Proceedings of the Fifth IIEEJ International Workshop
on Image Electronics and Visual Computing 2017
Da Nang, Vietnam, February 28 - March 3, 2017

IMPROVEMENT OF ATTACK RESISTANCE FOR THE USER AUTHENTICATION METHOD FOR TOUCH SCREEN DEVICES "SWIPASS" BY IMAGE BLURRING

Tsuyoshi Suzuki[†] Masafumi Kosugi[††] Osamu Uchida[‡]
[†]Tokai University [††]Yahoo Japan Corporation [‡]Tokai University

ABSTRACT

Users of smartphones and/or tablet computers browse and download confidential document files routinely. Therefore, the higher security level is needed for smartphones and tablet computers than conventional mobile phones (feature phones). From this kind of background, we proposed SWIPASS, an image-based user authentication method for touch screen devices by using images shot by user oneself and gotten from the Web. SWIPASS has resistance to observation attack and recording attack, the most serious threats for touch screen devices. However, there is an issue with SWIPASS such that the fake image, which is a kind of pass image, is comparatively easily recognized by attackers. Then, in this study, we propose a method that prevents identification of the fake image by attackers by blurring images that appear on authentication screen. We moreover conduct experiments to verify the effectiveness of the proposed method.

1. INTRODUCTION

In recent years, touch-screen-enabled mobile terminals such as smartphones and tablets have spread rapidly, and this trend is expected to continue in the future. The functions to unlock the screen lock that are installed to touch screen devices are generally vulnerable to the various kinds of attacks by attackers who tries to use these devices illegally. In order to resolve this issue, we proposed SWIPASS [1], an image-based user authentication method for touch screen devices by using the images shot by the user and the images on the WEB in a previous study. However, there is an issue such that the fake image, which is always become the swipe object, is comparatively easily recognized by attackers. Therefore, in this study, we propose a method that prevents identification of the fake image by attackers by blurring images that appear on authentication screen. Moreover, we conduct experiments to verify the effectiveness of the proposed method.

2. SWIPASS: IMAGE-BASED USER AUTHENTICATION FOR TOUCH SCREEN DEVICES

2.1. BRIEF OVERVIEW

SWIPASS [1], a user authentication for touch screen devices proposed by Kosugi et al. is an image-based authentication method [2, 3, 4, 5] and is based on the method proposed by Takahashi and Uchida [6]. The greatest characteristic of SWIPASS is to use the images shot by user oneself and gotten from the WEB as images for authentication. These images are updated frequently, then the resistance for observation attacks of SWIPASS is higher than the lock screen release functions installed to touch screen devices generally such as the PIN method, the password method , and the pattern lock.

At the time of authentication operation, P images are displayed in a grid N times in total (Fig. 1). There are three kinds of authentication screen in SWIPASS as follows:

(a) the pass image and $P-1$ decoy images are displayed,

(b) the fake image and $P-1$ decoy images are displayed,

(c) only decoy images (P images) are displayed,

where the pass image is the most recent image that a user shot and saved before the authentication operation (hereinafter referred to as the latest image), the decoy images are images shot by the user except the latest image, and the fake image which is an image acquired from the Web. In the case of authentication screen (a), only images shot by the user oneself are displayed on the authentication screen. One out of P images is the latest image and has the role of the pass image, and the rest $P-1$ decoy images are randomly selected from the images shot by the user oneself. In this case, the user has to swipe the pass image in the direction the user set in advance (the numbers of swipe directions is 8, that is, the upward, downward, left, and right directions as well as four diagonal directions). In the case of authentication screen (b), $P-1$ decoy images and one image acquired from the Web. The image is called the fake image and assume a role of a kind of a pass image. In this

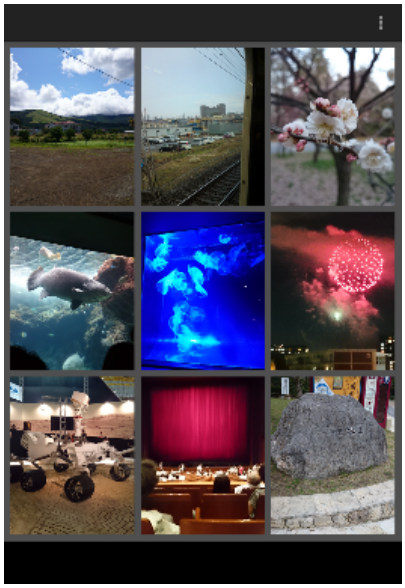


Figure 1: An example of an authentication screen in SWIPASS ($P = 9$)

case, the fake image becomes an object for the swipe manipulation and the direction of swiping should be the one determined depending upon which round of the verification phase it falls into out of the N rounds (configured by the user in advance). In the case of authentication screen (c), only decoy images are displayed, and these images are selected randomly from the images shot by the user oneself. In this case, the user can swipe any P decoy image and the direction of swiping is equal to the case of (b). SWIPASS displays authentication screen (a) one time, authentication screen (b) one time, and authentication screen (c) $N - 2$ times and the probability that the authentication operation by the attacker is successful by chance is $1/P^2D^N$ where D is the number of kinds of swipe directions . Both the indication sequence of authentication screens (a), (b), and (c), and the display position of P images on each authentication screen are random. Suitable swipe manipulations in all verification phase result in an authentication success. Figure 2 shows an example of an authentication operation in SWIPASS in the case of $D = 8$, $P = 9$, and $N = 3$. Because the pass image is modified each time the user takes a picture in SWIPASS, its resistance to an observation attack is close to a one-time password for users who frequently take pictures. In addition, users who perceive themselves at risk of shoulder surfing can update the pass image through the simple operation of taking another photograph.

2.2. ISSUE OF SWIPASS

There is an issue with SWIPASS such that the attack resistance is insufficient. SWIPASS uses an image obtained from the Web as the fake image. The atmosphere of the fake image is generally different from the images stored in the user's terminal (that are shot by the user), because the fake image is obtained from the Web. Then, there is a possibility that attackers identify the fake image in the authentication screen (b) easily.

3. PROPOSED METHOD

We propose an improvement method of SWIPASS that prevents identification of the fake image by attackers based on blurring images that appear on authentication screen. Though there are various kinds of image blurring, in this study we blur images appeared on the authentication screens by the stained glass-like image generation using Voronoi diagram. The flow of the stained glass-like image generation is as follows:

(1) The initial kernel points of Voronoi diagram are placed at regular intervals. In this study, the image size was fixed to 300 $\times$ 300 [pixels] and the intervals was set to 15 pixels.

(2) All the kernel points are moved within the compass of 8 $\times$ 8 [pixels] randomly (Fig. 4 (a)), and the Voronoi diagram is generated using them (Fig. 4 (b)).

(3) In each Voronoi region, we calculate average pixel values of the input image and change the value of all pixels in the region into it (in the case that the input image is the fake image, we decrease the saturation value of the image by 40 $\%$ in advance).

4. EXPERIMENT

In order to verify the usefulness of the proposed method, we performed two experiments on the identification of fake images.

4.1. IDENTIFICATION OF FAKE IMAGES BY ATTACKERS

4.1.1. Experimental method

We performed an experiment on the identification of fake images by attackers as described below with 10 subjects (twenty-something males). Subjects in this experiment were regarded as attackers against SWIPASS.

(1) A person (other than the subjects) was ordered to provide 50 latest images taken by his smart phone (these

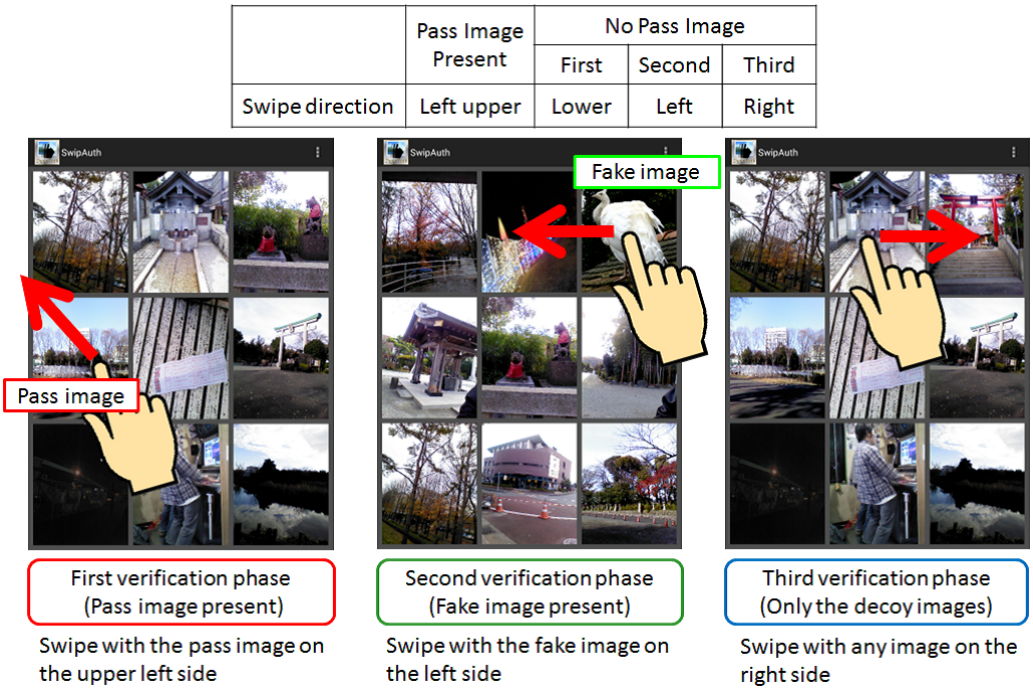


Figure 2: An example of authentication by SWIPASS [1]

pictures are considered as the pass image and the decoy images).

(2) Various images were obtained from Pixabay, an image sharing service (these images are considered as fake images).

(3) The stained glass-like images of both the provided images and the fake images were generated by applying the proposed method.

(4) Presentation of screens similar to those during the verification phases of SWIPASS is performed 20 times (the number of presented images P was set to 9). Out of the 20 screen presentations, fake images appear in only 10 presentations selected at random.

(5) Each subject answers which image is the fake image when they determine that there is a fake image among the nine presented on the screen. If they determine that there is no fake image on the presented screen, they answer "no fake image."

4.1.2. Results and discussion

The mean and standard deviation of the rate of success in identification fake images are 0.33 and 0.18, respectively. Then, the proposed method improves the attack resistance for SWIPASS, because the mean of the rate of success in identifying fake images in Ref. [1] is 0.6 (the experimental methods of this study and Ref. [1] are slightly different). Moreover, it revealed that when the color of the fake image was quite different from the other images, subjects recognized the fake image with high probability. Therefore, it is desirable that a fake image the color of which is similar to the ones of images shot by the user is presented in the authentication screen (b).

4.2. IDENTIFICATION OF FAKE IMAGES BY LEGITIMATE USERS

4.2.1. Experimental method

We performed an experiment on the identification of fake images by legitimate users as described below with 5 subjects (twenty-something males).

(1) Subjects were ordered to provide 50 latest images taken by their smart phones.

(2) Various images were obtained from Pixabay, an image sharing service (these images are considered as fake images).

(3) The stained glass-like images of both the provided images and the fake images were generated by applying the proposed method.

Table 1: Rate of success in identifying fake images by legitimate users

Subject	u_1	u_2	u_3	u_4	u_5	Average	Standard dev.
Fake image present	0.7	1.0	0.9	0.9	0.8	0.86	0.11
No fake image	0.3	0.9	1.0	0.8	0.1	0.62	0.40

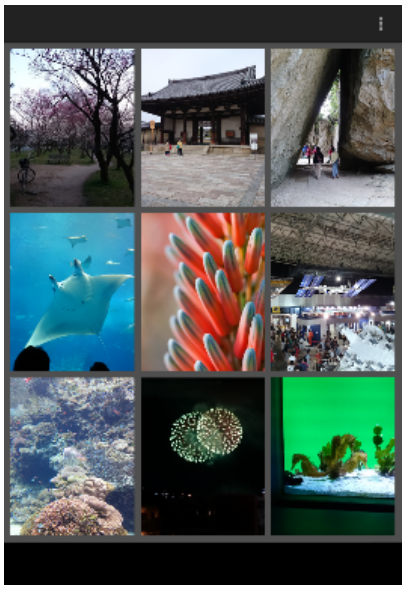


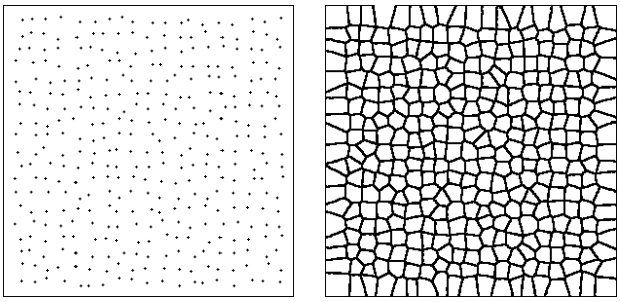
Figure 3: An example that the atmosphere of the fake image is greatly different from the images stored in the user's terminal (the center image is the fake image)

(4) Presentation of screens similar to those during the verification phases of SWIPASS is performed 20 times (the number of presented images P was set to 9). Out of the 20 screen presentations, fake images appear in only 10 presentations selected at random.

(5) Each subject answers which image is the fake image when they determine that there is a fake image among the nine presented on the screen. If they determine that there is no fake image on the presented screen, they answer "no fake image."

4.2.2. Results and discussion

Results of the experiment (the percentage of those answering the correct fake image in the case where there is a fake image, and the percentage of those selecting "no fake image" in the case where there is no fake image) are shown in Table 1. The table shows that the means of the rate of success in identifying fake images decreases slightly for both cases compared to Ref. [1]. Especially, the rate of success by subjects u_1 and u_5 are low in the case where there is no fake image. We plan to analyze details of causes of the result .



(a) Kernel points (b) Voronoi diagram

Figure 4: Generation of a Voronoi diagram

(a) An original image (b) A stained glass-like image

Figure 5: Generation of a stained glass-like image

5. CONCLUSION

In this study, we proposed a method that prevents identification of the fake image by attackers by blurring images that appear on authentication screen. In addition, we conducted experiments to verify the effectiveness of the proposed method. We plan to consider the method to obtain a fake image the color of which is similar to the ones of the pass and the decoy images from the Web.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number 25330159.

REFERENCES

[1] M. Kosugi, T. Suzuki, O. Uchida, and H. Kikuchi, "SWIPASS: Image-Based User Authentication for Touch Screen Devices", Journal of Information Processing, Vol.24, No.2, pp.227–236 (2016).

[2] R. Biddle, S. Chiasson, and P.C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years", ACM Computing Survey, Vol.44, No.4, Article No.19 (2012).

[3] H. Koike, T. Masui, and T. Takada, "Image-based User Authentication, IPSJ Magazine, Vol.47, No.5, pp.479–484 (2006). (in Japanese)

[4] R. Dhamija, A. Perrig, "Déjà vu: A User Study Using Images for Authentication", Proc. 9th USENIX Security Symposium, pp. 45–58 (2000).

[5] T. Takada and H. Koike, "Awase-E: the Method Enables an Image-based Authentication to be More Secure and Familiar for Users with Providing Image Registration and User Notification", IPSJ Journal, Vol.44, No.8, pp.2002–2012 (2003). (in Japanese)

[6] T. Takahashi and O. Uchida, "A User Authentication Method for Smartphones Having the Tolerance to Smudge Attacks", The journal of the Institute of Image Electronics Engineers of Japan, Vol.42, No.5, pp.650–654, (2013). (in Japanese)