2009 International Conference on Advanced Information Networking and Applications

Advantages of User Authentication Using Unclear Images

－Automatic Generation of Decoy Images－

Takumi Yamamoto[1,4], Atsushi Harada[2], Takeo Isarida[3], Masakatsu Nishigaki[1,5]
[1]Graduate School of Science and Technology Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, JAPAN
[2]Mitsubishi Electric Corporation 5-1-1 Ofuna Kamakura, JAPAN
[3]Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, JAPAN
[4]Research Fellow of the Japan Society for the Promotion of Science (DC1)
[5]Japan Science Technology and Agency， CREST
E-mail: f5745037@ipc.shizuoka.ac.jp, Harada.Atsushi@dw.MitsubishiElectric.co.jp,
isarida@inf.shizuoka.ac.jp, nisigaki@inf.shizuoka.ac.jp

***Abstract*— A user authentication system using "unclear images" as pass-images has been proposed, in which only legitimate users can understand their meaning by viewing the original images corresponding to these unclear pass-images, which are meaningless to unauthorized users. Hence, it is difficult for attackers to memorize them, even though they may have observed authentication trials by legitimate users. This paper reports another advantage of the user-authentication system using unclear images: their adaptation enables decoy images to be automatically generated, which are displayed along with the pass-images in the authentication window. Here, we explore various methods of automatically generating decoy images.**

image-based user-authentication; observing attackers; schema; unclear-image; decoy image (key words)

I. INTRODUCTION

Although password-based systems are now widely used in all kinds of authentication, they have various shortcomings in neglecting human limitations. Most users of password-based systems prefer to use simple passwords or hesitate to change them frequently since it is not easy to memorize strong passwords such as long random strings. Further misgivings about the shortcomings of password-based systems have already been discussed [1, 2].

To cope with these shortcomings, image-based user-authentication systems using "pass-images" instead of passwords have been studied to reduce the burden of having to memorize passwords. Authentication based on the recognition of pass-images [2-4] is especially effective since people are much more efficient at recognizing previously seen images than accurately recalling passwords. However, there is another problem with such systems, where these pass-images need to be presented on their displays at each authentication trial. Consequently, these systems are vulnerable to being observed by attackers (shoulder surfing). Observing attackers can be a serious problem for image-based authentication systems since the use of images makes it easier not only for legitimate users to memorize their pass-images, but also for attackers to peep at and memorize these.

Moreover, attention needs to be paid to unauthorized acts by legitimate users; a legitimate user could intentionally divulge his/her own authentication information to others (e.g., for illegally sharing content). Pass-images are still easy to share since users can tell others their meanings even if "random-art" images (abstract images consisting of some geometric patterns produced by random computation [5]) are used.

To solve these problems, a user-authentication system using "unclear images" as pass-images has been proposed, in which only legitimate users can understand what they mean by viewing the original images corresponding to the unclear pass-images [6]. As these unclear images are meaningless to unauthorized users, it is difficult for them to memorize these, even though they have observed legitimate users' authentication trials. In addition, it is not easy even for legitimate users to divulge their unclear pass-images accurately to anyone in words via e-mails or telephone.

In addition to pass-images, decoy images are also an essential factor in image-based authentication systems. Although decoy images are necessary for hiding the pass-images displayed in the authentication window, their use also poses some problems regarding preparation, which have yet to be solved. Therefore, we report another advantage of the user-authentication system using unclear images: the adaptation of unclear images enables decoy images to be automatically generated, which are displayed along with pass-images in the authentication window. Here, we explore various methods of automatically generating decoy images. This paper refers to the previous system (authentication system using unclear image [6]) as the "basic system". The next section reviews our basic system. We then discuss the problems encountered in preparing decoy images in Section III. Our algorithm for automatically generating decoy images is described in Section IV. Finally, we discuss our future work and draw conclusions in Section V.

II. BASIC SYSTEM: AUTHENTICATION SYSTEM USING UNCLEAR IMAGES

A. Concept underlying basic system

This section provides a brief overview of the basic system [6]. To solve the problems with conventional image-based authentication systems (user authentication systems using original images), a user authentication system using

1550-445X/09 $25.00 © 2009 IEEE
DOI 10.1109/AINA.2009.22

"unclear images" as pass-images has been proposed. An unclear image is produced from an original meaningful image by image processing such as grayscaling, mosaicing, and noise added to the spatial frequency domain. The left image in Fig. 1 has an example of the original image. The right image in the same figure has been obtained by image processing. Although the unclear image has lost a considerable amount of color and resolution, it still holds a certain degree of information about the original image.

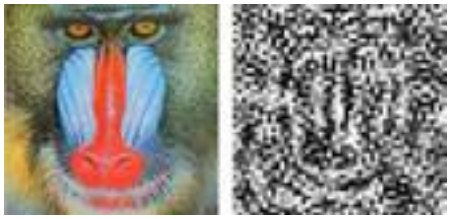

Figure 1. Original image and corresponding unclear image.

An unclear image still retains some meaning from the original image, but it looks meaningless to users who have never seen the original image. Even for legitimate users find it hard to memorize meaningless images. That is why we expected it to be difficult for unauthorized users to memorize legitimate user's unclear pass-images, even if they were allowed to freely observe their authentication trials.

Only legitimate users were allowed to see the original images corresponding to their unclear pass-images in the registration phase. By seeing the original images, the legitimate users could recognize the meaning of the unclear pass-images and could easily memorize them by using the original images as cues. In other words, the basic scheme only gave legitimate users underlying knowledge of their unclear pass-images by having seen the original corresponding images. This kind of knowledge is called a "schema" in cognitive psychology [7]. A schema means a structure for knowledge that is unconsciously organized in the human mind when we memorize any incoming information. Once a legitimate user has formed the schema for his/her unclear pass-images that is associated with the original corresponding images, he/she can easily recognize the meaning of the unclear pass-images. Therefore, as legitimate users can memorize unclear images as being meaningful, the burden imposed by their having to memorize unclear pass-images is limited.

Users cannot usually learn an appropriate schema without seeing the original corresponding image. Therefore, it would also be difficult for anyone who did not understand the schema to interpret an unclear pass-image even if a legitimate user intentionally divulged his/her unclear pass-image accurately to someone in words via e-mails or telephone.

B. *Authentication procedure*

1) *Registration phase:* The registration phase involves four steps.

   a) The system shows a certain numbers of original images to the legitimate user.

   b) The user chooses one original image that he/she would like to use as the source for his/her pass-image.

   c) The system produces an unclear image from the original image chosen by the user.

   d) The user memorizes the unclear image as his/her pass-image. Note that since the user has seen the original image in Step 1, he/she can easily memorize the unclear image.

2) *Authentication phase: The authentication phase is involves three steps.*

   a) The system presents the legitimate user's unclear pass-image along with some randomly chosen unclear decoy images. (The decoy images could be different in all authentication trials.)

   b) He/she should recognize his/her unclear pass-image from the images.

   c) If he/she can identify the correct pass-image, he/she is authenticated.

The number of pass-images, the number of decoy images, and the number of repetitions (rounds) of authentication phases are determined according to the required security level. Note that this authentication procedure scarcely differs from the procedure employed by conventional image-based authentication systems [2-4] except for the use of unclear images. There is an example of an authentication window with nine-alternative unclear images in Fig. 2.

Figure 2. Authentication system with nine-alternative unclear images.

III. AUTOMATIC GENERATION OF DECOY IMAGES

A. Shortcomings with conventional image-based authentication schemes

In addition to pass images, decoy images are also an essential factor for an image-based authentication system. Although decoy images are necessary for hiding the pass-images displayed in the authentication window, their use also poses some problems that have yet to be solved.

For example, in a situation where the same set of decoy images is used for each authentication trial, an attacker can employ a strategy known as an "exhaustive attack". This attack can be explained as follows: if the attacker fails in an authentication trial after selecting one of the images from the set of image choices, he/she now knows that this particular image is not the correct answer. Consequently, he/she can continue to repeat this process, eventually finding the correct answer through a simple process of elimination.

Confusion about images is another potential problem. In recognition-based authentication, a user has to select a previously seen image (i.e., the correct memorized pass-image) from the set of images choices (which includes decoy images). The user can be confused by trying to recognize the correct pass-image if the authentication system exploits used images (already used in previous authentication trials) as decoy images, or if it uses images familiar to the legitimate user (e.g., photos taken by the user) as decoys. To reduce this possibility of confusion, it is preferable to use unfamiliar images as decoys.

One solution to both these problems is for all decoy images to be renewed at every authentication trial. In other words, only use decoy images once and never show them again after they appear at a single authentication trial. Unfortunately, this solution is not ideal. If the same pass-image is used at every authentication window, an attacker can employ a so-called "intersection attack". As the name implies, the attacker in this technique finds the pass-image easily by comparing the image choice sets in two authentication windows, and he/she only needs to find the image common to both to obtain the correct pass-image.

One possible way of reducing vulnerability to such attacks would be to repeat a random number of decoy images used in previous authentication trials at each new authentication trial, while renewing the rest of the decoy images in the choice set. However, there is still the problem of how to obtain entirely new images for each new authentication trial. Although this problem may be avoided by storing a sufficient number of decoy images in advance, or by downloading decoy images automatically, it is difficult to use such measures in mobile terminals, which have severe constraints on storage and incur (packet) communication fees.

As we previously described, preparing and updating decoy images are problematic in conventional image-based authentication systems, and to our knowledge, no effective solution has been found so far. Our research has focused on finding ways of avoiding these problems, and as we described in our previous paper [6], we believe that the use of "unclear images" employed in a basic system is a promising technique. This paper describes and proposes a novel scheme of generating decoys through this use of unclear images, i.e., a technique that can avoid many of the problems experienced by other conventional image-based authentication systems.

Figure 3. Example image

B. Automatic scheme for generating decoy images

First, let us look at Fig. 3. What does this unclear image mean? We have already seen the original (source) image it corresponds to in this paper. Fig. 3 was created by rotating the right image in Fig. 1 clockwise. Although we have already seen the corresponding source image (Fig. 1), it is still difficult to guess the meaning of Fig. 3. However, as shown in Fig. 4, after the same clockwise turn is given to the left image in Fig. 1, we can see the similarities (e.g., what the image is and what shape the object in the image has) between Fig. 1 and Fig. 4 in one glance. Thus, we can say that if genuine unclear image is altered (i.e., such as by turning it), it is not easy even for legitimate users to determine whether the image has been seen before or not. By taking advantage of this disorientating characteristic, an unclear image that has had its orientation altered can be used as a decoy image. Here, it should be noted that this technique can only be used with an unclear image – not with an original (photorealistic) image that can readily be recognized, regardless of orientation (as in Fig. 4). From this, we can understand that it is possible to generate decoy images in the authentication phase from images familiar to legitimate users (as with pass-images) without causing any cognitive confusion with the correct pass-image. In addition, we know that the clockwise turn is not only the way to get decoy images. Various decoy images can easily be generated by combining various image-processing schemes. Therefore, we expect that the problems with the preparation of decoys in conventional image-based authentication systems can be solved by using unclear images. This paper explains how the basic system can be enhanced by employing various methods of generating decoy images. After this, we will refer to this system with the decoy image generation methods as the "enhanced system".

Figure 4. Original image corresponding to that in Fig. 3.

C. *Procedure for generating decoy images*

Obviously, the best decoy images will be ones that are most effective at preventing invalid users (e.g., attackers and crackers) from being able to distinguish the pass-image from the decoys. After this, we will refer to the decoys generated by our method as "altered unclear images" (AUIs), and to the original images merely rendered unclear (e.g., through mosaicing) as "genuine unclear images" (GUIs). To create confusion effectively, AUIs must appear as GUIs to invalid users. In other words, the scheme for generating AUIs has to produce decoy images that look like the genuine unprocessed unclear image (i.e., the pass-image).

In this paper, we used quadrupedal mammals as the photographic subjects for our image-generation method. We made the following assumptions:

- Images usually have the following structures:
  - *a)* If all body part appear in the photos, the legs are likely to appear in the lower half of the image, the head in the upper half, and the torso in the center.
  - *b)* If the photo is of an animal's face, its eyes are likely to appear in the upper half, and its mouth in the lower half.
- People tend to recognize unclear images that retain these two structures a) and b) as genuine unprocessed images.

Therefore, we assumed that if the processed image would retain these structures intact, we can recognize it as an "image that retained the appearance of a genuine unprocessed unclear image (GUI)". The image in Fig. 4, for instance, would be unsuitable for processing a decoy image because it does not comply with these assumptions since its 90° clockwise rotation has altered its structure. In the sections that follow, we will introduce three methods of generating decoy images in which generated images are effectively given the appearance of GUIs.

1) Method 1: The first method uses two images to create one decoy image and involves three steps.

a) Image X is created by connecting the upper half of original image A and the lower half of original image B as shown in Fig. 5.

b) Then, to remove the discontinuity in the boundary of X, gradation processing is done on X and image Y is obtained.

c) AUI is obtained by rendering Y unclear (e.g., by mosaicing).

There is an example of AUI using Method 1 in Fig. 6.

Figure 5. Overview of Method 1

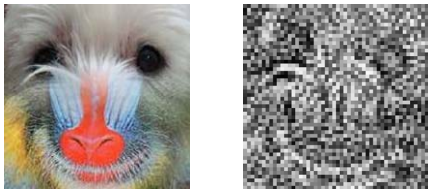

Figure 6. Example unclear image and corresponding original image produced with Method 1

2) Method 2: The second method also uses two images to create one decoy image and involves three steps.

a) Image X is created by rotating the original image A. There are three angles for rotating original image A clockwise, i.e., 90°, 180°, and 270°.

b) Then, Y is created by overlapping X and original image B as shown in Fig. 7.

c) AUI is obtained by rendering Y unclear (e.g., by mosaicing).

There is an example of AUI using Method 2 in Fig. 6. Although only rotating eliminates the structure of AUI, the structure of AUI can be retained by overlapping the original image B with the rotated image X.

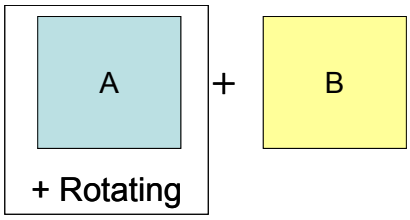

Figure 7. Overview of Method 2

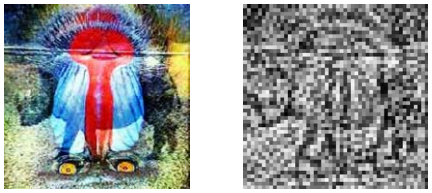

Figure 8. Example unclear image produced with Method 2

3) Method 3: The third method combines Methods 1 and 2 as shown in Fig. 9 and involves three steps.

a) X is obtained with Method 1 with original images A and B, and likewise, Y is obtained by using Method 1 with original images C and D.

b) Z is created by using Method 2 with X and Y, i.e., Z is obtained by overlapping Y and rotated X.

c) AUI is obtained by rendering Z unclear (e.g., by mosaicing).

There is an example of AUI using Method 3 in Fig. 10. The original images used in the examples in Figs. 6, 8, and 10 are shown in Fig. 11.

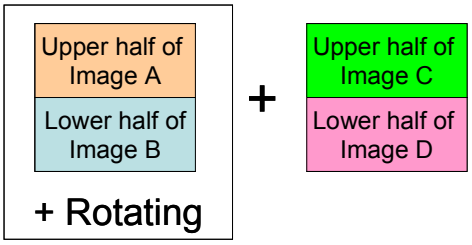

Figure 9. Processing scheme 3

Figure 10. Example unclear image produced with Method 3

Figure 11. Original images used in examples in Figs. 6, 8, and 10.

IV. Evaluation Experiments

We carried out two experiments to evaluate the effectiveness of the enhanced system. In both experiments, decoy images were created by using Methods 1–3 described in Section III.C. The subjects in the experiments were 10 volunteers who were college students.

A. Differentiation experiment (distinguishing GUI from AUI)

As described in Section III.B, AUIs must appear as GUIs to invalid users. To check this, we carried out an experiment to confirm whether the proposed AUIs (images generated by the Methods 1–3) looked like GUIs (genuine unprocessed unclear images).

1) Experimental procedure: A two-alternative system[1] was used in this experiment. One GUI was presented along with an AUI, and the subject was required to identify the GUI with a mouse click. The experiment was conducted for all three AUI generating methods (Methods 1–3). First, an experiment using Method 1 was done using the following procedures:

a) The experimenter told the subject that the AUIs were produced with Method 1.

b) The system prepared five original images org(i) (i=1~5).

c) Five genuine unclear images gui(i) (i=1~5) were obtained by rendering all org(i) (i=1~5) unclear (e.g., by mosaicing).

d) For each org(i), all possible altered unclear images all_aui(i, method 1) were created with Method 1 using org(j) (j ≠ i). For instance, all_aui(4, method 1) were all possible altered unclear images created with Method 1 using org(1), org(2), org(3) and org(5). That is, all_aui(4, method 1) consisted of m1(1,2), m1(1,3), m1(1,5), m1(2,1), m1(2,3), m1(2,5), m1(3,1), m1(3,2), m1(3,5), m1(5,1), m1(5,2), and m1(5,3), where m1(A,B) stands for an altered unclear image created with Method 1 with the upper half of original image A and the lower half of original image B.

e) k was selected from 1–5 randomly. For each gui(k), an image was selected randomly from all_aui(k, method 1). The selected image was expressed as aui(k, method 1).

f) aui(k, method 1) was presented along with gui(k) on the display. It should be noted that the altered unclear image aui(k, method 1) was generated from gui(j) (j ≠ k) other than gui(k) that was shown as the genuine unclear image in the current display.

g) The subject was required to identify the GUI with a mouse click.

h) While changing k, Steps (e) to (g) were repeated five times. The system never chose any k that had already been chosen previously. In other words,

[1] This paper refers to a system in which one pass-image is displayed along with k decoy images as "(k+1)-alternative authentication".

Steps (e) to (g) were repeated until all gui(k) (k=1~5) were exhausted.

i) The system updated five original images org(i) (i=1~5), and Steps (c) to (h) were repeated. The repetition was iterated four times. That is, each of the ten subjects was required to make twenty two-alternative selections. Thus, all 10 subjects made a total of 200 two-alternative selections.

The experiments for Methods 2 and 3 were then conducted using equivalent procedures.

2) Experimental results: Table I lists the results for the experiments using Methods 1–3.

TABLE I. EXPERIMENTAL RESULTS OF DISCRIMINATION.

	Method 1	***Method 2***	***Method 3***
Success rate	117/200 (58.5%)	121/200 (60.5%)	115/200 (57.5%)

About 60% of images were successfully selected by all subjects. We evaluated these three results with a t-test. The null-hypothesis in our test was that successful selection was 50% (this meant that a subject randomly selected one of two images). The p-value for the results of all three methods (Methods 1−3) corresponded to p=0.0634, p=0.0109, and p=0.0119. The results for Methods 2 and 3 yielded statistically significant differences (p-values of below 0.05). However, considering that the experiments were particularly advantageous to subjects because of the two-alternative system, the results meant that the AUIs created with Methods 1–3 looked sufficiently like GUIs.

B. Authentication by legitimate users

Numerous decoy images can be automatically obtained by altering pass-images using the methods described in Section III.C. In other words, an authentication system only needs to prepare pass-images. To achieve this, our AUIs (images generated with the Methods 1–3) should not cause legitimate users to confuse these with the correct pass-image. Therefore, we carried out an experiment to confirm whether using AUIs as decoy images caused legitimate users any confusion in recognizing pass-images.

1) Experimental procedure: In this experiment, we used four rounds in an authentication system that offered nine alternatives, i.e., one pass-image was presented along with eight decoy images in each authentication round, four rounds were carried out in each authentication trial, and each user memorized four pass-images. When the user could identify all the pass-images correctly in each of the four rounds, he/she was authenticated. The probability that a brute-force attack would be successful was $1/9^4$, which is nearly comparable to the four-digit PIN system ($1/10^4$).

It should be noted that this experimental system was founded on Harada et al.'s basic system (four rounds in a nine-alternative authentication system with four pass-images) discussed in Sec. 4.1 [6]. Actually, the only differences between both systems were the decoy images, which were automatically generated by Methods 1–3. That is, by directly comparing the results of this experiment with those of Harada et al.'s [6], we could evaluate to what extent our AUIs caused legitimate users confusion in recognizing pass-images. The procedure for this experiment involved three steps.

a) Legitimate users were assigned four original images org(i) (i=1~4). Four genuine unclear images produced from each original image gui(i) (i=1~4) were used as pass-images. For each gui(i), all possible altered unclear images all_aui(i, method 1), all_aui(i, method 2) and all_aui(i, method 3) were created using org(j) (j ≠ i) with equivalent procedures to that in Section IV.A.

b) On the following day, all legitimate users were required to attempt authentication (four rounds in nine-alternative authentication):

i) k was selected from 1–4 randomly.

ii) Eight decoy images were selected randomly from a combined set of {all_aui(k, method 1) + all_aui(k, method 2) + all_aui(k, method 3)}. This meant that the decoy images were generated from gui(j) (j ≠ k) other than gui(k), which was displayed as the pass-image in the current round.

iii) The system displayed the eight decoys selected in Step ii) and gui(k) in the same way as in Fig. 2.

iv) Legitimate users were required to identify GUIs with a mouse click.

v) While changing k, Steps i) to iv) were repeated four times. The system never chose any k that had already been chosen during the previous rounds in any authentication trial. In other words, Steps i) to iv) were repeated until all pass-images gui(k) (k=1–4) were exhausted.

The rate of successful authentication and the time taken to find the pass-images from the nine alternatives for each round of authentications were recorded. This was repeated five times with the same set of pass-images. That is, each of ten legitimate users was required to carry out five authentication trials. Thus, all legitimate users underwent a total of 50 authentication trials.

c) Eight days later, all legitimate users were required to re-attempt authentication. The rate of successful authentication and the time taken to find the pass-images for each round of authentications were recorded. This was repeated five times with the same set of pass-images.

Note that the legitimate users were not allowed to review their pass-images once the registration phase (Step 1) was complete, except during the authentication trials on the following day and eight days later.

2) Experimental results: Table II lists the results of the experiments. Harada et al.'s experimental results on their basic system [6] have been provided for comparison.

TABLE II. EXPERIMENTAL RESULTS OF DISCRIMINATION.

	Basic System		*Enhanced System*	
	1 day later	*8 days later*	*1 day later*	*8 days later*
Success rate	50/50 (100%)	49/50 (98%)	46/50 (92%)	47/50 (94%)
Average time [sec]	8.19	7.10	20.60	17.673

There was a slight decline in the rate of successful authentication for the enhanced system compared to the basic one. We also confirmed that the average time to find the pass-images from the decoys in the enhanced system was longer than that in the basic system. This meant that our AUIs caused legitimate users a slight degree of confusion in recognizing pass-images. This confusion may have been caused because the AUIs still held a certain amount of information about the pass-images. To reduce this possibility for cognitive confusion, it might be preferable to devise a way of generating AUIs or create AUIs from not only pass-images but also a very small number of other images that are unfamiliar to legitimate users.

V. CONCLUSIONS AND FUTURE WORK

We reported another advantage of the user-authentication system using unclear images: the adaptation of unclear images enables decoy images to be automatically generated. Although, our proposed AUIs were still insufficient, we believe these results represent a huge step toward making image-based authentication systems feasible. To further reduce the cognitive confusion caused by AUIs, it would be more effective to use information about pass-images with words [8]. We expected that when a brief explanation of unclear pass-images is given in words, only legitimate users can use the explanation as a cue to recognizing his/her pass-images, while no illegal users will be able to understand the cue as was confirmed in the previous studies [6][8]. In our system, decoy images displayed in an authentication window are not generated from pass-images that are displayed in the current window. Therefore, our system should be successful with verbal cues [8].

ACKNOWLEDGMENT

This work was supported by Grant-in-Aid for JSPS Fellows (No.20-6290) and Secom Science and Technology Foundation, Japan.

REFERENCES

[1] A. Perrig, and D. Song, "Hash Visualization: a New Technique to Improve Real-World Security", International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC), 1999.

[2] R. Dhamija, and A. Perrig, "Deja Vu: A User Study Using Images for Authentication", 9th USENIX Security Symposium, pp. 45-58, 2002.

[3] T. Takata and H. Koike, "Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images", LNCS 2795, Human-Computer Interaction with Mobile Devices and Services, pp. 347--351, Springer, 2003.

[4] Real User Corporation, "PassFaces", http://www.realuser.com/ (Feb. 2007).

[5] A. Bauer, "Gallery of random art", http://www.cs.cmu.edu/~andrej/art/, (Jul. 2005)

[6] A. Harada, T. Isarida, T. Mizuno, and M. Nishigaki, "A User Authentication System Using Schema of Visual Memory", Biologically Inspired Approaches to Advanced Information Technology, LNCS 3853, pp. 338--345, Springer, 2006.

[7] W. F. Brewer, "Schemata", In R. A. Wilson & F. C. Keil (Eds.), MIT Encyclopedia of the Cognitive Sciences (Bradford Books), pp.729-730, MIT Press, 1999.

[8] T. Yamamoto, A. Harada, T. Isarida, and M. Nishigaki, "Improvement of User Authentication Using Schema of Visual Memory: Guidance by Verbal Cue", 2007 International Conference on Security and Management (in 2007 World Congress in Computer Science, Computer Engineering, & Applied Computing), pp. 58--64, 2007.