WP2-D-2

A Study on an Image Synthesis Method for Graphical Passwords

Madoka Hasegawa, Yuichi Tanaka and Shigeo Kato
Graduate School of Engineering, Utsunomiya University
7-1-2 Yoto, Utsunomiya, Tochigi 321-8585 Japan
E-mail: {madoka, tanaka, kato}@is.utsunomiya-u.ac.jp Tel: +81-28-689-6297

***Abstract*— In this paper, we present an image synthesis method for graphical passwords. Graphical passwords are an authentication method that uses pictures as passwords instead of using alphanumeric characters. However, they are usually easy to memorize for not only users but also observers or attackers who stand behind the users. In our method, we combine low frequency components of a decoy picture with high frequency components of a pass-picture. This makes it difficult for observers to recognize the pass-image.**

I. Introduction

Entering a user name and textual password is a major method for the computer login procedure. Unfortunately, this method is vulnerable to spyware and key-loggers. Once such malicious software infects a computer, the password is easily stolen and used by attackers. In addition, it is difficult to remember long complex textual passwords. Studies have shown that users tend to use short passwords or passwords that are easy to remember [1]. This means that textual passwords are easily guessed or broken by attackers.

To address this issue, several authentication methods have been proposed. In this paper, we focus on graphical passwords which use pictures as passwords instead of using alphanumeric characters. It is difficult to steal pictures with key-loggers. In addition, the difficulty in memorizing pictures, such as pets, human faces, and favorite objects, is less than in remembering textual passwords. Although graphical passwords are generally easy for legitimate users to memorize, they are also easy for observers or attackers who stand behind the users to memorize. To alleviate this risk, graphical passwords, which use degraded images, have been proposed [6],[7].

These proposed approaches utilize the property that degraded images look like noise or ink blots for observers and they are difficult to memorize. On the contrary, legitimate users are able to find his/her pass-image easily because the knowledge of the original clear image becomes a clue to remember the pass-image. These methods are effective to enhance the security level against observation attacks. However, the security level and the memorability of pass-images become a trade-off relationship. If the pass-image is degraded too much to enhance the security, the image becomes completely unclear or looks like a random noise. Therefore, the user's ability to recognize the image is degraded and authentication becomes more time consuming. As a result, the system becomes less usable. In addition, graphical passwords require more storage space compare to text passwords.

In this paper, we present an image synthesis method for a user authentication system using graphical passwords. In our method, we combine low frequency components of a decoy picture with high frequency components of a pass-image. For human eyes, it is difficult to recognize the subtle high frequency components. Especially in the case that the person is far from the screen, the high frequency components become less visible. Therefore, our method makes it difficult to know the pass-image for observers who stand behind a user, while it is easy to find the pass-image for the user who is just in front of the screen of the computer or PDA. Our method aims to intentionally mislead observers to hide what is displayed on the screen and draw their attention to the decoy image. Moreover, this method uses less storage space because only high frequency components are stored as user's pass-images.

II. Related Works

Graphical passwords can be classified into two categories: recall-based techniques and recognition-based techniques [2].

In the recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Jermyn, et al. proposed "Draw-a-Secret" method in which users are asked to draw a text or a shape on a 2D grid [3]. Wiedenbeck, et al. proposed the Passpoint system in which users are asked to click several pre-registered points in an image [4].

On the other hand, in the recognition-based techniques, a set of images, which consists of decoys and pass-images, is presented to the user and they are asked to recognize and identify their pass-image that was selected at the registration phase.

Dhamija and Perrig proposed "Déjà vu" system based on Hash visualization techniques [5]. In their system, a set of computer-generated (CG) random pictures are presented to a user and the user is asked to select and register some of them as his/her pass-images. During authentication, the user is asked to identify their pre-registered images.

Harada, et al. proposed a user authentication scheme using unclear pass-images [6]. They overlaid a background image

978-1-4244-5016-9/09/$25.00 ©2009 IEEE

on a foreground image (pass-image) by alpha blending. Then, the blended image was further processed to make it more unclear by image mosaicing and adding random noise. The right image in Fig.1 shows an example of image generated by their method. This method generates a monochrome image as an unclear image. It is difficult to generate a memorable color unclear image with this method because colors in the foreground image and the background image may become completely different in the output image because of the alpha blending process.

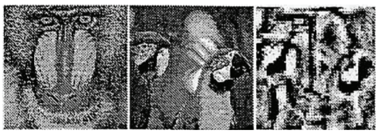
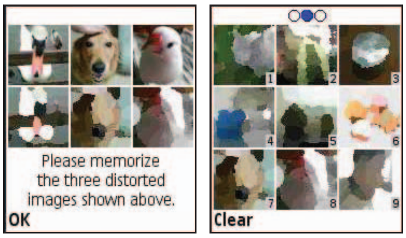


Fig. 1 A graphical password method proposed by Harada, et al. [6] (Left: foreground image, middle: background image, right: blended unclear image.)

Hayashi, et al. proposed a user authentication mechanism which relies on the human ability to recognize a degraded version of a previously seen image [7]. They used an oil-painting filter to degrade portfolio images from the original photos which are selected by the user at the registration phase. Their method is suitable for user authentication on a portable color device.



Please memorize the three distorted images shown above.

Fig. 2 A graphical password method proposed by Hayashi, et al. [7]

Generally, memorizing images of natural objects is easier than memorizing artificial CG images. However, natural images require more storage space than CG images not only for pass-images but also for decoy images. Secure, usable, and storage-saving graphical passwords are desired.

III. Authentication Method

Suppose we use our authentication method for PDAs or web-based services. When a user wants to use a service, s/he may start login procedure at his/her desk and his/her friends or coworkers may see the computer screen when they walk behind his/her desk. Our method aims to prevent such observers from knowing the user's pass-image. If a pass-image is faintly printed on a decoy image, the legitimate user who is close to the PC screen can see the pass-image but someone who is far from the screen cannot recognize the pass-image. Our method tries to utilize this property.

Fig. 3 shows an example of a set of images for a challenge using our graphical password method. Beforehand, users register several images as their pass-images. On the screen, a set of images are shown to the user. Four images are synthesized images which consist of low frequency components of decoy images and high frequency components of other decoy images, or consist of low frequency components of a decoy image and high frequency components of a pass-image. The user is asked to choose a synthesized image in which his/her pass-image is vaguely blended. If s/he does not find any of his pass-images in the set, he is supposed to choose "No pass-image" as his answer. This challenge is repeated several times and if all answers are correct, he will be successfully authenticated. The number of challenges and registered pass-images depends on the requirements for security and usability. If the number is greater, the system becomes more secure but becomes less usable because the user has to remember more pass-images and takes more time for the authentication.

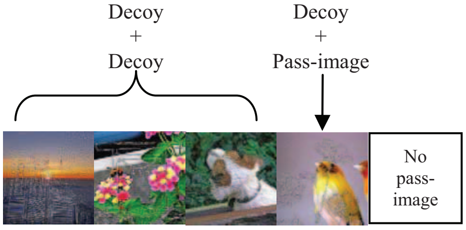


Fig. 3 A set of images for authentication.

IV. Image Synthesis Method

How to generate the synthesized image is key in this authentication system. Fig. 4 shows the flow of our image synthesis method. We used a discrete wavelet transform (DWT) to extract low and high frequency components from images.

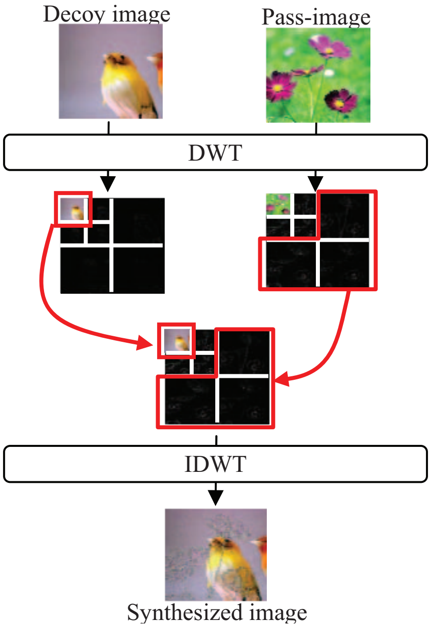


Fig. 4 Overview of image synthesis procedure.

First, DWT is applied to each color plane in a decoy image and a pass-image. The LLx band, that is the lowest frequency band of x-level DWT, contains the average information of the input image. On the other hand, the LH1, HL1, and HH1 bands contain mostly the edges of the images. Names of each sub-band in 2-level DWT is shown in Fig. 5.

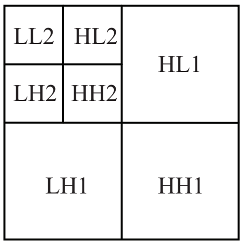
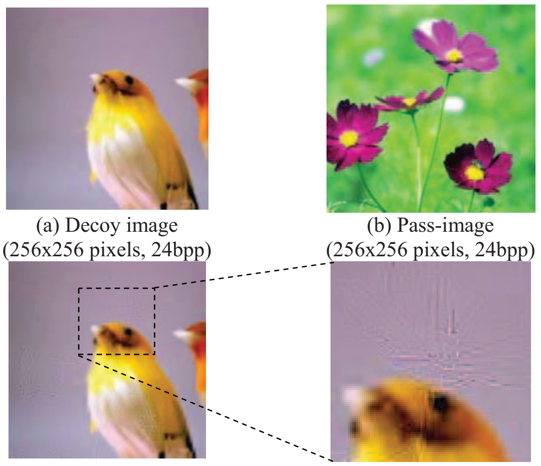


Fig. 5 Names of each sub-band in 2-level DWT.

In the second step, the LL*x* band of the decoy image and the LH1, HL1, and HH1 bands of the pass-image are merged. We set 0 for the middle frequency sub-bands, such as LH2, HL2, and HH2, to add some blur effect for the decoy image. If the decoy image has many edges, these edges are mixed with the edges of the pass-images and it becomes difficult for the user to recognize the pass-image.

After the inverse DWT (IDWT) and merging of color planes, we obtain a synthesized image for our authentication method.

An advantage of this method is storage space reduction for the pass-image. Only the high frequency components, that is LH1, HL1, and HH1 bands, are required to be stored in the system. In general, distribution of signals in these sub-bands follows Laplacian distribution and effective compression is possible. For the authentication, the system randomly chooses a decoy image and mixes it with the pass-image to generate a synthesized image.



(a) Decoy image (256x256 pixels, 24bpp)

(b) Pass-image (256x256 pixels, 24bpp)

(c) Synthesized image

(d) A part of synthesized image (Enlarged 400%)

Fig. 6 An example of synthesized image.

In this study, we used 5x3 DWT which is a reversible DWT used in JPEG 2000 [8],[9]. Low frequency signals and high frequency signals are given by following equations.

$$L(n) = x(2n) + \left\lfloor \frac{H(n-1)+H(n)}{4} \right\rfloor \qquad (1)$$

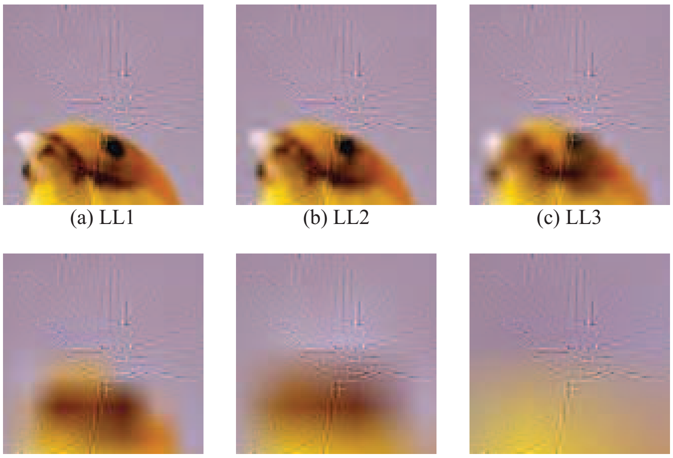
$$H(n) = x(2n+1) - \left\lfloor \frac{x(2n)+x(2n+2)}{2} \right\rfloor \qquad (2)$$

where $x(n)$ is a pixel value in position n. Samples belonging to the low and high frequency sub-bands are represented as $L(n)$ and $H(n)$ respectively. Examples of a decoy image, a pass-image, and a synthesized image obtained using this DWT are shown in Fig.6.

V. Low Fidelity Test

A. *Visibility of pass-image*

Fig. 7 shows examples of synthesized images of various levels of DWT on a decoy image. As shown in Fig.7 (a), legitimate users, who can see the image near the display, can recognize the pass-image regardless of sharpness of the decoy image, although the pass-image is less visible on the edge of the decoy image, such as the stem of the flower on the bird's face. On the contrary, for shoulder-surfers who are far from the display, the pass-image is less visible and the decoy image disturbs to notice the pass-image if it is sharp. However, if the decoy image is too blurry, only the pass-image remains in the image and it becomes noticeable for everyone.



(a) LL1 (b) LL2 (c) LL3

(d) LL4 (e) LL5 (f) LL6

Fig. 7 Relationship between DWT level of decoy image and visibility of pass-image.

We conducted a low fidelity test to evaluate the relationship between DWT level of decoy image and visibility of pass-image. We used 100 images of objects, scenery, and animals to make 50 pairs of images. We prepared 6 images in different DWT levels for synthesized images which consist of each pair. The size of the synthesized images is 256 by 256 pixels. In the test, one of the synthesized images is shown to participants on a 17-inch SXGA LCD monitor while the decoy image becomes gradually less clear. Participants asked to answer, as legitimate users, whether s/he can see the high frequency signal of the pass-image. All participants are 20s male students. Distance between a participant and a computer screen is 30 cm. After that, participants seated 50 cm behind the legitimate user and asked to answer same question as attackers. In addition, the monitor screen is recorded using a video camera from the attacker's position.

Table 1 shows the results of the test. These results indicate that legitimate users recognize most pass-images around level 1 or level 2, although there is a large difference among individuals. While clear decoy images make it difficult for attackers to recognize pass-images. Attackers notice some noise exist in the images around level 4, but it was difficult to know its content. This method is not strong enough against recording with a video camera, although pass-images are less visible.

We also need to consider that content of the image affects the visibility. A combination of a decoy image which has many edge contours and a pass-image which has thin and low-contrast edges was difficult to recognize the pass-image even though they are legitimate users. Fig.8 shows an example of a synthesized image which was a difficult combination of images to recognize pass-image.

TABLE I
Number of images each user could recognize pass-image.

DWT level	user				attacker				video camera
	1	2	3	4	1	2	3	4	
Level 1	30	30	12	25	1	0	1	1	10
Level 2	34	36	20	31	2	2	1	1	18
Level 3	40	45	27	38	4	7	4	3	34
Level 4	42	50	39	40	7	21	9	3	43
Level 5	47	50	46	45	10	30	15	6	47
Level 6	50	50	49	49	19	38	29	19	48
invisible	0	0	1	1	31	12	21	31	2

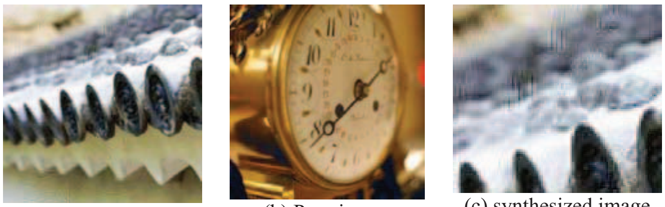

(a) Decoy image (b) Pass-image (c) synthesized image (enlarged)

Fig. 8 An example of combination difficult to recognize pass-image.

B. *Memorability of pass-image*

We also evaluated memorability of pass-images overwritten on the synthesized images. Before the user test, 5 pass-images are given to a user and he memorizes these images for 10 minutes. During the user test, a set of 4 synthesized images, that are generated using 2-level DWT, is shown to the user at one challenge. One or no pass-images are included in the set and the user is asked to specify the location of the pass-image. One authentication trial consists of 7 challenges. We carried out this test 5 times. Therefore, we obtained 35 answers from each participant. We did not add a limitation on the number of decoy image appearances. Therefore, the same decoy image could appear several times. Participants of this test are same as those from the prior low fidelity test.

Table 2 shows the correct answer ratios for this test. This result shows that participants could recognize pass-images correctly.

TABLE II
Number of correct answers and its ratio.

	user1	user2	user3	user4
# of correct answers	35	35	34	35
Ratio	100%	100%	97%	100%

VI. CONCLUSIONS

We proposed a graphical password authentication concept using the property that it is difficult to recognize subtle high frequency components with human eyes. Our method is difficult for observers who stand behind a user to know the pass-image, while it is easy for a user who is just in front of the computer screen. We also discussed an image synthesis method for this graphical password concept. This paper presented the idea and results of preliminary experiments. Further detailed user study is required to evaluate authentication time, authentication success ratio, and memorability of pass-images in the synthesized images from the viewpoint of observers. We also need to consider the effect of age on visibility of high frequency components.

In our future work, we will evaluate the memorability in longer term and compare it with other graphical password methods.

REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.

[2] Xiaoyuan Suo, Ying Zhu and G. Scott Owen, "Graphical Passwords: A Survey," *21th Annual Computer Security Application Conference* (ACSAC2005), pp.463-472, December 2005.

[3] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII 2005)*, Las Vegas, NV, 2005.

[5] R. Dhamija and A. Perrig, "Déjà vu: A user study, using images for authentication," *Proc. 9th USENIX Security Symposium*, August 2000.

[6] Atsushi Harada, Takao Isarida, Masakatsu Nishigaki, "A proposal of user authentication using mosaic images," Proc. of Computer Security Symposium, pp.385-390, October 2004. (in Japanese)

[7] Eiji Hayashi, Nicolas Christin, Rachna Dhamija, Adrian Perrig, "Use Your Illusion: Secure Authentication Usable Anywhere," Proc. of the 4th symposium on usable privacy and security (SOUPS08), pp.35-45, 2008.

[8] David Taubman, Michael Marcellin, "JPEG2000: Image Compression Fundamentals, Standards and Practice," Springer, 2001.

[9] JPEG 2000, http://www.jpeg.org/jpeg2000/index.html