28th Picture Coding Symposium, PCS2010, December 8-10, 2010, Nagoya, Japan

A STUDY ON MEMORABILITY AND SHOULDER-SURFING ROBUSTNESS OF GRAPHICAL PASSWORD USING DWT-BASED IMAGE BLENDING

Takao Miyachi[*1], *Keita Takahashi*[*2], *Madoka Hasegawa*[*1], *Yuichi Tanaka*[*1], *Shigeo Kato*[*1]

[*1]Graduate School of Engineering, Utsunomiya University,[*2] Faculty of Engineering, Utsunomiya University
7-1-2 Yoto, Utsunomiya, Tochigi 321-8585 Japan
E-mail: {miyachi@mclaren., takahashi@mclaren., madoka@, tanaka@, kato@}is.utsunomiya-u.ac.jp

ABSTRACT

Graphical passwords are an authentication method that uses pictures as passwords instead of using alphanumeric characters. We propose a graphical password method which is difficult to steal original pass-image by using characteristics of human vision system. In our method, we combine low frequency components of a decoy picture with high frequency components of a pass-image. It is easy for legitimate users to recognize the pass-image in the blended image. On the other hand, this task is difficult for attackers.

We used discrete wavelet transform (DWT) to blend a decoy image and a pass-image. User studies are conducted to evaluate memorability and shoulder-surfing robustness of this method. We also compared our method with other existing methods in terms of the authentication time and the success ratio by the user test. The results show that our method is more usable and secure against shoulder-surfing.

Index Terms— *Graphical password, discrete wavelet transform, authentication, usable security*

1. INTRODUCTION

Entering a user name and a textual password is a major method for the computer login procedure. Unfortunately, this method is vulnerable to spyware and key-loggers. 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].

To address this issue, several authentication methods have been proposed. In this paper, we focus on graphical passwords [2] which use pictures as passwords instead of using alphanumeric characters. Pictures are difficult to steal with key-loggers. In addition, remembering pictures are easier for human than 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 [3], [4]. These proposed approaches utilize the property that degraded images look like noise or ink blots and they are difficult for observers 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, a trade-off exists between the security level and the memorability of pass-images. As a result, the system becomes less usable.

In the preliminary study [5], [6], we presented a concept of an image synthesis method for a user authentication system using graphical passwords. In this method, we combine low frequency components of a decoy picture with high frequency components of a pass-image by using DWT. 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. However, former user study was conducted in a short term and memorability of the graphical password in longer term was an open question. In this paper, we evaluate longer term memorability and shoulder-surfing robustness of our graphical password.

2. OVERVIEW OF PROPOSED SYSTEM

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. 1 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. One image in the set consists of low frequency components of a decoy image and high frequency components of a pass-image. The other three images are blended images which consist of low frequency components of decoy images and high frequency

978-1-4244-7133-1/10/$26.00 ©2010 IEEE

components of other decoy images. The user is asked to choose the image in which his/her pass-image is vaguely blended in the image. If s/he does not find any of his pass-images in the set, s/he is supposed to choose "No pass-image" as his/her answer. This challenge is repeated several times and if all the answers are correct, s/he will be successfully authenticated. The number of challenges and registered pass-images depend 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 properly remember more pass-images and takes more time for the authentication.

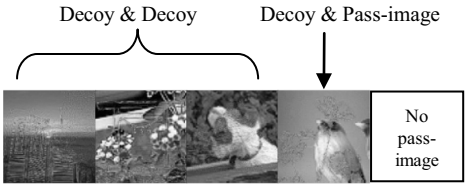


Fig. 1 Example of images displayed for a challenge.

3. IMAGE BLENDING METHOD FOR GRAPHICAL PASSWORD

How to generate the blended image is the key in this authentication system. Fig. 2 shows the flow of our image synthesis method. We used a discrete wavelet transform (DWT) to extract low and high frequency components from images because DWT requires less computation than DCT to split the frequency components of two input images and to blend those frequency components for generating a blended image.

First, DWT is applied to each color plane in a decoy image and a pass-image. The LL*x* band, that is the lowest frequency band of *x*-level DWT, contains the average information of the input image. In contrast, the LH1, HL1, and HH1 bands contain mostly the edges of the images. Names of each sub-band in 2-level DWT are shown in Fig. 3.

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 zeros 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 even for the legitimate user to recognize the pass-image. We obtain a blended image for our authentication method after the inverse DWT (IDWT) and merging of color planes.

An advantage of this method is storage space reduction for the pass-image. Only the high frequency components, that are LH1, HL1, and HH1 bands, are required to be stored in the system. For the authentication, the system randomly chooses a decoy image and mixes it with the pass-image to generate a blended image.

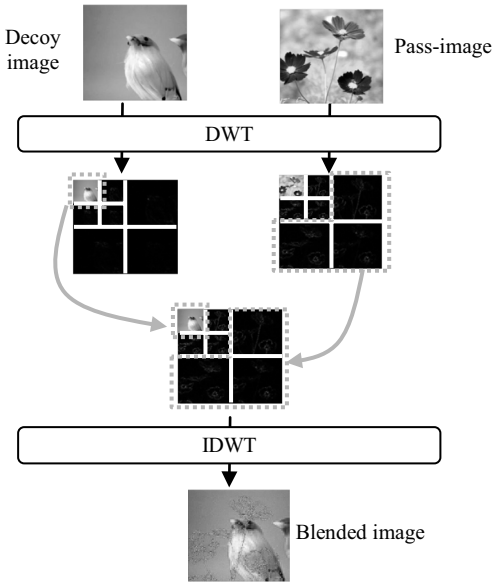


Fig. 2 Overview of the image blending procedure.

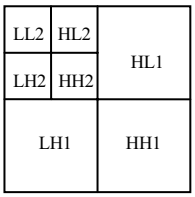


Fig. 3 Names of each sub-band in 2-level DWT.

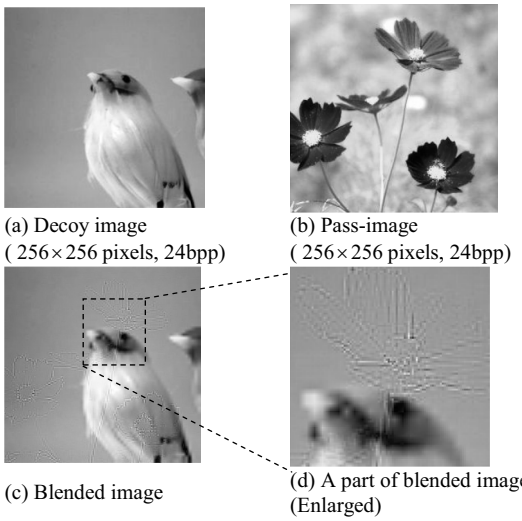


Fig. 4 Example of the blended image.

In this study, we used 5/3-DWT filter which is a reversible DWT used in JPEG 2000 [7]. Low frequency signals and high frequency signals are given by following equations.

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

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

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 blended image obtained using this DWT are shown in Fig. 4.

4. LOW FIDELITY TEST OF PASS-IMAGE MEMORABILITY

We evaluated memorability of pass-images overwritten on the blended 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 blended images, that are generated using 2-level DWT, is shown to the user at one challenge. One or no pass-image is 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 lo-fi test are 4 male students and all of them are 20s.

Table 1 shows the correct answer ratios for this test. This result shows that most of the participants could recognize pass-images correctly.

Table 1 Number of correct answers and its ratio

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

5. USER TEST AND COMPARISON

5.1. Memorability

We compared our method with the existing graphical password methods proposed by Harada et al. [3] in terms of the authentication time and the success ratio. Fig. 5 shows examples of images generated by our method and Harada's methods. The 2-level DWT was used for the proposed method. The mosaicing block sizes for the Harada's methods were 4 by 4 pixels. The alpha-blending ratio was pass-image : decoy = 6 : 4 for the Harada's method 2.

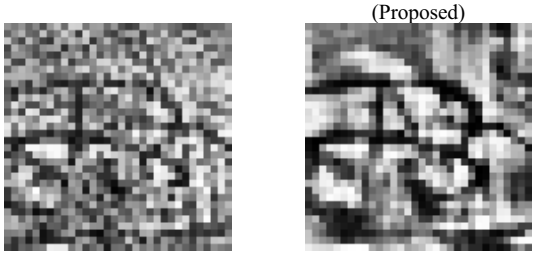
Prototypes of the graphical password system was implemented as an web application using Apache and PHP. An authentiocation process consists of seven challenges and four blended images and an icon of "no pass image" are displayed for each challenge. In this test, each participant played a role of a legitimate user. They memorized 5 pass-images, which were imposed by the system, and answered their location using the mouse pointer.

There were 40 participants and we divided them into four groups to evaluate the effect of test intervals. The number of participants and intervals of user tests for each group are shown in Table2. On the day "0", participants practiced the authentication procedure several times until they became familiar with the usage of the system. Then, they started the user test of the authentication for each method. The participants in group A carried out the authentication test without the practice 1day later, 1 week later, 2 weeks later, 3 weeks later, and 1 month later. The intervals of the authentication test were longer for other groups.

Table 2 Number of participants and intervals of user tests

Group	#	Intervals
A	10	0day, 1day later, 1week later, 2weeks later, 3weeks later, 1month later
B	10	0day, 1week later, 2weeks later, 3weeks later, 1month later
C	10	0day, 2weeks later, 1month later
D	10	0day, 1month later
Total	40	

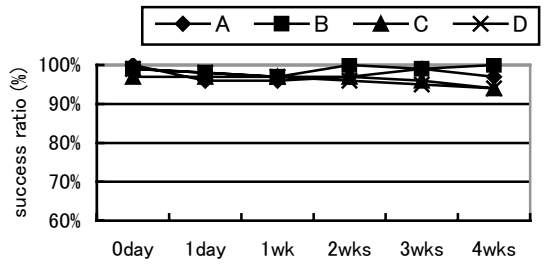
(a) Original pass-image (b) Blended image (Proposed)



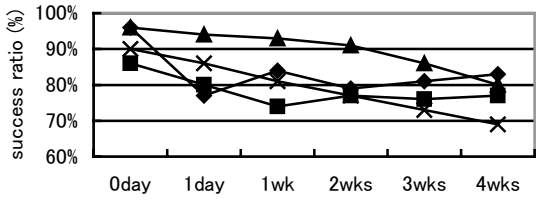
(c) Harada's method 1 (Mosaicing, and adding random noize) (d) Harada's method 2 (pass-image: decoy = 6:4) (Alpha blending , mosaicing, and adding random noize)

Fig. 5 Comparison with Harada's methods.

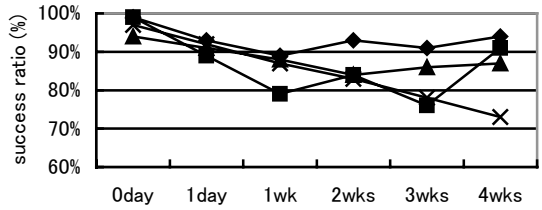
Fig. 6 shows the effect of test interval for success ratio. Fig. 6(a) is the result of the proposed method, Fig. 6(b) is the result of the Harada's method 1, and Fig. 6(c) is the result of the Harada's method 2. Fig. 6(a) shows that participants could choose almost correct pass-images irrelevant to the test intervals in our method. On the contrary, the success ratio decreases as the interval becomes longer in the Harada's methods. This is due to the memorability of the pass-images.



(a) Proposed method



(b) Harada's method 1



(c) Harada's method 2

Fig.6 Effect of test interval for success ratio.

5.2. Robustness against Shoulder-surfing

We also compared our method with the graphical password using original clear image and the Harada's method 2 in terms of robustness against shoulder-surfing.

There were 6 participants and they played a role of an attacker. First, they complete a short training session on how each graphical password system is used. Next, the participants try to gain pass-images through shoulder-surfing while the experimenter carried out the authentication correctly. The experimenter chose a pass-image out of 5 images every 5 seconds. This challenge is repeated 7 times. The participants stood about 50cm behind the experimenter. Each participant was permitted taking notes during the shoulder-surfing. After the shoulder-surfing session, the participants were asked to carry out the authentication as attackers using same pass-images. They could use their notes if they wanted.

Table 3 shows the false acceptance rate (that is, attack success ratio). This result shows that proposed method is secure against the shoulder-surfing. Participants indicated that they could not recognize high frequency components of a pass-image because they are far from the screen.

Table 3. Success ratio of shoulder-surfing

	Original image (w/o image blending)	w/ image blending	
		Harada's 2	Proposed
FAR	95%	69%	7%

6. CONCLUSIONS

We proposed a graphical password 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 blending method for this graphical password system. We conducted a lo-fi tests and a user test. The lo-fi tests revealed the feasibility of this system and suitable parameters for the image blending. The results of the user test showed participants could complete the authentication faster than existing methods while the authentication success ratio was higher than them. In addition, the user test of shoulder-surfing shows our method prevents attackers from stealing pass-images.

We will study the details of the relationship between the visibility of the pass-image and the complexities of the image content in the future work. Hybrid images [8], which blends two images of similar structure but slightly different, are good candidates to compare with our method in terms of image content and visibility of pass-image because our method blends two images of completely different structure.

In addition, the further user study with more participants is required to evaluate robustness of pass-images from the viewpoint of more powerful attackers, i.e. video cameras. We also need to consider the effect of age on visibility of high frequency components.

ACKNOWLEDGMENTS

This work was supported in part by KAKENHI 22500105.

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

[3] A. Harada, T. Isarida, M. Nishigaki, "A proposal of user authentication using mosaic images," Proc. of computer security symposium, pp.385-390, 2004. (in Japanese)

[4] E. Hayashi, N. Christin, R. Dhamija, A. Perrig, "Use Your Illusion: Secure Authentication Usable Anywhere," Proc. of SOUPS08, pp.35-45, 2008.

[5] M. Hasegawa, Y. Tanaka, S. Kato, "A Study on an Image Synthesis Method for Graphical Passwords," Proc. of ISPACS, WP2-D-2, Dec. 2009.

[6] M. Hasegawa, T. Miyachi, Y. Tanaka, S. Kato, "A graphical password using discrete wavelet transform and its evaluation," IEVC 2010, 1P-5, Mar. 2010.

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

[8] A. Oliva, A. Torralba, P.G. Schyns, "Hybrid images", ACM Trans. on Graphics, Vol.25, No.3, pp.527-530, 2006.