Electronic Preprint for Journal of Information Processing Vol.24 No.2

Regular Paper

SWIPASS: Image-Based User Authentication for Touch Screen Devices

Masafumi Kosugi[1,†1] Tsuyoshi Suzuki[1] Osamu Uchida[1,a)] Hiroaki Kikuchi[2,b)]

Received: June 1, 2015, Accepted: November 5, 2015

Abstract: Users of smartphones and/or tablet terminals browse and download confidential document files routinely. Therefore, a higher security level is needed for smartphones and tablet terminals than conventional mobile phones. From this kind of background, Takahashi and Uchida proposed an image-based user authentication method for touch screen devices by using the latest image shot by the user as the pass-image. The proposed authentication method is resistant to smudge attacks, one of the most serious threats for touch screen devices. However, the security strength of the method is low. Therefore, in this paper, we propose SWIPASS, an image-based user authentication method for touch screen devices that has higher security strength, by improving on the method proposed by Takahashi and Uchida. This improves the security strength without any change in either the resistance to smudge attacks or the users' burden of memorizing. Although Takahashi and Uchida implemented their method only as a prototype system in their study, we implement SWIPASS as a real Android application in this study. Moreover, we also examined the usability and the resistance of SWIPASS against observation attacks by conducting several experiments in this paper.

Keywords: smartphone, touch screen, user authentication, image-based authentication, smudge attacks, observation attacks

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 improvement of communication speeds and the spread of cloud storage services make the experience of browsing and editing document files using a smartphone similar to an ordinary PC; thus, smartphones require better security than what is required for a conventional mobile phone. There are generally four ways of unlocking the screen on an Android terminal: "slide," "pattern," "PIN," and "password" (Android 5.0 provides "Trusted Face," a screen unlock method based on face authentication). Among these, the pattern lock method involves releasing the screen lock by swiping (tracing with a finger) four or more of the nine points displayed on the screen in the order set by the user themselves (there are limitations such as a prohibition against passing the same point twice). While it is an easy-to-use authentication method that takes advantage of the features of the touch screen, Aviv et al. show that there exists an attack technique called a smudge attack (dirt attack) [1]. This is an attack performed by guessing the lock pattern from the dirt on the touch screen (trajectory traces of swipe).

With this background, our research group proposed a image-based authentication method for smartphone that uses an image (pass image, decoy image) to be displayed at the time of image authentication that the user takes beforehand (hereinafter referred to as the Takahashi and Uchida method) [2]. The Takahashi and Uchida method has a high resistance to smudge attacks, but the security strength is not foolproof. Thus, we propose an image authentication method called SWIPASS for touch screen terminals that has higher security strength by improving on the Takahashi and Uchida method. This improvement reduces the probability of an authentication operation by an attacker resulting in a haphazard success of $1/P$ over the Takahashi and Uchida method (P: the number of images to be displayed at the time of verification). In other words, it enhances the security strength but never diminishes the resistance to a smudge attack or increases the user's burden of memorizing. Although Takahashi and Uchida implemented their method only as a prototype system [2], in this study we implement SWIPASS as a real Android application. Also, in there work, there was no discussion on the usability and the resistance against attacks [2]. In this paper, we discuss the usability and the safety against observation attacks in the proposed method based on several experiments by using SWIPASS-installed Android tablet terminals.

2. User Authentication in a Smartphone and a Tablet Terminal

Here, we introduce the standard user authentication methods in a smartphone and a tablet terminal. First, we explain three types of lock screen release methods that are standard in an Android-based system: PIN method, password method, and pattern lock.

The PIN method involves the inputting of numerals set by the user in advance, which is identical to the existing methods typified by a bank code number. However, there is a limitation: it is

[1] Tokai University, Hiratsuka, Kanagawa 259–1292, Japan
[2] Meiji University, Nakano, Tokyo 164–8525, Japan
[†1] Presently with Yahoo Japan Corporation
[a)] o-uchida@tokai.ac.jp
[b)] kikn@meiji.ac.jp

easy to guess if set with a number associated with the user such as their birthday. When the number of digits of the PIN is M, the number of possible patterns is 10^M. Therefore, security strength is enhanced by increasing the number of PIN digits, but the user may find it difficult to memorize. In addition, it is extremely vulnerable to a shoulder surfing attack.

The password method performs authentication by entering an alphanumeric set by the user, which is the same method widely used, for example, when logging into a PC. There is a drawback in that it is vulnerable to a guess attack or dictionary attack in the case where the password is a word associated with the user or a simple English word. The number of password patterns is S^L, where the number of types of characters used for the password is S and the password length is L. In other words, a longer password enhances security strength, but the user finds it more difficult to memorize; moreover, it is not easy to enter a long string on a touch screen terminal with a small screen area such as a smartphone.

The pattern lock is an authentication method that takes advantage of the features of a touch screen by swiping four or more of the nine points that are displayed on the screen in the order set by the user (**Fig. 1**). The number of patterns is 389,112 in total [1], and it has higher security strength than a five-digit PIN code. However, it has been demonstrated that there remains the risk of a smudge attack in which a lock pattern is guessed by obtaining information about recent user input from dirt (locus marks) that remains on the touch screen when swiping [1]. In addition, it has no resistance to shoulder surfing attacks.

Next, we explain two biometric methods: face authentication and fingerprint authentication.

Android 5.0 provides an authentication method called “trusted face” which is a face recognition-based unlock method. The necessary action of a user is only to look the in-camera of the terminal and the authentication speed is very fast. However, face recognition-based authentication methods are basically week against illumination fluctuation. It is, for example, often pointed out that face recognitions are not available under low light condition.

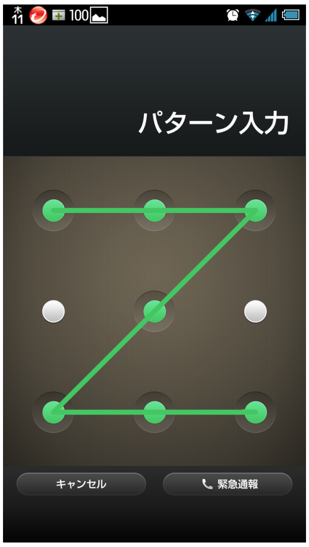


Fig. 1 An example of an authentication pattern in the pattern lock method [2].

Recent iPhones and iPads have fingerprint authentication function called Touch ID. Moreover, it was presented that the new Android version supports fingerprint authentication[*1]. The primary advantage of fingerprint authentication is the speed and the accuracy of verification. However, there are some biometrics-specific issues. For example, a German group announced that the Touch ID sensor could be fooled by using a sheet of latex or wood glue hosting the fingerprint ridges of a person only a few days after the iPhone 5S equipped with the Touch ID sensor was released [3]. Moreover, the ratio of devices equipped with a fingerprint sensor is not high at the present moment.

3. Image-Based User Authentication

Image-based user authentication is a method of using an image instead of numbers in the PIN method or text in the password method [4], [5], [6]. The advantages of image authentication are that an image is relatively easy to memorize [7] and has a high resistance to hacking by key loggers and similar tools. Various types of image authentication methods have been proposed, many of which perform authentication by correctly selecting the pass image that the user registered in advance as an alternative to a password from an image group including decoys.

For example, Déjà vu, proposed by Dhamija et al., [8] is an image authentication method that uses a random art image generated by a hash visualization algorithm [9]. The user selects five pass images from the image group generated by the system. A total of 25 images comprising five pass images and 20 decoy images are displayed at random positions on the grid at the time of authentication; the proper selection of the five pass images results in an authentication success. The combination patterns of selecting the five pass images out of the 25 possible are ${}_{25}C_5 = 53{,}130$ ways, and its security strength is greater than the one of a four-digit PIN. Because it employs random art for pass and decoy images, it is resistant to the educated guess attack (attack by guessing a pass image by utilizing knowledge about the user) [8], [10], [11]; however, the users themselves cannot memorize it easily.

Awase-E proposed by Takada et al. [12], [13] is a system that is primarily devised for use in mobile phones. Authentication is performed by selecting pass images from an image group mixed with pass and decoy images in the same manner as Déjà vu. The authentication is performed by choosing one pass image out of the nine available photos several times, and provides instances when no pass images are included. In the case of a system in which the pass image(s) are always displayed at the time of authentication, an intersection attack identifies pass images the difference in the probability of occurrence of pass and decoy images [8]. Awase-E is resistant to this type of attack. In addition, the latter enables the updating of pass images by transmitting images taken by the cellular phone to the authentication server by e-mail. It has the advantage of having a lower storage burden than Déjà vu, since it is possible to use pictures that users themselves took as pass images, but it is less resistant to the shoulder surfing attack. The number of input patterns in Awase-E is $10^N - 1$, where the num-

[*1] https://events.google.com/io2015/

ber of matching phases is N, and it has a security strength that is about the same as that for a four-digit PIN when $N = 4$.

Harada et al. proposed a method of creating meaningless images at a glance by applying a blurring process, including changing meaningful original images into a mosaic for use as pass images in order to provide resistance to a shoulder surfing attack [14]. In addition, Miyachi et al. proposed an image authentication method using an image generated by combining the high-frequency components of a pass image with the low-frequency components of another image for authentication [15]. This system assumes that a legitimate user who performs the authentication operation at a position close to the authentication screen can recognize the image, whereas it is difficult for an attacker who is further from the authentication screen to recognize the image in contrast. However, these systems have no resistance to attacks of photo voyeurism of authentication actions (recording attacks) by a camera or similar device.

Anzai et al. proposed an image authentication method that is resistant to recording attacks [16]. However, the method by Anzai et al. has 64 images (traffic signs) to display and thus it is not suitable for authentication for terminals with a small display area such as smartphones. Moreover, the time required for authentication is significant long, and poses a problem in terms of usability. The number of input patterns in the method by Anzai et al. is 16,834, and its security strength is slightly better than that of a four-digit PIN.

SmudgeSafe proposed by Schneegass et al. [17] is an authentication method that uses random geometric image transformations, such as translation, rotation, scaling, shearing, and flipping, to increase the security of cued-recall graphical passwords. Though SmudgeSafe has high resistance to smudge attacks and the security strength is higher than that of a four-digit PIN and the pattern lock, it has no resistance to observation attacks.

4. Attack Technique against Image Authentication

This section consolidates attack techniques that are carried out against image authentication.

A brute force attack involves trying all possible password patterns. Therefore, resistance to this attack increases as the number of input patterns becomes larger. Furthermore, resistance is improved by limiting the number of frequencies for which authentication failure is allowed (in bank ATMs, for example, authentication is made impossible when the PIN is entered incorrectly beyond a predetermined frequency).

The educated guess attack (guessing attack) is an attack in which pass images are guessed by utilizing knowledge about legitimate users [8], [10], [11]. The resistance to this attack is lower when pass images are highly relevant to authorized users (for example, images taken by legitimate users themselves), and decoy images are less relevant to the legitimate users.

An intersection attack is one that uses the difference in the probability of occurrence between pass images and decoy images [8]. For example, in an authentication method in which pass images are always presented, it would be possible to identify pass images by determining the product set of image groups of two matching phases.

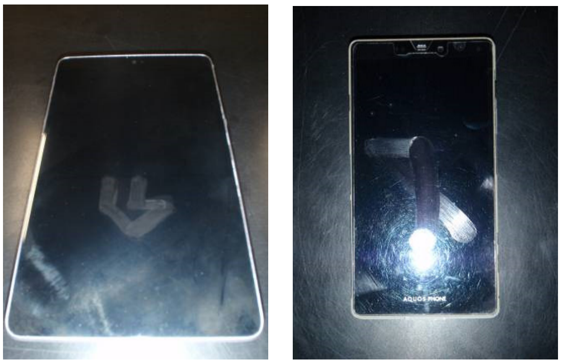


Fig. 2 Examples of smudge on touch screen devices.

An observation attack (peeping attack) is an attack technique that identifies pass images by peeping at the legitimate user's authentication operation (also called shoulder surfing). Threats include not only the attack whereby the attacker directly peeps at the authentication operation but also the attack of photo voyeurism of the authentication act (recording attack) with a camera or similar device, which has become a significant problem in recent years.

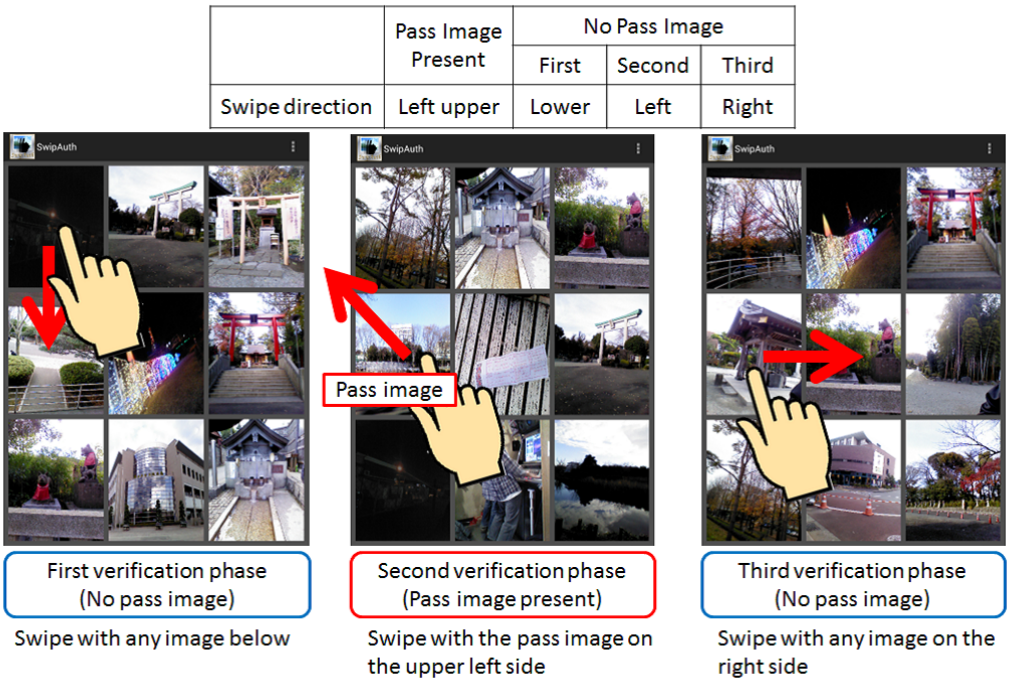
A smudge attack (dirty attack) is an attack technique that is performed against personal authentication performed using a touch screen by guessing the authentication pattern based on the locus marks (dirt) left on the screen by a finger. It has been reported that the authentication pattern of the pattern lock used in user authentication of the Android terminal can be inferred with high probability [1]. When the authors actually conducted verifications with their own smartphones and tablet terminal, smudges (locus marks of swipes) could be photographed (**Fig. 2**), and they could be confirmed easily through visual inspection.

5. Image Authentication Method for a Touch Screen Device

5.1 Method Proposed by Takahashi and Uchida

The image authentication method for touch screen terminals proposed in this study, SWIPASS, is based on the authentication method for smartphones that was proposed by Takahashi and Uchida [2]. Therefore, we describe an outline of the Takahashi and Uchida method first (hereinafter, the method described in the literature [2] is discussed in a generalized form).

The Takahashi and Uchida method is a kind of image authentication method, in which users themselves take pictures with their devices (smartphones) to be authenticated, using images stored in their terminals as pass and decoy images. The most recent image that a user shot and saved before the authentication operation (hereinafter referred to as the latest image) is regarded as the pass image, and other images stored in the terminal are used as decoy images. To identify which image is the latest one, the time stamp recorded in the Exif information of the image is used. When the user discards a photo image stored in the terminal, the image is not used as both pass and decoy image. (If the user eliminates the pass image, that is the latest image, the second latest image becomes the new pass image, even though it was used as a decoy image before that.) At the time of authentication, P images



	Pass Image Present	No Pass Image		
		First	Second	Third
Swipe direction	Left upper	Lower	Left	Right

SwipAuth
SwipAuth
SwipAuth
Pass image
First verification phase
(No pass image)
Swipe with any image below
Second verification phase
(Pass image present)
Swipe with the pass image on the upper left side
Third verification phase
(No pass image)
Swipe with any image on the right side

Fig. 3 An example of the authentication method by Takahashi and Uchida.

are displayed in a grid N times in total ($N = 3$ and $P = 9$ in Ref. [2]). Out of the N times of verification phases, a total of P images with a pass image and $P - 1$ decoy images are displayed at one time, whereas only decoy images (P images) are displayed for the remaining $N - 1$ times (**Fig. 3**). The user swipes the pass image displayed during authentication. Directions allowing the swipe are determined to be D kinds (a total of eight directions with the upward, downward, left, and right directions as well as four diagonal directions in Ref. [2]), out of which the user swipes in the direction they set in advance in the case of the pass image. If only decoy images are displayed, conversely, any one of the P decoy images is swiped. 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). The positions of the pass images and decoy images are determined at random every time, and at which round of the verification phase out of the N rounds the pass image will be displayed is also determined at random for each authentication. Information to be memorized by the user in the Takahashi and Uchida method contains the following $N + 2$ pieces of information:

- Pass image (one latest image)
- How to swipe the pass image (one direction out of the D directions)
- The direction of swiping any one decoy image in the case where only decoy images are displayed at the nth ($= 1, \cdots, N$) round of the verification phase (one direction out of the D directions)

The user's burden of memorizing in the case of $N = 3$ and $D = 8$ [2], for example, is presumed not to increase overwhelmingly in comparison with a four-digit PIN. (In order to compare the burden of memorizing of the two different authentication methods correctly, considering the viewpoint of the chunking mechanisms for memorability of the password [18] is thought to be important. We would like to consider this issue as part of our future work.)

The Takahashi and Uchida method is resistant to smudge attacks because the display positions of pass images and decoy images are random every time. It is highly resistant to observation attacks because it updates the pass image every time, and it is also resistant to intersection attacks because the former pass image becomes (a candidate of) the decoy image after updating. Moreover, given that images taken by the users themselves are used for both the pass images and decoy images, both are expected to be more relevant to the user. Therefore, it is also believed to be resistant to educated-guess attacks.

In the meantime, the combination of images and swipe directions has PD ways. Therefore, the probability that the attacker's attempt becomes the correct answer by chance is $1/PD$, because only when the image to be swiped and the swipe direction are in the correct combination is the answer correct during the verification phase when the pass image appears. Meanwhile, any image can be swiped and only the swipe direction determines whether or not it is the correct answer at the verification phase when only decoy images are displayed. Therefore, the probability that the attacker's attempt becomes the correct answer by chance is $P/PD = 1/D$. As the verification phase that contains the pass image appears once and the verification phases in which only the decoy images are displayed appears $N - 1$ times, the probability that the authentication operation by the attacker would be successful by chance is $(1/PD) \times (1/D)^{N-1} = 1/PD^N$. It is $\frac{1}{4{,}608}$ in the case of $N = 3$, $P = 9$, and $D = 8$ [2], larger than the case of a four-digit PIN ($\frac{1}{10{,}000}$). A remedy for the security strength for this problem may be to increase the number of verification phases, N, but it is in a trade-off relationship between the time needed for the authentication operation and the user's burden of memorizing. Although it is possible to enhance security strength by increasing the number of images displayed, P, it is possible that the identi-

	Pass Image Present	No Pass Image		
		First	Second	Third
Swipe direction	Left upper	Lower	Left	Right

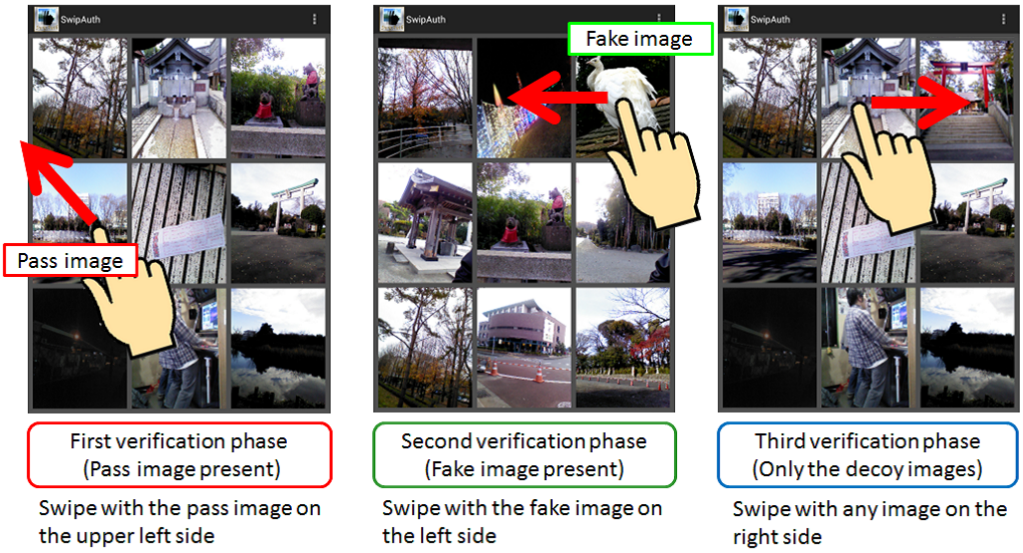

SwipAuth
Pass image
Fake image
First verification phase (Pass image present)
Swipe with the pass image on the upper left side
Second verification phase (Fake image present)
Swipe with the fake image on the left side
Third verification phase (Only the decoy images)
Swipe with any image on the right side

Fig. 4 An example of authentication by SWIPASS.

fication of images would become difficult in the case of utilizing a smartphone with a small display area. It is also less practical to increase the number of swipe directions, D, to more than eight.

5.2 Proposed Method: SWIPASS

This study aims to strengthen the security level by improving the method proposed by Takahashi and Uchida. Only decoy images are displayed at the time of $N - 2$ rounds of the verification phases during which no pass image (the latest image) appears in the Takahashi and Uchida method. In the SWIPASS method proposed and implemented in the present study, we decided to display an image acquired from the Web (hereinafter referred to as the fake image) at the time of either round of the verification phase to use it as a kind of pass image. When the fake image is displayed at the time of authentication, the fake image is swiped in the preset direction (the swipe direction should be the same as the case when only decoy images are displayed. In other words, it is the direction that determines upon which round of the authentication operation it falls). **Figure 4** shows an example of an authentication operation in SWIPASS in the case of $D = 8$, $P = 9$, and $N = 3$. Because fake images are not images taken by the legitimate users themselves, it is expected that legitimate users can identify them easily whereas it is difficult for attackers.

It was decided in this study that photos should be acquired using an image sharing service in the public domain, Pixabay[*2], to make them candidates for fake images. In the meantime, the "Survey on Photos" by the Life Media Research Bank [20] reports that "nature such as mountains and the sea" has a high percentage as a subject to be imaged. Thus, it was decided in this study that landscape photographs should be acquired in which nature, such as mountains or the sea, would be subjects to be photographed by providing an appropriate query to Pixabay, to be used as fake images at the time of authentication (it was originally desirable that the types of pictures to be acquired are changed in accordance with a group of photographs taken by users or, to paraphrase, queries given to Pixabay are changed, but that has not yet been realized at this time). This method has high resistance to intersection attacks because it changes the fake images in each authentication. Also, as described above, information indicating "whether or not they are the photographs taken by the legitimate users themselves" is required in order for attackers to determine decoy images and fake images. It is expected to be harder for attackers to distinguish fake images if appropriate fake images can be displayed. Note that resistance to the smudge attack is not deteriorated in this method as compared with the Takahashi and Uchida method. **Figure 5** shows a smudge after the authentication operation using the same pass image where it is found to be a different smudge. In addition, there is no change in the amount of information to be memorized by the user, compared to the Takahashi and Uchida method.

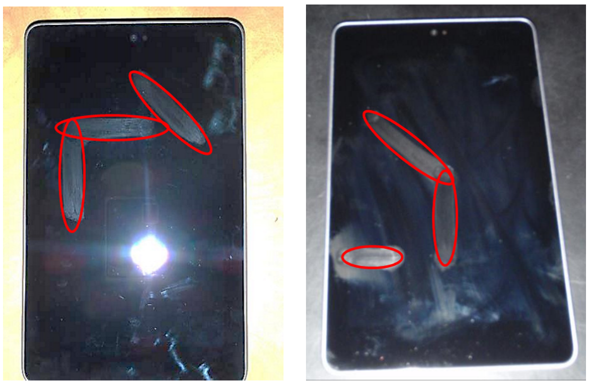


Fig. 5 An example of smudges after authentication in SWIPASS.

Note that the proposed method was implemented as an Android application in the present study. The development language

[*2] http://pixabay.com/

is Java, and Android Studio was used as the development environment. The terminal used for the operation verification was a Nexus 7 by Asus Inc., and the OS was Android 4.4.2. In addition, we verified that it can also work properly with a Nexus 7 by Asus Inc. using Android 5.0.2 and a Sharp ISW16SH using Android 4.0.2.

6. Discussions

6.1 Security Strength

If P images are displayed and the number of possible types of swipe direction is D, then a combination of images and swipe directions is PD. Since the correct answer appears only when the image to be swiped and the swipe direction are correct during the verification phase where pass and fake images appear, the probability that the attacker's attempt is correct by chance is $1/PD$. Meanwhile, any images can be swiped and only the swipe direction determines the correct answer or not in the verification phase when only decoy images are displayed. Therefore, the probability that the attacker's attempt is correct by chance is $P/PD = 1/D$. When the frequency of verification phases is N, the verification phase containing the pass image appears once, the verification phase containing the fake image appears once, and the verification phases in which only the decoy images are displayed appears $N - 2$ times, the probability that the authentication operation by the attacker is successful by chance is $(1/PD) \times (1/PD) \times (1/D^{N-2}) = 1/P^2D^N$, which is $1/P$ of the Takahashi and Uchida method. It is $\frac{1}{41{,}472}$ when $N = 3$, $P = 9$, and $D = 8$ [2], for example, which means it has higher security strength than a four-digit PIN. It is believed from this fact that the issue of security strength that had been problematic in the Takahashi and Uchida method could be resolved to some extent.

6.2 Usability Verification

To evaluate the usability of SWIPASS, we conducted an experiment to measure the authentication time with 5 subjects (under graduate and graduate students at Tokai University). The experimental method is as follows:

(1) Authentication time of SWIPASS is measured three times.

(2) Subjects memorize all 56 images stored in the terminal for the experiment (Nexus 7 by Asus, Inc.) and predetermined swipe directions beforehand.

(3) Subjects experience the SWIPASS authentication several times in order to get used to the operation of SWIPASS before the experiment.

(4) The frequency of verification phases of SWIPASS is three times, the number of presented images is nine, and the possible swipe directions comprise eight directions, that is, $N = 3$, $P = 9$, and $D = 8$.

(5) Subjects are asked to write their opinions on SWIPASS authentication

Table 1 shows the result of the experiment. Zezschwitz et al. [19] have shown that the authentication times of the PIN approach and the pattern lock are about 1.5 sec and 3 sec, respectively. Therefore, SWIPASS has users spend more time than the PIN approach and the pattern lock. That is, SWIPASS is inferior compared to the PIN and the pattern lock in terms of usability. However, in this experiment, the sets of pass images and decoy images are not of the subjects themselves, and moreover the swipe directions are determined by the examiners. Several subjects commented that time was needed to distinguish fake images from decoy images because the set of images is not his/hers. Several subjects also remarked that if he/she determined the swipe directions by himself/herself, he/she would not hesitate with the direction of swipe behavior. From these, it is expected that the actual authentication time of SWIPASS is shorter than the results of the experiment.

Table 1 Authentication time.

	Average [s]	Max [s]	Min [s]	Standard dev.
1st challenge	8.14	10.42	6.54	1.29
2nd challenge	8.59	11.23	5.68	1.90
3rd challenge	8.47	11.33	6.7	1.65

6.3 Verification of the Identification of Pass Images and Fake Images by the Legitimate Users

In order to verify if it is easy for legitimate users to distinguish between the latest image required for authentication (pass image) and the image acquired from the Web (fake image), we performed two experiments as described below with 10 subjects ($u_1, \ldots, u_{10}$: under graduate and graduate students at Tokai University).

6.3.1 Identification of Pass Images

We verified whether legitimate users can identify the latest images (pass images) correctly (Experiment 1). The experimental method is as follows:

(1) Presentation of screens similar to those at the verification phases of SWIPASS is performed 20 times (the number of presented images P was set to 9 this time).

(2) Out of the 20 screen presentations, pass images appear in only 10 presentations selected at random (that is, only decoy images are displayed for the remaining 10 presentations).

(3) The subjects each answered which image is the pass image when they determine that there is a pass image among the nine presented on the screen. If they determine that there is no pass image on the presented screen, they answer "no pass image."

(4) The image group to be used in the experiment consists of the 30 most recent images taken by the subjects.

(5) An experiment is performed on the day following the provision of images or later, considering the possibility that subjects accidentally view them when providing them.

Results of Experiment 1 (the percentage of those answering the correct pass image in the case where there is a pass image, and the percentage of those selecting "no pass image" in the case where there is no pass image) are shown in **Table 2**. It shows the polarization of subjects with high identification success rates and those with low rates.

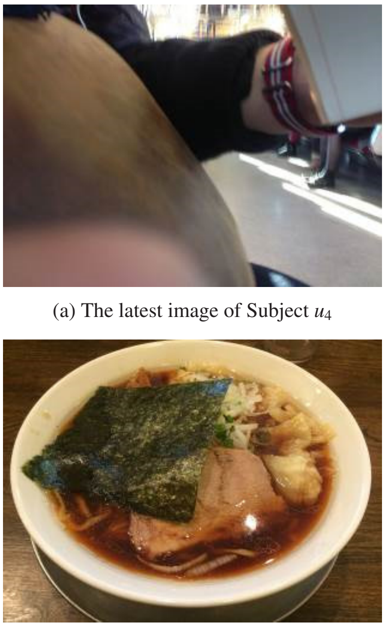
The latest images of Subjects u_4 and u_5 are shown in **Fig. 6** as an example of a case where the identification success rate is low. It is inferred that the latest image of Subject u_4 could not be identified as the latest image, because it was an image that he shot unintentionally. In addition, the latest image of Subject u_5 was an image of noodles but the image group included many noodle images and thus it is presumed that the identification of the lat-

Table 2 Rate of success in identifying pass images by legitimate users.

Subject	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	Average	Standard dev.
Pass image present	0.9	1.0	0.9	0	0	0	0.1	0	0.7	0.7	0.43	0.42
No pass image	1.0	1.0	1.0	0.8	0.6	0.8	0.7	0.1	0	1.0	0.7	0.35

Table 3 Rate of success in identifying fake images by legitimate users.

Subject	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	Average	Standard dev.
Fake image present	1.0	1.0	1.0	0.9	1.0	1.0	1.0	0.9	0.9	0.9	0.96	0.05
No fake image	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0


(a) The latest image of Subject u_4

(b) The latest image of Subject u_5

Fig. 6 The latest images of two subjects with low identification success rates.

est image was difficult. Because the inability to identify the pass images implies that legitimate users themselves fail to pass the authentication, it is necessary to consider countermeasures. For example, the accuracy of identifying pass images is expected to be improved by excluding images whose shooting dates/time are close to those of the pass image or those having similar characteristics from the group of candidates for decoy images. In the future, we would like to consider such ideas.

Note that the subjects were not requested to memorize the latest images before the experiments. The actual identification success rate is expected to be higher than the result of Experiment 1, because it is anticipated that users are eager to memorize the latest images proactively in a situation where SWIPASS is actually supposed to be utilized for user authentication. In the future, experiments on the identification of the latest images are to be performed under an environment close to the actual utilization of SWIPASS, namely where the memorization of the latest images is required during authentication of the user's own terminal.

6.3.2 Identification of Fake Images

We verified whether legitimate users can identify images acquired from the Web (fake images) correctly (Experiment 2). The experimental method is as follows:

(1) 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 this time).

(2) Out of the 20 screen presentations, fake images appear in only 10 presentations selected at random (that is, only decoy images are displayed for the remaining 10 presentations).

(3) 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) The image group used in the experiment consists of the 30 latest images taken by the subjects.

(5) An experiment is performed on the day following the provision of images or later, in order to take into account the possibility that subjects accidentally view them when providing them.

Results of Experiment 2 (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 3**. It is presumed from Table 3 that it is easy to identify between the images shot by users themselves and fake images, or that the legitimate users are able to identify fake images with a high level of accuracy.

6.4 Verification of the Resistance to Observation Attacks

SWIPASS is believed to be more resistant to observation attacks than other image authentication methods because it updates the pass image each time a photograph is taken. However, this tolerance is in a trade-off relationship with the frequency of the taking of photographs. Therefore, we tried verification through experiments to determine its resistance to observation attacks in a situation where pass images are not updated. This experiment was conducted with 10 subjects ($v_1, \ldots, v_{10}$: under graduate and graduate students at Tokai University). Subjects in this experiment were attackers against SWIPASS, and the experiment was conducted after the SWIPASS authentication method was explained to them to allow them to fully understand it.

6.4.1 Identification of Pass Images and Fake Images by Attackers

We asked the subjects to view video images prepared by shooting actual authentication operations (**Fig. 7**), followed by implementation of the experiment on whether they could guess pass images and fake images (Experiment 3). The experimental method is as follows:

(1) The video image consists of 10 authentication operations of SWIPASS that was shot by the legitimate user himself.

(2) Considering cases where the authentication operation is hard to see, the images swiped at each verification phase and the swiped directions are presented as character information.

(3) The frequency of verification phases of SWIPASS is three

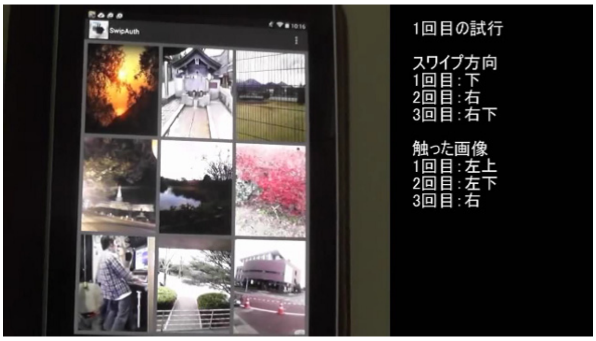


Fig. 7 A clip on the authentication operations.

Table 4 Rate of success in identifying pass images and fake images by attackers.

	Average	Standard dev.
Pass image	0.28	0.28
Fake image	0.6	0.25
Successful in simultaneous identification of pass images and fake images	0.23	0.23

times, the number of presented images is nine, and the possible swipe directions comprise eight directions, that is, $N = 3$, $P = 9$, and $D = 8$.

(4) The image set stored in the terminal to be attacked (Nexus 7 by Asus, Inc.) contains 30 images.

(5) The subject chooses the pass image when they see a video of the authentication operation, as well as the phases and the locations where they guess the fake images have appeared.

The mean and standard deviation of the rate of success in identification in Experiment 3 is shown in **Table 4**. Fake images had a high average of correct answer rates, as high as 0.6, indicating that it was possible for attackers to guess them with a relatively high probability. In particular, both of the fake images displayed in the second and seventh authentication operations had a very high probability of identification (success rate was 0.9).

These images with the highest identification success rates (**Fig. 8**) are considered to be attributed to the fact that their photographic subjects (their impressions) were significantly different compared with other images displayed on the authentication screen. Additionally, the low rate of success in identifying fake images in **Fig. 9** appears to be attributed to the fact that incongruity was small or there was a small difference between them and other decoy images. It is believed from the above results that if it is possible to present images similar to the ones that the user photographed as fake images, it would be difficult for attackers to guess the fake images. In the future, we would like to consider the application of of similarity-based image retrieval techniques [21], [22].

6.4.2 Experiment that Assumes a Recording Attack

Subjects were asked to view video images prepared by shooting authentication operations, followed by the implementation of an experiment by actually performing their authentication operation (attack) on the target terminal (Experiment 4). The experimental method is as follows:

(1) The video image consists of 10 authentication operations of SWIPASS that was shot by the legitimate user himself (it is a different video from that used in Experiment 3).

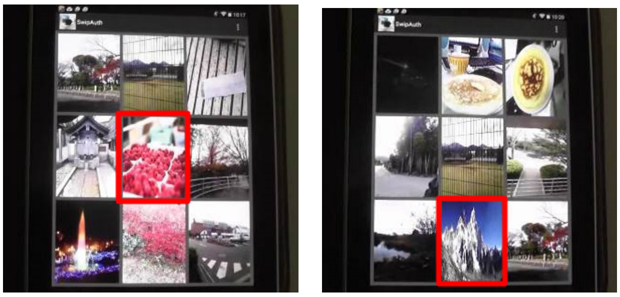


Fig. 8 An example of an authentication screen with a high rate of identifying fake images.

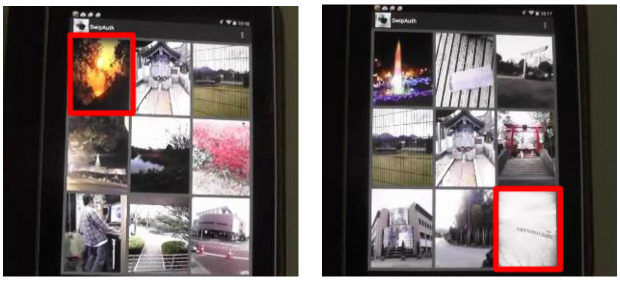


Fig. 9 An example of an authentication screen with a low rate of identifying fake images.

(2) Considering the case where the authentication operation is hard to see, the images swiped at each verification phase and the swiped directions are presented as character information.

(3) The frequency of verification phases of SWIPASS is three times, the number of presented images is nine, and the possible swipe directions comprise eight directions, that is, $N = 3$, $P = 9$, and $D = 8$.

(4) The image set stored in the terminal to be attacked (Nexus 7 by Asus, Inc.) contains 30 images (they are different video images from those used in Experiment 3).

(5) The subject actually performs the authentication operation (attack) on the terminal to be attacked each time they see a video image of an authentication operation.

(6) The frequency of attempts until the attack is successful is measured (however, the maximum frequency of attempts was set to 10).

The results of Experiment 4 (frequency of attempts required for success in authentication) are shown in **Table 5** (F means an attack failure in all of the 10 attempts). As can be seen from Table 5, two out of the ten subjects failed to attack in all of the 10 attempts, whereas the remaining eight subjects were successful in attacking within 10 attempts. The minimum value for the frequency of attempts required until a successful attack was three.

While Experiment 4 was anticipated to be a very favorable situation for attackers in which users' authentication operations were spied on continuously more than once through voyeurism and similar methods (recording attack) and with no pass image (latest image) being updated, we verified that this method had a certain degree of resistance even under such circumstances. The pass image appearance probability and the probability that the pass image makes no appearance for each verification phase are $1/N$ and $1 - 1/N$, respectively, where N is the number of verification phases. Therefore, observing several authentication operations continuously enables attackers to infer the pass image,

Table 5 Frequency of attempts required for success in authentication.

Subject	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}
Frequency of attempts	3	6	8	4	3	4	3	9	*F*	*F*

the swipe direction of the pass image, and the swipe directions of the decoy or fake images for each verification phase. However, attackers have to identify the fake image correctly in order to become successful with authentication. This means that if it is difficult for attackers to discriminate fake image from decoy images, attackers cannot break through SWIPASS authentications. This also indicates that introducing fake images improves the tolerability against observation attacks of the Takahashi and Uchida method.

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. In the future, we plan to compare our method with other image-based user authentication methods that are resistant to observation attacks (e.g., Refs. [23], [24]).

6.5 Comparison with Other Authentication Method

In this section, we compare between SWIPASS against other image-based authentication methods. SWIPASS as well as the Takahashi and Uchida method [2] is resistant against smudge attacks, however, the security strength of SWIPASS is higher than that of the Takahashi and Uchida method. We expect the authentication time of SWIPASS to be slightly longer than that of the Takahashi and Uchida method. The resistance of SmudgeSafe [17] against smudge attacks is considered to be no less high than that of SWIPASS. Moreover, the usability and the security strength of SmudgeSafe are better than SWIPASS. However, it does not tolerate observation attacks very well. Anzai et al. [16] insisted that their proposed method is resistant to recording attacks. It is difficult to conclude which of SWIPASS and the method proposed by Anzai et al. is better from the viewpoint of resistance to recording attacks, however it is obvious that the usability of the method of Anzai et al. is not enough for practical use because the average authentication time is longer than 40 secs.

7. Conclusion

In this study, we proposed an image authentication method, SWIPASS, for a touch screen terminal, and implemented it as an Android application. In addition, we discussed the usability and security of the proposed method. Future challenges include the examination of a method for displaying images with high similarity to the images stored in the terminal as fake images, addressing the cases where legitimate users cannot identify any pass images, and a detailed comparison with other image authentication methods. We think that there is a need to verify the details regarding authentication time and users' burdens of memorizing in the long run. In addition, we also plan to extend our research to multi-touch authentication [25], [26].

Acknowledgments We are grateful to Emeritus Prof. Shohachiro Nakanishi, Tokai University, for his valuable comments. We also thank reviewers for their valuable comments which helped to improve the paper. This study was partially supported by JSPS KAKENHI Grant Number 25330159.

References

[1] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. and Smith, J.M.: Smudge Attacks on Smartphone Touch Screens, *Proc. 4th USENIX Workshop on Offensive Technologies* (2010).

[2] Takahashi, T. and Uchida, O.: 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).

[3] Marasco, E. and Ross, A.: A Survey on Antispoofing Schemes for Fingerprint Recognition Systems, *ACM Computing Surveys*, Vol.47, No.2, Article 28 (2015).

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

[5] Suo, X., Zhu, Y. and Owen, G.S.: Graphical Passwords: A Survey, *Proc. 21st Annual Computer Security Applications Conference*, pp.463–472 (2005).

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

[7] Goldstein, A.G. and Chance, J.E.: Visual Recognition Memory for Complex Configurations, *Perception Psychophysics*, Vol.9, No.2, pp.237–24 (1970).

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

[9] Dhamija, R.: Hash Visualization in User Authentication, *Proc. Human Factors in Computing Systems*, pp.279–280 (2000).

[10] Hayashi, E., Hong, J.I. and Christin, N.: Educated Guess on Graphical Authentication Schemes: Vulnerabilities and Countermeasures, *Proc. 5th Symposium on Usable Privacy and Security*, Article No.25 (2009).

[11] Hayashi, E., Hong, J.I. and Christin, N.: Security through a Different Kind of Obscurity: Evaluating Distortion in Graphical Authentication Schemes, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.2055–2064 (2011).

[12] Takada, T. and Koike, H.: 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).

[13] Takada, T., Onuki, T. and Koike, H.: A User Evaluation Study about Security and Usability of Awase-E, *IPSJ Journal*, Vol.47, No.8, pp.2602–2612 (2006) (in Japanese).

[14] Harada, A., Isarida, T., Mizuno, T. and Nishigaki, M.: A User Authentication System Using Schema of Visual Memory, *IPSJ Journal*, Vol.46, No.8, pp.1997–2013 (2005) (in Japanese).

[15] Miyachi, T., Hasegawa, M., Tanaka, Y. and Kato, S.: A Study on a Graphical Password Using a Feature of Human Visual System, *IEICE Trans. Inf. Syst.*, Vol.J94-D, No.9, pp.1513–1521 (2011) (in Japanese).

[16] Anzai, T. and Iyoda, M.: Proposal of Personal Authentication Technique Based on Images, *The Journal of the Institute of Image Electronics Engineers of Japan*, Vol.38, No.5, pp.608–613 (2009) (in Japanese).

[17] Schneegass, S., Steimle, F., Bulling, A., Alt, F. and Schmidt, A.: SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication, *Proc. 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp.775–786 (2014).

[18] Huh, J.H., Kim, H., Bobba, R.B., Bashir, M.N. and Beznosov, K.: On the Memorability of System-generated PINs: Can Chunking Help?, *Proc. 11th Symposium on Usable Privacy and Security*, pp.197–209 (2015).

[19] von Zezschwitz, E., Dunphy, P. and Luca, A.D.: Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices, *Proc. 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pp.261–270 (2015).

[20] Lifemedia, Inc.: A survey on Photo (online), available from ⟨http://research.lifemedia.jp/2014/07/140730_photo.html⟩ (accessed 2014-07-30).

[21] Smeulders, A.W.M., Worring, M., Santini, S., Gupta, A. and Jain, R.: Content-Based Image Retrieval at the End of the Early Years, *IEEE Trans. Pattern Analysis and Machine Intelligence*, pp.1349–1380 (2000).

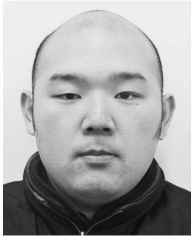
[22] Hiroike, A.: Similarity-based Image Retrieval System “EnraEnra”, *Journal of the Japanese Society for Artificial Intelligence*, Vol.29, No.5, pp.430–438 (2014) (in Japanese).

[23] Takada, T.: fakePointer: A User Authentication Scheme that Makes Peeping Attack with a Video Camera Hard, *IPSJ Journal*, Vol.49, No.9, pp.3051–3061 (2008) (in Japanese).

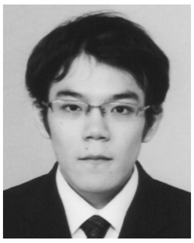
[24] Kita, Y., Okazaki, N., Nishimura, H., Torii, H., Okamoto, T. and Park, M.: Implementation and Evaluation of Shoulder-Surfing Attack Resistant Users, *IEICE Trans. Inf. Syst.*, Vol.J97-D, No.12, pp.1770–1784 (2014) (in Japanese).

[25] Ritter, D., Schaub, F., Walch, M. and Weber, M.: MIBA: Multitouch Image-Based Authentication on Smartphones, *Proc. CHI'13 Extended Abstracts on Human Factors in Computing Systems*, pp.787–792 (2013).

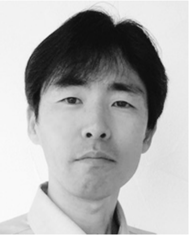
[26] Takada, T. and Kokubun, Y.: Extended PIN Authentication Scheme Allowing Multi-Touch Key Input, *International Journal of Pervasive Computing and Communications*, pp.276–290 (2014).



Masafumi Kosugi received his B.E. and M.E. degrees from Tokai University in 2012 and 2014, respectively, and has been engaged in Yahoo Japan Corporation since 2015. His research interests include image processing, music information processing, information security, and disaster mitigation information systems.



Tsuyoshi Suzuki received his B.E. degree from Tokai University in 2015. He is currently a Master course student in the Graduate School of Engineering at Tokai University. His research interests include image processing, and information security.



Osamu Uchida received his B.E. degree from Meiji University in 1995, M. Info. Sci. degree from Japan Advanced Institute of Science and Technology in 1997, and Ph.D. from University of Electro-Communications in 2000. From 2000 to 2002, he was a research associate at Kanagawa Institute of Technology. He joined Tokai University in 2002, and since 2007, he has been an associate professor at the Department of Human and Information Science, Tokai University. He was a visiting researcher at the Department of Information and Computer Sciences, University of Hawaii at Manoa in 2014. His research interests include information theory, image processing, Internet technology, information security, natural language processing, and disaster mitigation information systems. He received a prize for his contribution to the activities of the IIEEJ (The Institute of Image Electronics Engineers of Japan). He is a member of IEEE, IEICE, IIEEJ, JSAI (The Japanese Society for Artificial Intelligence), NLP (The Association for Natural Language Processing), and JASDIS (The Japan Society for Disaster Information Studies). Since 2012, he has been a vice editor in chief of the IIEEJ.

Hiroaki Kikuchi received his B.E., M.E. and Ph.D. degrees from Meiji University in 1988, 1990 and 1994, respectively. After working in Fujitsu Laboratories Ltd. from 1990, and in Tokai University from 1994, he joined Meiji University in 2013. He is currently a professor at the Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences, Meiji University. He was a visiting researcher at the School of Computer Science, Carnegie Mellon University in 1997. His main research interests are fuzzy logic, cryptographic protocol, network security, and privacy-preserving data mining. He received the Best Paper Award for Young Researcher of the Japan Society for Fuzzy Theory and Intelligent Informatics in 1990, the Best Paper Award for Young Researcher of IPSJ National Convention in 1993, the Best Paper Award of the Symposium on Cryptography and Information Security in 1996, the IPSJ Research and Development Award in 2003, the Journal of Information Processing (JIP) Outstanding Paper Award in 2010, and the IEEE AINA Best Paper Award in 2013. He is a member of IEEE, ACM, IEICE and SOFT (Japan Society for Fuzzy Theory and Intelligent Informatics). He is a fellow of IPSJ.