed photos. Therefore, if an original photo is modified to interfere with the accumulation of photo counts, the attack tool may be difficult to find the correct photo and thus may enhance the security of PA. The popular method to modify a photo is noise displacement and salt and pepper (S&P) noise is a common type of image noise. Therefore, a noise displacement step is added into the process of authentication tool as shown in Fig. 2. An example of noise displacement is also shown in Fig. 3.

The process of the attack tool is shown in Fig. 4. Firstly, a designated user ID is entered and the displayed photos are captured from the authentication tool. A noise reduction step is then used to remove the noise on the captured photos. Each photo is matched with those captured previously. If it is a new photo, its count is set to one. Otherwise, the count of the matched photo is increased by one. After all the four photos are matched, the tool selects the one with highest count. The above process is repeated until the authentication is successful.

Noise Reduction and Fuzzy Match: In order to accumulate the correct times of photos, the match of captured photos and historical photos is the key step. Noises are added to the original photo to interfere with the photo match of attach tool. Therefore, a noise reduction method is used to remove noises as largely as possible. For the S&P noise, two noise reduction methods are used in attack tool. One is the general medium filter and the other is adaptive range order filter (AROF). Medium filter is the most common noise reduction method. AROF is the

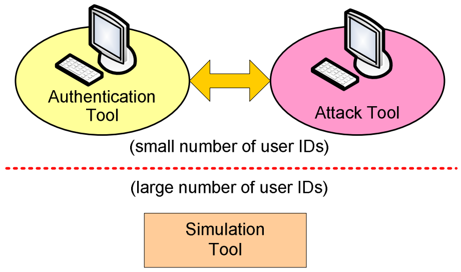


Fig. 2. The security analysis tools

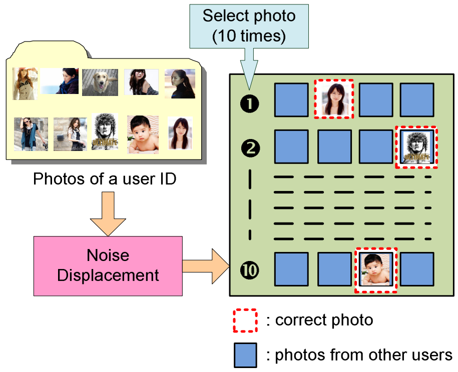


Fig. 1. The process and enhancement of authentication tool

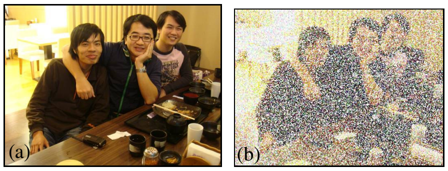


Fig. 3. An example of noise displacement (a) original photo (b) 50% S&P noise

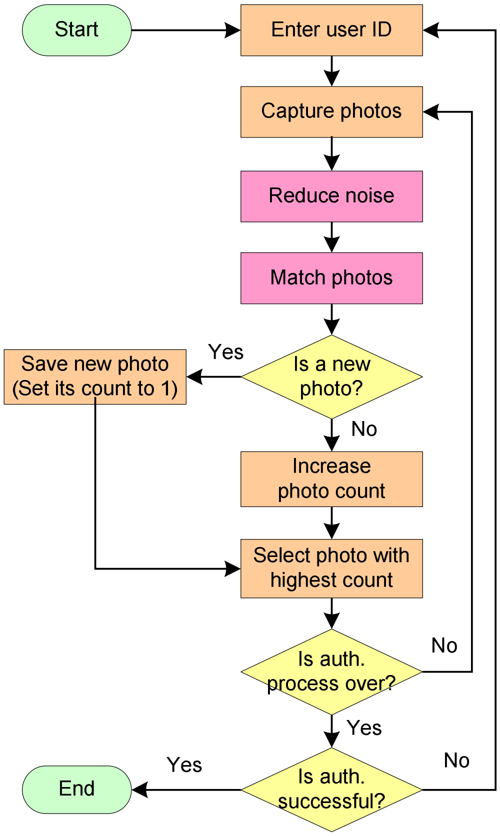


Fig. 4. The process of the attack tool

extension of medium filter and designed in this study. The initial area for AROF is the same as medium filter, i.e., 3×3. If the pixel value ranked in the middle of the nine values is a noise, i.e., zero or 255, a non-noise value is looking forward or backward from the sorted list. If all the values within the 3×3 area are all noises, the range is expanded to 5×5. The area will be expanded further until either a non-noise value is found or the area is expanded to 13×13. AROF is an adaptive method since its area for medium filtering is depended on the noise level. That is, it can keep the balance on the effectiveness and efficiency of noise reduction.

After the noise of a captured photo is reduced, the next step is the match of photos. For the same photo, two random noise displacements cause the results of noise reduction are different. It means that the match of photos cannot simply be based on their basic information, such as size. In this paper, a content-based method is utilized in this step. The method is a fuzzy similarity measurement proposed by Zhai et al. (2005). The method computes the similarity of photos from their histograms. The steps are listed below:

(1) Transform two photos into grey scale and generate a 16 levels color histogram separately.
(2) Sort the 16 levels of two photos and denote as h_l (l=1 to 16) and $h_{l'}$ (l'=1 to 16).
(3) Compute the similarity of two levels when l equals to l' based on the following membership function.

$$\mu_S(h_l, h_{l'}) = \frac{\min(h_l, h_{l'})}{\max(h_l, h_{l'})} \quad (1)$$

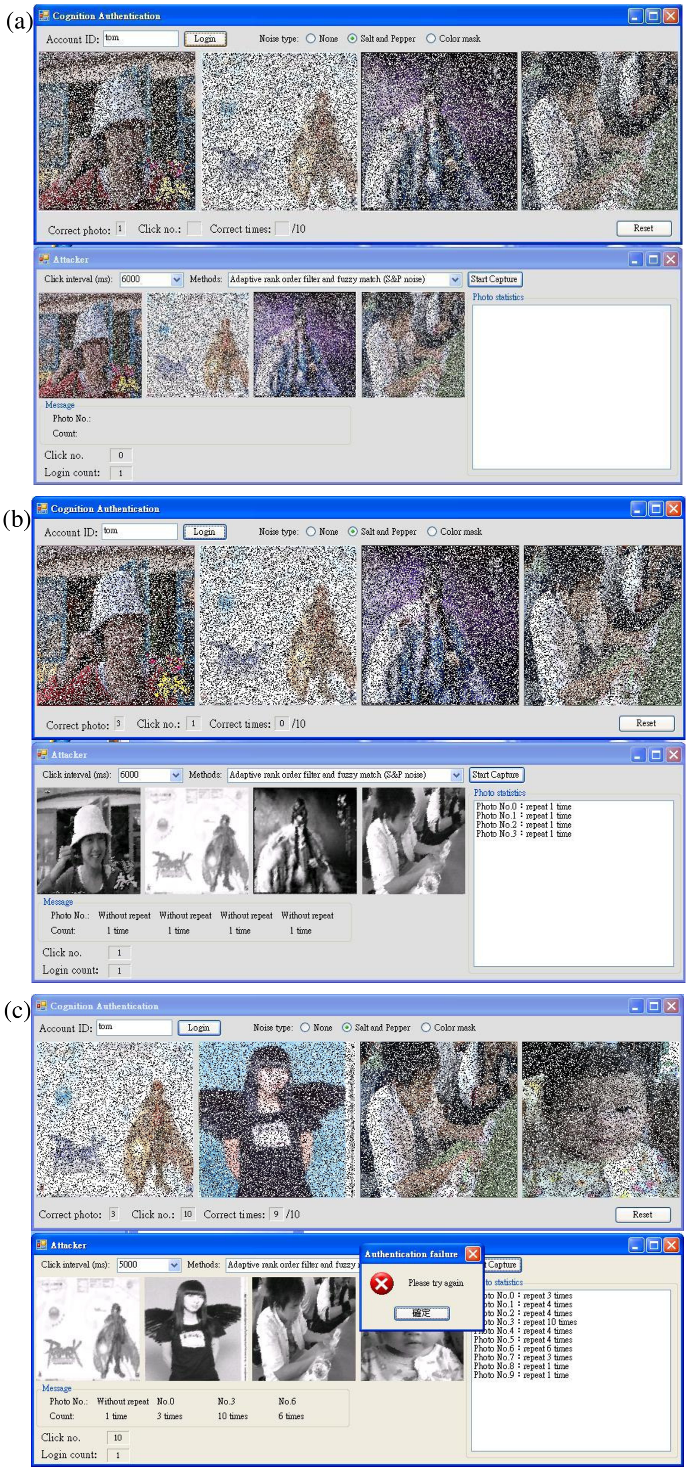
(4) $\alpha 2$-cut defuzzification: $\mu_S(h_l, h_{l'})$ is set to one when it is larger than α2. Otherwise, it is set to zero. That is, this step is used to determine whether $\mu_S(h_l, h_{l'})$ is included in the similarity computation.
(5) Similarity computation: the similarity R_h is computed according to the Eq. (2). H_l Represents the weight of the level l. It is set to one here for uniform weight.

$$R_h = \sum_{l,l'=1}^{M} H_l \mu_{S_{\alpha 2}}(h_l, h_{l'}), \text{ where } H_l = \beta_l \min(h_l, h_{l'}) \quad (2)$$

In the above Steps 1 and 2, the generation of sorted histogram is one-time effort. The histograms of photos can be saved to increase the computation efficiency.

IMPLEMENTATION OF ANALYSIS TOOLS

Three tools described in the previous section were implemented by using Visual Studio 2005. The screen shots of the authentication and attack tools are shown in Fig. 5. In Fig. 5(a), the upper and bottom windows are authentication and attack tools, respectively. For the authentication tool, the noise type can be chosen via the radio buttons. The number of the correct photo, the selection times (click no.) and the number of correct selections (correct times) are shown on the bottom of the tool. They are exposed for experimental study. For the attack tool, it inputs the account to the authentication tool and clicks the "Login" button automatically after the "Start Capture" button is clicked. Then, the photos are captured and displayed on the attack tool. Then, the noises of the captured photos are reduced as shown in Fig. 5(b). The accumulated counts are listed below the captured photos. The attack tool clicks the photo with the highest count. If there is more than one photo with the highest count, the tool selects a photo randomly. After the login procedure is finished, i.e., the tool selects photo for ten turns, a dialog is



(a)

Account ID: tom

Noise type: ○ None ● Salt and Pepper ○ Color mask

Correct photo: 1 Click no.: Correct times: /10

Click interval (ms): 6000

Methods: Adaptive rank order filter and fuzzy match (S&P noise)

Photo No.:

Count:

Click no. 0

Login count: 1

(b)

Account ID: tom

Noise type: ○ None ● Salt and Pepper ○ Color mask

Correct photo: 3 Click no.: 1 Correct times: 0 /10

Click interval (ms): 6000

Methods: Adaptive rank order filter and fuzzy match (S&P noise)

Photo No.:	Without repeat	Without repeat	Without repeat	Without repeat
Count:	1 time	1 time	1 time	1 time

Click no. 1

Login count: 1

```
Photo No.0 : repeat 1 time
Photo No.1 : repeat 1 time
Photo No.2 : repeat 1 time
Photo No.3 : repeat 1 time
```

(c)

Account ID: tom

Noise type: ○ None ● Salt and Pepper ○ Color mask

Correct photo: 3 Click no.: 10 Correct times: 9 /10

Click interval (ms): 5000

Methods: Adaptive rank order filter and fuzzy

Please try again

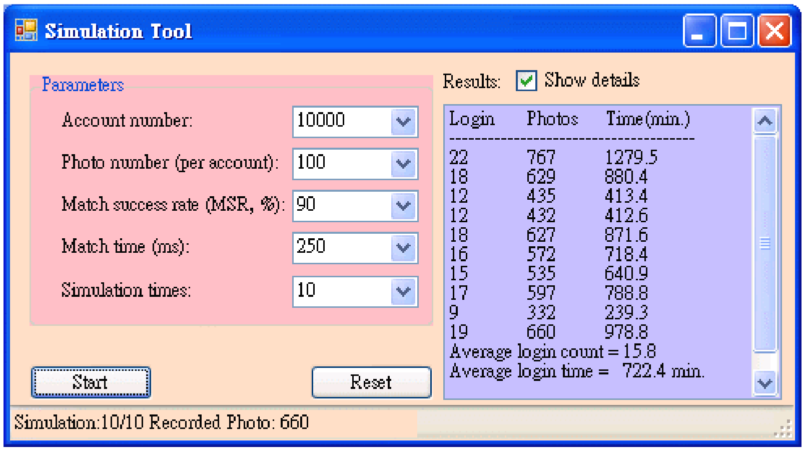
Photo No.:	Without repeat	No.0	No.3	No.6
Count:	1 time	3 times	10 times	6 times

Click no. 10

Login count: 1

```
oto No.0 : repeat 3 times
oto No.1 : repeat 4 times
oto No.2 : repeat 4 times
oto No.3 : repeat 10 times
oto No.4 : repeat 4 times
Photo No.5 : repeat 4 times
Photo No.6 : repeat 6 times
Photo No.7 : repeat 3 times
Photo No.8 : repeat 1 time
Photo No.9 : repeat 1 time
```

Fig. 5. The screen shots of authentication and attack tools (a) photos are captured (b) photos after noise reduction (c) the authentication result



Account number: 10000

Photo number (per account): 100

Match success rate (MSR, %): 90

Match time (ms): 250

Simulation times: 10

Results: ☑ Show details

```
Login    Photos    Time(min.)
-------------------------------
22       767       1279.5
18       629       880.4
12       435       413.4
12       432       412.6
18       627       871.6
16       572       718.4
15       535       640.9
17       597       788.8
9        332       239.3
19       660       978.8
Average login count = 15.8
Average login time =  722.4 min.
```

Simulation:10/10 Recorded Photo: 660

Fig. 6. The screen shot of simulation tool

shown in Fig. 5(c). The attack tool checks the dialog and repeats the above process until a dialog with successful login message is appeared. Then, the login count can be recorded from the bottom of the attack tool.

Obviously, the above analysis process is time-consuming. It is only suitable for a small number of user accounts or photos. In order to realize the possible outcomes under a large number of user accounts, a simulation tool was implemented. Its screen shot is shown in the Fig. 6. Several parameters, including account number, photo number per account, match successful rate (MSR), match time, and simulation times, are designed for the simulation. The MSR is used to simulate the photo match in the attack tool. When noises are added to the photo, it causes the successful rate of photo match is limited under a specific value. When the photo match is fail, the captured photo is deemed as a new one. It causes that the time needed for successful authentication becomes longer. The parameter, match time, is used to estimate the total time needed for successful authentication. The estimated total time equals the total times of photo match multiplying by the match time.

When “Start” button is clicked, the tool lists the simulation results on its right-hand side. For the setting of parameters shown in Fig. 6, the average login count is 15.8 and average time needed for successful authentication is 722.4 minutes.

EXPERIMENTAL AND SIMULATION STUDIES

There are two kinds of studies for analyzing the security of PA.

Table 1: The parameter setting of small number of user IDs experiment

	Parameters			
Items	Noise type	Number of user IDs	No. of photos per user ID	Algorithms
Photo number vs. login count	None	10	10, 20, 30, 40,…,100	Fuzzy match
User ID vs. login count	None	10, 15, 20	10, 20, 30, 40,…,100	Fuzzy match
Algorithm vs. login count	S and P	10	10, 20, 30, 40,…,100	1.Medium filter 2. AROF+Fuzzy match

Experimental Results: The experimental items and parameter settings are listed in Table 1. These three items are used to realize the security related to photo number, user accounts (IDs), and noise reduction algorithms. The results are presented below.

- **Photo number vs. security**: The results are depicted in Fig. 7. When the photo number per user ID is ten, the average login count of successful authentication is about five. The login count is 55 when the photo number is increased to 100. As expected, a large photo number can increase the security of PA.
- **User ID vs. security**: In this experiment, various number of user IDs is used to analyze the security of PA. The results are depicted in Fig. 8. There are three curves for 10, 15, and 20 user IDs, respectively. For the same number of photos per user ID, the increase of user IDs causes the decrease of login count. It means that the increase of user IDs causes the counts of captured photos belongs to the attacked user ID is easily higher than the others.
- **Algorithm vs. security**: In this experiment, two noise reduction algorithms are used to analyze their influence on the security of PA. The results are depicted in Fig. 9. By observing the curves of

MF (medium filter) and AROF, the login counts of AROF is smaller than that of MF. It means that the performance of AROF on noise reduction is better than MF. Besides, if noise can be removed entirely, the result should be close to the result, i.e., the red curve in Fig. 8.

The elapsed time of successful authentication for AROF and MF is also listed on Table 2. Although the computing time of AROF is longer than MF, the login count of AROF is small as shown in Fig. 9. It causes the time of successful authentication is shorter than that of MF.

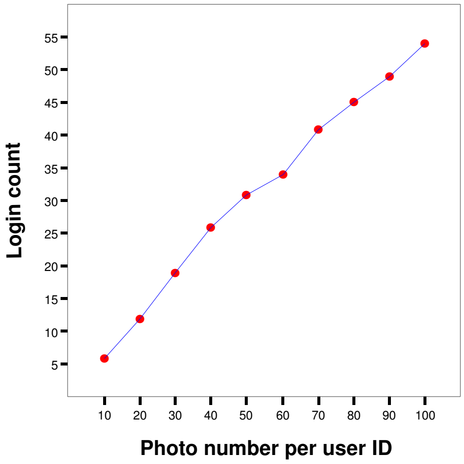


Fig. 7. Photo number vs. login count

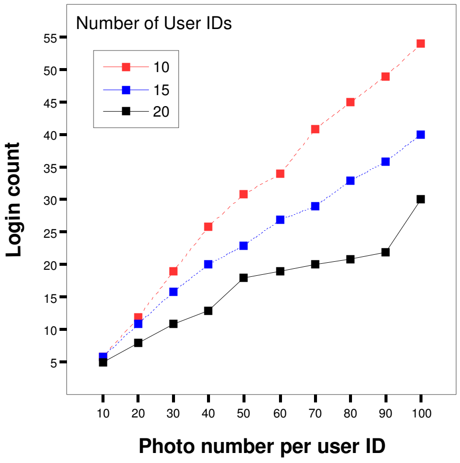


Fig. 8. Number of user IDs vs. login count

Simulation Results: Four simulation items are designed and their parameters are listed on Table 3. They are used to realize the influence of photo number, user IDs, MSR (match successful rate), and the login time. The first two simulations are similar to the previous experiments. The third one is used to analyze the possible influence of noise reduction algorithms. The last one is the estimation of total time needed for successful login. The results are presented below.

Table 2: The time of two algorithms needed for successful authentication

	Algorithms	
	AROF	MF
Photo number	(min.)	(min.)
10	3	3
20	8	8
30	11	13
40	15	17
50	18	22
60	20	28
70	26	34
80	28	42
90	31	49
100	35	56

Table 3: The parameter setting of large number of user IDs simulation

	Parameters		
Items	No. of user IDs	No. of photos	MSR (Match Successful Rate, %)
Photo number vs. login count	2000, 4000,..., 10000	1000, 2000, 3000,..., 10000	100
User ID vs. login count	1000, 2000, 3000,..., 10000	2000, 4000,..., 10000	100
MSR vs. login count	2000, 4000,..., 10000	1000	100, 95, 90,…., 50
Login time	1000	100, 200,…,500	100, 90,…, 60

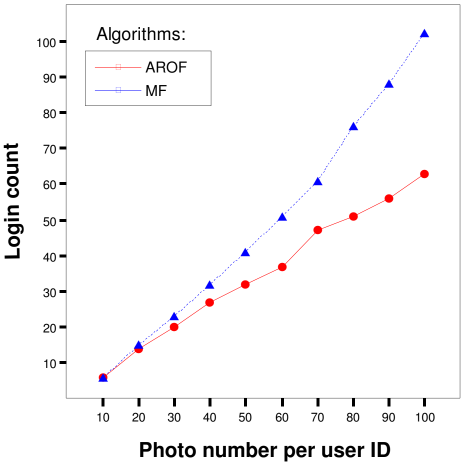


Fig. 9. Algorithm vs. login count

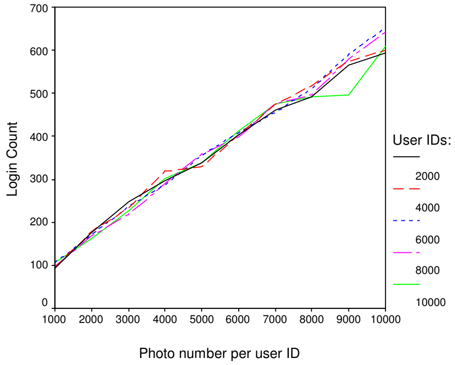


Fig. 10. Photo number vs. login count

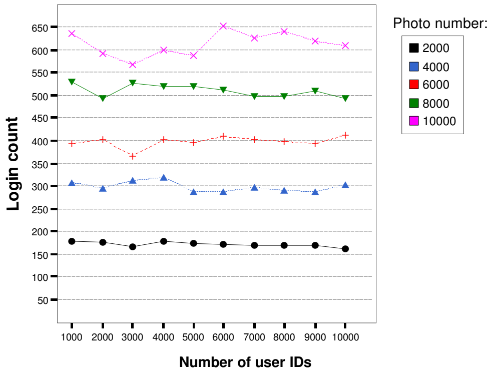


Fig. 12. Number of user IDs vs. login count

- **Photo number vs. security**: The simulation results are depicted in Fig. 10. The login count is increased as the increasing of photo number. It is similar to that in Fig. 7. However, these five curves are very close to each other that differ from that in Fig. 7. According to the previous experimental results in Fig. 7, it means that the security of PA may be compromised since there are usually more than thousands of accounts in a server. But, the simulation results show that the security of PA is almost unrelated to the number of user IDs under large number of user IDs and photos.
- **User ID vs. security**: The simulation results are depicted in Fig. 11. The x-axis is the number of user IDs from 1000 to 10000. The y-axis is the login count. There are five curves in the figure. They represent the login counts from the photo numbers from 2000 to 10000. By observing these curves, the increase of user IDs is almost no influence on the login count. It is the same as the conclusion in the first simulation.

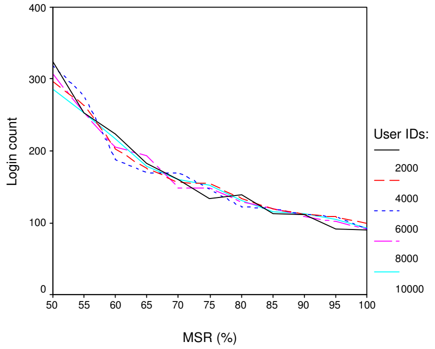


Fig. 11. MSR vs. login count

- **MSR vs. security**: The simulation results are depicted in Fig. 12. The x-axis represents the MSR from 100 to 50 percentages. The y-axis represents the login count. There are five curves in the figure that represent the photo number from 2000 to 10000. By observing the curving, the increase of MSR causes the decrease of login count as expected. The increase of MSR means the attack tool is easier to accumulate the times of captured photos effectively and thus causes the tool can break PA quickly. It means that if some techniques, such as noise, can be added on the photo to decrease MSR to less than 50 percent, the security of PA can be increased several times than the original method.
- **Login time**: In this simulation, the match time of two photos is assumed to 250 milliseconds. The login time under various photo numbers and MSRs are listed in Table 4. When the photo number is 100 and MSR is 100 percentages, the login time is 684 minutes. If the matching time can be shortened to one tenth by using special hardware or software techniques, the login time will be shortened to 68 minutes. It is vulnerable for an authentication server. Therefore, if a technique, such as noise displacement, is used to decrease the MSR to 60 percentages, the login time is increased rapidly to 8752 minutes. Oppositely, if the attack tool wants to increase the MSR; it means the tool needs more computing time for noise reduction. That is, the matching time will be even longer than 250 milliseconds. The login time is longer as well.

Enhancement Suggestions of PA: According to the above experimental and simulation results, the enhancement of PA can be summarized in the following ways:

Table 4: The time needed for successful login under various conditions

	MSR(%)				
Number of photos	100	90	80	70	60
100	684	902	2217	3610	8752
200	2349	3127	5635	8063	13294
300	4632	6163	7869	13345	25864
400	6475	9741	12743	19204	38413
500	10966	14567	19888	28959	45203

1000 user IDs, unit: min.

- In general, the number of user IDs is large for an authentication server. Therefore, the photo number is an important factor related to the security of PA. A user should provide enough number of photos for PA. According to the above simulation on login time, if some technique can keep the MSR under 60 percentages, 100 photos can be the minimum number to ensure enough security of PA.
- Except the noise displacement method, some simple methods can be used to extend the total login time of the attack tool. For example, the server can delay the response of authentication result for several seconds. It is usually used in the general authentication mechanism.
- In order to prevent the attack of a computerized tool, many Web sites utilize a technique called human verification image. It is a distorted image can be only understood by the human but not computer. Alphanumeric data is stored in the image and is difficult to recognize by a tool. Such a technique can prevent the successful authentication of a computerized tool.

The above ways are useful for enhancing the security of PA. They are also important for fulfilling PA in the practical environment.

DISCUSSION

In this study, the security of PA is analyzed systematically by using attack and simulation tools. Several parameters related to the security of PA, including the number of user IDs, number of photos, noise type and reduction algorithm, and MSR, are used in the security analysis. According to the experimental and simulation results, they show that the polling attack could be happened. The security of PA is highly related to the number of photos but less related to the number of user IDs when it is large. Besides, some suggestions, such as noise displacement method, are given to increase the login count for breaking the PA and thus enhance its security. These findings are very useful for considering the implementation of PA in the practical environment.

The authentication techniques of the previous studies are diverse, such as Passfaces, PassPoints, cued click points, PassShapes, and PA. Most of them are analyzed on a small number of subjects to test their usability, such as easy to use, create, or memorize. Only the model proposed by Dirik et al. (2007) for the PassPoints (Wiedenbeck et al., 2005) was designed to analyze possible dictionary attacks again PassPoints. It identifies the most likely region for users to click in order to create a graphical password of PassPoints. In addition to use the identification results for dictionary attacks, the results can also be used to evaluate whether a given image well suited for PassPoints.

Similarly, the attack and simulation tools designed in this study are based on the principle of PA. The tools can be used to not only analyze the possible weakness of PA, but also summarize the enhancement suggestions of PA from the experimental and simulation results. The model proposed previously by Dirik et al. was incorporated with pattern recognition technique to identify the most likely regions, called focus of attention (FOA). In this study, the image processing techniques is incorporated into the analysis tools to enable the analysis process being performed automatically and systematically. Therefore, the analysis of graphical password methods should be incorporated with image processing or pattern recognition techniques to obtain sophisticated analysis results.

CONCLUSION

For the photographic authentication (PA) proposed in the previous study, authors state that polling attack cannot work since attacker cannot deduce which images are the correct ones. However, an attack tool based on image processing and image retrieval techniques is proposed and shows that polling attack is possible. In advance, the experimental results show that the increase of photos can increase the security of PA. However, the increase of user accounts may decrease the security of PA when the numbers of user accounts and photos are small. Besides, noise addition can be also used to interfere with the operation of the attack tool and thus enhances the security of PA.

In advance, a simulation tool is used to analyze the security of PA under large number of photos and user accounts. The results show that the security of PA is increased as the increasing of photo number. The security is un-related to the number of user accounts. Besides, if the noise technique can be used to reduce the match successful rate (MSR) of the attack tool, the security of PA is enhanced several times than the original technique.

PA is an alternative way for providing a more secure way for user authentication than alphanumeric password. The security analysis results and enhancement suggestion presented in this paper is helpful to increase its security. PA is expected to be practiced in the ubiquitous environment and provides a secure and convenient authentication way.

ACKNOWLEDGEMENT

This project was financially supported by the National Science Council under Grant No.: NSC 97-2815-C-324-008-E.

REFERENCES

Blonder, G.E., 1996. Graphical Passwords. Lucent Technologies, Inc., Murray Hill, New Jersey.

Chiasson, S., P.C. van Oorschot, and R. Biddle, 2007. Graphical Password Authentication Using Cued Click Points. In: Research in Computer Security, Biskup, J. and J. Lopez (Eds.). Springer Verlag, Berlin Heidelberg, pp: 359-374.

Dirik A.E., N. Memon, and J.C. Birget, 2007. Modeling User Choice in the PassPoints Graphical Password Scheme. Int. J. of Human-Compu. Stud., 63:102-127.

Eljetlawi, A.M. and N. Ithnin, 2008. Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods. Proceedings of the 3rd International Conference on Convergence and Hybrid Information Technology, Nov. 11-13, Busan, pp: 1137-1143.

Pering, T., M. Sundar, J. Light, and R. Want, 2003. Photographic Authentication Through Untrusted Terminals. IEEE Perv. Comp., 2: 30-36.

Renaud, K. and A.D. Angeli, 2005. My Password is Here! An Investigation into Visuo-Spatial Authentication Mechanisms. Interacting with Comput., 16: 1017-1041.

Suo, X., Y. Zhu, and G.S. Owen, 2006. Analysis and Design of Graphical Password Techniques. Proceedings of the 2nd International Symposium, Advanced in Vis. Comp., Nov. 6-8, Springer, Berlin Heidelberg, 4292: 741-749.

Weiss, R. and A.D. Luca, 2008. PassShapes-Utilizing Stroke Based Authentication to Increase Password Memorability. In: Proceedings of 2008 Nordic Conference on Human-Computer Interaction, Oct. 20-22, Lund, Sweden, pp: 383-392.

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy, and N. Memon, 2005. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. Int. J. of Human-Comput. Stud., 63:102-127.

Zhai, H., P. Chavel, Y. Wang, S. Zhang, and Y. Liang, 2005. Weighted Fuzzy Correlation for Similarity Measure of Color-Histograms. Opt. Commun., 247:49-55.