Awase-E: Recognition-based Image Authentication Scheme Using Users' Personal Photographs

Tetsuji TAKADA
National Institute of Advanced Industrial Science and Technology
Akihabara Dai-biru, 1-18-13 Sotokanda, Chiyoda-ku, Tokyo, 101-0021, JAPAN
zetaka@ computer.org

Takehito ONUKI and Hideki KOIKE
University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, JAPAN
nukky@ vogue.is.uec.ac.jp and koike@ acm.org

Abstract

In this paper, we propose a recognition-based image authentication system, named "Awase-E". There are two unique features in the system. One is to use users' personal photographs as their secret information. The other is that the system introduces a "no answer" case in a verification of an authentication trial. We developed an web-base prototype system and conducted exploratory experiments to determine the memorability of this secret information. As a result of the experiments, we determined that the memorability of the secret information in Awase-E is almost the same as the memorability of a PIN number, even over a long period of time with infrequent use. Moreover, even after users are forced to update their secret information, they can pass the authentication without forgetting the secret information or confusing the old and new secret information. We also present a comparison between Awase-E and PIN authentication regarding both security and usability, and we indicate that the Awase-E has potential to become a reasonable candidate as an alternative to PIN authentication.

1. Introduction

Recognition-based image authentication systems have been proposed as an alternative to text-based password authentication [1-4] because they might improve the memorability issue in knowledge-based authentication. The reason is that humans have good capability for visual memory, and such systems make a user's task easier. The task changes from precisely recalling a password and inputting it into recognizing an image and selecting it. This change makes effective use of the human cognitive ability to recall images: "An image once seen is easy to recall" [1-3].

On the other hand, Personal Identification Number(PIN) authentication is still widely used although its vulnerabilities have been reported repeatedly. One of the reasons why it has not been replaced with a more secure authentication system is that there is no appropriate authentication that has the same level of security and usability as PIN authentication.

We, therefore, propose a recognition-based image authentication scheme, named "Awase-E". The word "awase" refers to the identity of two objects, and in this case, we are using "Awase-E" to refer to the sense of identity a user feels when a photo shown on a screen matches the secret information in the user's brain. In this paper, we propose Awase-E as an alternative to PIN authentication. Our scheme enables users to use their secret personal photographs as their "pass-images". Moreover, we introduce a case of "no pass-image" answer to the scheme for ensuring security without an additional memory burden. We have also developed an web-based prototype system based on the above proposal and conducted exploratory user studies to evaluate how well the subjects remembered their secret images in Awase-E. We discuss whether Awase-E is a reasonable alternative by comparing it with PIN authentication in respect to both usability and security.

In the next section, we explain the details of the Awase-E authentication scheme and prototype system. Section 3 reports on the user evaluation study of the Awase-E concerning memorability. An overall discussion of our scheme is represented in section 4, and we concluded the paper in section 5.

2. Awase-E: User Authentication System using Personal Photographs

2.1. Authentication Scheme

Users must decide on at least one pass-image before using Awase-E. We call users' secret photographs "pass-images" and photos that are not pass-images "decoy images". We assume that users select pass-images from their personal photo collections. There are two reasons: one is that a user already knows these images and it is not necessary to remember them by pre-training. The other reason is that it makes maximum use of the "Déjà Vu" effect because a user saw the scene and took a picture of it. These scenes help users not only to keep pass-images in their

1-4244-0674-9/06/$20.00 ©2006 IEEE.

memory but also to recall them from memory when they look at them.

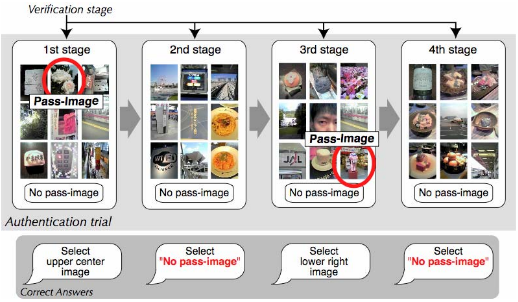


Figure 1. An authentication sequence of Awase-E (N_{image}=4, N_{stage}=9)

Fig.1 illustrates a sample authentication sequence of Awase-E. One authentication trial consists of N_{stage} times of verification stages. Awase-E authorizes a user as a legitimate user if all verification stages are successful. At each verification stage, Awase-E shows N_{image} photographs on the screen, and the image set in each verification stage includes one or zero pass-images. Fig. 1 shows an example of the authentication scheme with N_{stage}=4 and N_{image}=9.

A user has to select the pass-image correctly if the pass-image is included within the verification image set (1st and 3rd stages in fig.1), and the user has to answer as a "no pass-image" if no pass-image is included (2nd and 4th stages in fig.1). The answer "no pass-image" is always presented as one of the possible answers in each verification stage. For security reasons, the scheme does not allow the case in which all verification stages do not include a pass-image. At least one pass-image appears in each authentication trial, and a user has to select a pass-image at least one time during an authentication trial.

Each authentication trial is composed of unique photographs. There are six processes for composing an authentication trial.

1. Awase-E randomly decides how many pass-images are being used in each authentication trial. If a user has four pass-images, there are four cases as the number of pass-images. The minimum number of pass-images is one and the maximum number is limited to either the number of verifi-cation stages or the number of users' pass-images.
2. Awase-E randomly selects actually used pass-images in the trial from a user's pass-image collection.
3. Awase-E randomly selects which verification stage or stages include a pass-image, and which pass-images are actually embedded into each selected verification stage.
4. Awase-E randomly decides the location of the pass-image in each verification stage.
5. Awase-E randomly selects decoy images from an image database.
6. Awase-E randomly decides locations for decoy images.

This means that the location of both pass-images and decoy images is changed at every authentication trial. A location randomness in each verification stage has been widely adopted in this type of authentication system [1,2] and it was called a "challenge and response" feature in this type of system. However, the answer images were always same in such systems. On the other hand, we could say that the Awase-E has a more strict challenge and response feature because Awase-E randomly decides the number of pass-images and selects actually used pass-images in each trial. We consider that processes 1 and 2 in the above list are a unique random factor in this type of authentication. A user, therefore, can not assume either the number of pass-images or which pass-images are used in each trial. Moreover, this challenge and response feature does not need any special device for generating a response like a token-device or a matrix code. This is an advantage because the challenge and response feature is naturally embedded into the scheme, and users can simply regard this scheme as a knowledge-based authentication.

2.2. Prototype System

We developed an web-based prototype system, implemented as a collection of CGI programs in Perl language. In order to use users' personal photographs as their pass-images, Awase-E adds two modules into a traditional authentication system. These are "image registration" and "user notification" (Fig.2).

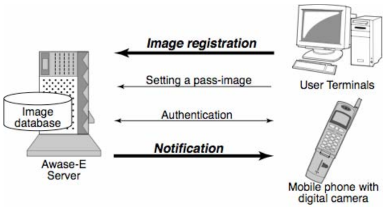


Figure 2. Four modules in Awase-E authentication system

The image registration module enables users to register selected photos to an image database at any time and from any location. The registration method is quite simple. A user uploads his or her pictures through an web interface. The pictures are pooled in a temporal space and are kept for a pre-defined period of time. The pictures are registered into the user's image database after the user confirms that he or she has indeed registered them. The method of setting pass-image is quite simple. A user just selects favorite pictures from his or her image set.

We make clear that image registration and setting of pass-images are completely different tasks. Image registration is just a registration of a user's photographs to the system. It does not mean that the newly registered photograph is automatically set as a pass-image. Users can, therefore, register a picture without authenticating themselves. They can, on the other hand, set or update their pass-images only if they have already passed the authentication.

The other module is a notification module. This module informs legitimate users of the occurrence of events in the authentication server by an e-mail. The notified events are as follows:

1) Image registration
2) Setting or updating of a pass-image
3) Starting authentication trial
4) Result of the authentication trial

The main goal of the module is that it gives legitimate users a trigger to handle an imminent threat. For example, a user receives an e-mail from the system although the user has not used the system today. It is clear that someone is trying to impersonate her or him. This function also enables users to confirm that user's request is correctly processed by the authentication system as well as to monitor malicious attempts.

3. Exploratory User Study

We conducted a memorability evaluation experiment in order to evaluate how easy it is to remember and recall personal photographs in the Awase-E scheme for a long period of time.

We selected four authentication methods for the experiment. As the character-based authentication method, we chose a 4-digit password(PIN) and an alphanumeric password of more than 6 characters (Password). As the "Déjà vu" like image-based authentication system(Random Art), we used the same authentication scheme as that of Awase-E. However, the system used 100 computer-generated abstract images instead of photographs. Each subject had to choose 4 images as pass-images from these abstracted images. In Awase-E, 1200 photos were pre-registered, and subjects were required to register 4 personal photographs.

Ten university students, all in their twenties, male, and belonging to the same laboratory, were involved in the experiment. They were all familiar with PIN and alphanumeric password authentication through the use of bank ATMs or PCs in daily life. However, they have no experience in using any image-based authentication systems. The experiments were done 0 (i.e., the initial authentication), 2, 4, 8 and 16 weeks after the subjects set their secret information (i.e., password or pass-image) to each authentication system. Just after the authentication at the 16th week, we forced the subjects to update their secret information. Then, after 2 weeks (i.e., 18th week), they were asked to authenticate again. The subjects were allowed up to 3 trials for each experiment.

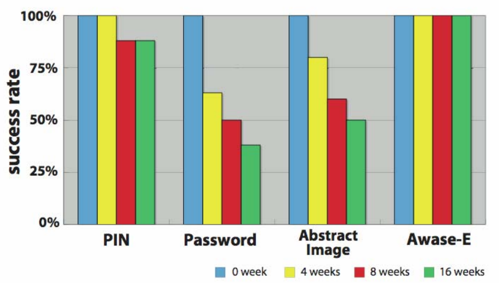


Figure 3. A transition of success rates in four authentications

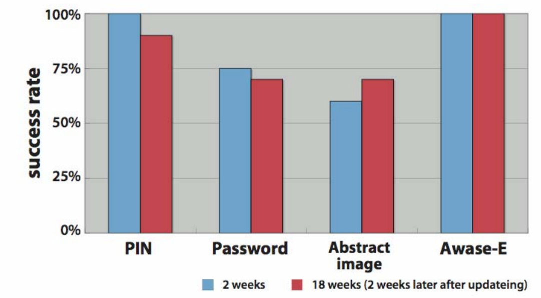


Figure 4. A transition of success rates before and after updating secret information

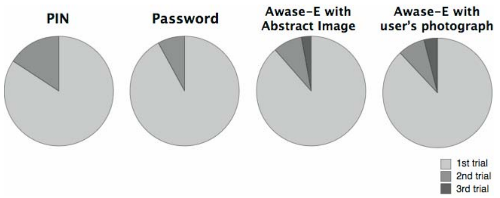


Figure 5. The number of trials when an authentication was successful

Fig.3 shows the success rate of four authentication methods after 0, 4, 8 and 16 weeks in the experiment. This result shows that the success rate of Awase-E was the highest, and it was 100 percent within 3 trials after 16 weeks. On the other hand, over 60 percent of the subjects forgot their passwords and 50 percent of the subjects forgot their abstract pass-images after 16 weeks.

Fig.4 shows the success rate transition when the subjects were forced to update their secret information. The subjects were asked to update their secret information just after the authentication at the 16th week. The graph shows the success rate at 2 weeks after setting the initial secret information and the success rate at 2 weeks after updating the secret information. From this graph, it is notable that the success rate of traditional authentications becomes lower but that of image-based authentication does not.

Fig.5 shows the number of trials when authentication was successful. This result shows that, in both image-based authentication systems, some subjects succeeded at the third trial. On the other hand, there is no case, in PIN or password authentication, that subjects succeeded at the third trial.

4. Considerations

4.1. Discussion of experiment result

From the result in fig.3, we could say that recognition-based image authentication using personal photographs makes it possible for users to remember four pass-images over a long period of time. The result also suggests that it is possible to provide a stable authentication even when an authentication is not used frequently. In this experiment, the minimum interval of the trials was 2 weeks. This is probably less frequent than the use of authentication at a bank ATM in our daily lives. The same implication was described in the paper[1] and a similar evaluation result was also reported in the paper[6].

The other interesting result of the experiment is the number of trials when the authentication was successful. It shows that, in recognition-based authentication systems, there is a possibility of recalling users' pass-images by doing a few trials even if they forgot them at the first trial. This phenomenon suggests that a recognition-based authentication reminds users of their secret information and helps them to pass the authentication through multiple trials.

The success rate transition after updating the secret information is also positive. We first assume that the success rate would decrease in all authentication schemes because subjects might confuse old and new secret information or they might fail to remember the new information since they had become familiar with the old information in 16 weeks. However, the experiment shows the unexpected result that the success rate in recognition-based authentications did not decrease over a period of time though the success rate in recall-based authentications did decrease. This result may suggest that recognition-based authentication avoids the confusion that would occur when users have updated their secret information.

4.2. Comparison between PIN and Awase-E regarding Usability and Security

We also made a comparison between PIN and Awase-E authentication with respect to usability and security. First, we discuss usability in the two schemes. We pick up three evaluation factors for usability: memorability, operation time, and the number of key operations. We could say that memorability of the secret information in Awase-E is the same or more than that of PIN number. The reason is that our experiment result shows that an authentication success rates through a long period of time with infrequent use of Awase-E is almost same as that of PIN authentication Moreover, even if a user is forced to update secret information, the number of authentication failures in Awase-E is less than that of PIN authentication.

On the other hand, the average operation time of Awase-E was 24.6 seconds. It is almost 10 times longer than that of PIN authentication. We believe that the operation time could be improved by both refining system implementation and getting users accustomed to the system. Finally, the number of keys to be typed is the same in both schemes if a user can directly choose an answer by a key.

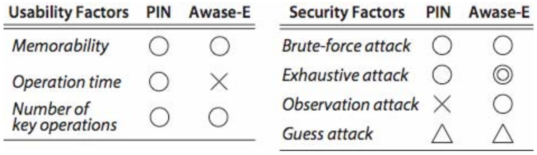
We then compare the security level against attack methods in both authentications. A security level against brute-force attack is almost same in both authentications because the security level is defined by the user interface of the authentication system. The probabilistic value by which an attacker accidentally succeeds in PIN authentication is 1/10000(=1/10^4). On the other hand, the probabilistic value in the Awase-E is 1/9999(=1/(10^4-1)) because Awase-E does not allow the answer “all no pass-image” as a correct answer.

The security level against exhaustive attack is different in both schemes. The exhaustive attack is a situation where an attacker tries to impersonate someone by providing all possible answers. Since PIN authentication has only ten answer candidates, the number of all combination for 4-digit number is 10000(=10^4). However, since the Awase-E could have more than 10 answer candidates, the number of all combination for four images becomes easily more than 10000. If a user registered 30 photographs in an image database, the number of all combination is 27405(=$_{30}C_4$).

The security level against observation attack is also different in both systems. There are no security measures against this attack in PIN authentication. On the other hand, we consider that Awase-E ensures some degree of security level against this attack because Awase-E has a challenge and response feature in the scheme. Even if an attacker managed to get a set of pass-images, the attacker could not always succeed to impersonate the victim because correct pass-images in an impersonation trial may not be same with stolen pass-images.

Finally, we could not reach a concrete answer about the security level against guess attack. Awase-E is considered most vulnerable against this type of attack. However, there is no evidence that the security level against the attack in Awase-E is inferior to that of PIN authentication. We believe that the memorability issue induces users to set easily guessable PIN numbers. Therefore, if an authentication system requires higher security against guess attack, the system must have good memorability of users' secret information. We consider that Awase-E is favorable in this respect. We summarize the comparison of usability and security in both authentications in table 1.

Table.1 Comparison of usability and security in PIN and Awase-E authentication



Usability Factors	PIN	Awase-E
Memorability	○	○
Operation time	○	×
Number of key operations	○	○

Security Factors	PIN	Awase-E
Brute-force attack	○	○
Exhaustive attack	○	◎
Observation attack	×	○
Guess attack	△	△

From the discussion, we conclude that Awase-E is superior to PIN authentication regarding security and Awase-E has same level of usability except for operation time. If there is no time requirement for an operation, Awase-E has sufficient usability and security as an alternative to PIN authentication.

4.3. Configurability of Balance between Security and Usability

Awase-E can be flexibly configured to balance security and usability according to the requirements of an authentication scene. This feature comes from the “no pass-image” answer. A unique point of the feature is that it enables increasing the security level without decreasing memorability and also improves memorability without decreasing the security level of the system.

If a user needs more secure authentication, Awase-E meets the requirement by adding more verification stages. If each user has 4 pass-images and the number of verification stages changes from 4 to 5, the probability value of an accidentally successful brute-force attack becomes to 1/40950. The important point is that Awase-E makes it possible to realize a more secure level without adding pass-images. Users, therefore, do not feel any extra memory burden in order to increase the security level of Awase-E.

On the other hand, if a user places a higher priority on memorability of user's pass-images than the security level of the system. Awase-E could reduce the number of pass-images while maintaining the number of verification stages. Awase-E could decrease the memory burden to users and still maintain the same security level of the system.

5. Conclusion

We proposed a recognition-based image authentication scheme named Awase-E. That has two unique features. 1) The scheme allows users to use their personal photographs as pass-images. This brings a memorability advantage into this type of authentication. 2) The scheme introduces a special answer “no pass-image”. This increases the security level of the system because it enables the integration of a challenge and response function to this type of authentication system. Moreover, it also enables an increased security level by adding to the number of verification stages without increasing the number of user's pass-images.

We implemented an web-based prototype system and conducted an exploratory study on how well personal photographs are remembered over a long period of time. From the results of experiment, we conclude that: 1) Personal photographs have almost same degree of memorability as a PIN number. 2) Using personal photographs and a recognition-based scheme shows superior performance even after updating a user's secret information. We discuss security and usability of both PIN and Awase-E authentication and concluded that Awase-E has sufficient security and usability levels to become a viable alternative to PIN authentication.

References

[1] R. Dhamija and A.Perrig, “Deja Vu: A User Study Using Images for Authentication”, *In proc. of 9th USENIX Security Symposium*, pp.45-58, August 2000.

[2] De Angeli, A., Coventry, L., Johnson, G., Renaud, K., “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems”, *International Journal of Human-Computer Studies*, Vol.63, No.1-2, pp.128-152, July 2005.

[3] T.Pering, M.Sundar, J.Light and R.Want, “Photographic Authentication through Untrusted Terminals”, *IEEE Pervasive Computing*, Vol.2, No.1, pp.30-36, 2003.

[4] T.Takada, H.Koike, “Awase-E: Image-based Authentication for Mobile Phones Using User's Favorite Images”, *Proc. of 5th Intl. Symposium on Human Computer Interaction with Mobile Devices and Services*, Springer, pp.347-351, 2003.

[5] D.Davis, F.Monrose and M.K.Reiter, “On User Choice in Graphical Password Schemes”, *In proc. of 13th USENIX Security Symposium*, 2004.

[6] T.S.Tullis and D.P.Tedesco, “Using personal photos as pictorial passwords”, *In proc. of ACM CHI2005, Conference on Human Factors in Computer Systems*, pp.1841-1844, 2005.