International Journal of Computer Science and Applications
©Technomathematics Research Foundation
Vol. 9, No. 3, pp. 20 – 36, 2012

PASS-IMAGE AUTHENTICATION METHOD TOLERANT TO RANDOM AND VIDEO-RECORDING ATTACKS

YUTAKA HIRAKAWA

Shibaura Institute of Technology,
3-7-5, Toyosu, Koto-ku, Tokyo, 135-8548 Japan
hirakawa@sic.shibaura-it.ac.jp

MOTOHIRO TAKE

Shibaura Institute of Technology,
3-7-5, Toyosu, Koto-ku, Tokyo, 135-8548 Japan
m108075@sic.shibaura-it.ac.jp

KAZUO OHZEKI

Shibaura Institute of Technology,
3-7-5, Toyosu, Koto-ku, Tokyo, 135-8548 Japan
ohzeki@sic.shibaura-it.ac.jp

User authentication is widely used in many Internet services and is also used by automatic teller machines (ATMs). Recently, there has been an increase in the ATM password thefts using small charge-coupled device cameras. This study discusses a user authentication method in which graphical passwords, instead of alphanumeric ones as, are used to mitigate observation attacks. Several techniques for password authentication have been discussed in various studies. However, there has not been sufficient research on authentication methods that use pass-images instead of pass-texts. This study proposes a user authentication method that is tolerant to serious attacks when a user's pass-image selection operation is video recorded twice. In addition, usage guidelines recommending eight pass-images are proposed, and the corresponding security strength is evaluated.

Keywords: User authentication; graphical password; random attack; video-recording attack.

1. Introduction

User authentication is widely used in many Internet services and is also used in all automatic teller machines (ATMs). A four-digit personal identification number (PIN) or a textual password is commonly used for user authentication. In Japan during October 2005, ATM passwords were stolen using a wireless charge-coupled device (CCD) camera recording. The criminal group had set up many cameras at various ATMs in Tokyo. The bank's investigation revealed that user activity was captured by hidden cameras at more than 60 ATMs in the Tokyo metropolitan area [Mitsubishi(2005)] [Yokohama(2005)].

Biometric authentication technology and sneak shot camera detection technology are possible solutions [Une(2005)][Banno(2007)][Secom(2007)][NEC(2006)] to this problem. However, because there are many ATMs installed around the world and the aforementioned solutions require additional equipment, these are not cost-effective solutions.

In this study, we discuss an authentication method that uses pass-images instead of a textual password. In Japan, alphabetic characters are commonly used as authentication passwords for Internet services. However, alphabetic characters are not so familiar to the elderly people and teenagers. Thus, authentication using pass-images might become a widely accepted method. In addition, this study discusses an authentication method that is tolerant to video-recording attacks. The security of the proposed authentication method is evaluated against random and video-recording attacks.

This study is organized as follows. Section 2 describes the requirements of the pass-image authentication method. Section 3 briefs the existing techniques. Section 4 explains the proposed authentication method and section 5 reports its security evaluation. Section 6 discusses the usability of the method. Section 7 describes the usage guidelines and section 8 summarizes the study.

2. Requirements

We consider the use of pass-images in ATMs. The security of the authentication method is evaluated against random and video-recording attacks as follows.

(1) Random attack

This is an attack that attempts to bypass the authentication process using a random operation. Because a four-digit PIN is used in ATMs, we adopt a success rate of less than 1/10000 as a requirement for a random attack.

(2) Video-recording attack

Presently, many cell phones and handheld devices are equipped with a camera. In addition, wireless CCD cameras are inexpensive. Therefore, the risk of sneaking a shot is increasing.

In an ATM, password authentication may be required more than once; for example, multiple bank transfers. Therefore, we should be concerned about multiple video recordings of the pass-image selection operation.

The success rate of video-recording attacks is not standardised. However, because the success rate of a random attack is 1/10000, we adopt the same rate for a video-recording attack.

3. Related Works

Few studies about authentication methods that use pass-texts have discussed observation attacks [Roth(2004)][Zhao(2007)][Takada(2007)][Takada(2008)][Sakurai(2004)].

In [Roth(2004)], a password authentication technique called PIN Entry, which uses numeric key entry, is proposed. On the display, a white or black background is randomly shown. A user does not designate a password, but selects white or black as the password's background colour. To enter a password entry of one digit, a user designates the background colour by a different colour pattern four times. This method is safe against shoulder surfing; however, if the input operation is video recorded, the password can be easily discovered.

In [Zhao(2007)], an interface for textual passwords, called S3PAS, is proposed. Many characters are displayed on the interface. A user designates three points where a pass-character is included in the triangle. This method is also safe against shoulder surfing; however, if the input operation is video recorded, the password can still be easily discovered.

In [Takada(2007)] and [Takada(2008)], an authentication method called 'fake pointer', which uses numeric key entry, is proposed. In this method, a disposable 'answer selection information' must be retrieved before each authentication. This answer selection information specifies a background mark such as a diamond, square, circle, or octagon for the displayed numeric password. At the time of authentication, a user presses the enter button that adjusts the password according to the background mark. If the answer-selection information can be safely retrieved before each authentication, it is tolerant to video-recording attacks by recording twice. However, the studies do not discuss how to safely retrieve the answer selection information.

A textual password entry interface called mobile authentication is proposed in [Sakurai(2004)]. In this method, all the selectable texts are arranged in a square. Each text has a background colour. Each password is alphanumeric, and the texts are arranged in a 10 × 5 square, in which 10 colours are used. Each colour appears only once in each row. The colour pattern of a row is the permutated colour pattern of another row. In this method, a user provides a password and the correct background colours beforehand. During password entry, the user changes the background colour of a pass-character until it matches the correct background colour, and then presses the enter button. Although this technique has the limitation that all available texts must be displayed on the authentication interface, it is secure against video-recording attacks by recording twice.

Next, we review the methods in which pass-images instead of textual passwords are used.

In [Dhamija(2000)], a method called Déjà vu is proposed. In this method, a user preselects five pass-images from numerous images produced by the computer. During authentication, a user selects a pass-image from 25 images displayed on the screen. However, a mechanically produced image is difficult for a user to memorize. The techniques described in [Dhamija(2000)] are not safe against shoulder surfing because a user specifies a pass-image using a keyboard or mouse.

In the AWASE-E method [Takada(2003)], 25 images including one correct pass-image are displayed on the screen similar to those described in the methods in [Dhamija(2000)]. However, this method also allows the display of a screen on which no pass-image is present. If the pass-image is not present on the screen, a user must select the 'no pass-image button'. Although this technique is highly ambiguous, its security against sneaking a shot is insufficient.

To the best of our knowledge, there is no report which includes enough discussion on a pass-image authentication method tolerant to video-recording attacks, where user operations are video recorded multiple times.

4. Proposed Authentication Method

4.1. *Requirements for authentication interface*

An authentication method is expected to be tolerant to video-recording attacks. Although a user's selection operation of pass-images is video recorded, many pass-image candidates must exist when an attacker analyzes the recorded video. To this end, providing secret information beforehand, such as the correct position of each pass-image in the interface, is one solution, which is analogous to the technique used in [Sakurai(2004)]. However, it increases the amount of information that a user needs to memorize.

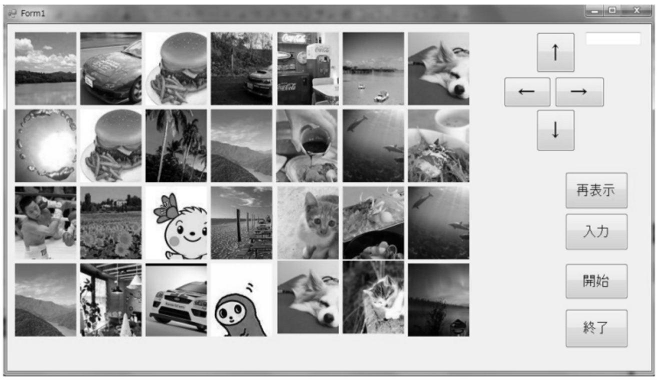
Thus, an authentication method must satisfy the following requirements:

- It should have sufficient ambiguity in pass-image selection operation in case the operation is video recorded and analysed.
- Any additional information except pass-images should not be asked beforehand.

4.2. *Authentication interface*

When a textual password is used, each pass-character is chosen from 26 alphabetic characters. In this study, pass-images are used instead of characters. We assume that there are N different images and that each pass-image is chosen from these images. The password generally consists of a number of pass-images. We use L to indicate the length of pass-images. For instance, when the password is composed of eight pass-images, we say that the length of the pass-images is eight.

We propose the authentication interface shown in Fig. 1. In the authentication interface, depth (D) × width (W) images are randomly selected and displayed.



A display example with 4 × 7 images

Fig. 1. Authentication Interface

For the authentication operation, a user presses the following buttons:

- Move button

  If a pass-image is displayed and a user wants to move it, a user uses the arrow button to move the image.

- Flash button
  If no pass-image is displayed, a user presses the flash button to redisplay a new set of images.
- Selection button
  If a pass-image is suitably positioned, a user presses the selection button. The system then shows a new display for the next pass-image selection.

The selection operation should be done for each pass-image. When the password is composed of L pass-images, the selection operation is repeated L times.

4.3. *Row restriction of each pass-image*

In this study, we restrict each pass-image location in the authentication operation assuming the number of rows in the interface to be four. Following are the rules:

- The first pass-image is located at any place on the display. Assume that a user presses the selection button to place the first pass-image in the d_1-th row on the display.
- For the k-th ($k \leq 4$) pass-image, a user can press the selection button to place the k-th pass-image in the d_k-th row, where d_k is not equal to $d_1, d_2, \ldots, d_{k-1}$.
- For the k-th ($k > 4$) pass-image, a user must press the selection button to place the pass-image in the d_{k-4}-th row.

Following the above rule, the first four pass-images must be placed in different rows. The fifth pass-image must be placed in the same row as the first one. The sixth pass-image must be placed in the same row as the second one and so on. The authentication system judges that a user is the authentic user when each L pass-image on the interface follows the aforementioned rules.

These rules are intended to make the method tolerant to random attacks while satisfying the requirements for the authentication interface. In addition, the aforementioned row restriction does not increase the amount of information that a user needs to memorize. The position of each pass-image is not recorded beforehand. A user selects suitable pass-image positions freely, following the aforementioned rules.

5. Security Evaluation

There are different ways to evaluate the authentication using pass-images. If L pass-images are selected using a user's favourite story, the order of the pass-image is important and each pass-image has its own order. If the user selects his/her favourite L pictures randomly, the order of the pass-images is not important.

In our evaluation, we consider the ordered pass-image and the non-ordered pass-image schemes as follows.

- Ordered pass-image
  The number of the pass-images is L. A user selects L pass-images and a sequence of pass-images is registered beforehand. Authentication must be achieved using the registered pass-image sequence.

- Non-ordered pass-image

  A user selects and registers L pass-images beforehand. A user can select L pass-images in random order. Authentication must be achieved L times with each different pass-image.

5.1. *Security against random attacks*

(1) Ordered pass-image

We assume that each pass-image is chosen from N different images. If N is large enough, the success probability of a random attack is very small.

Figs. 2, 3 and 4 show the success probabilities of random attacks. Each value is a mean value of the simulation conducted one million times.

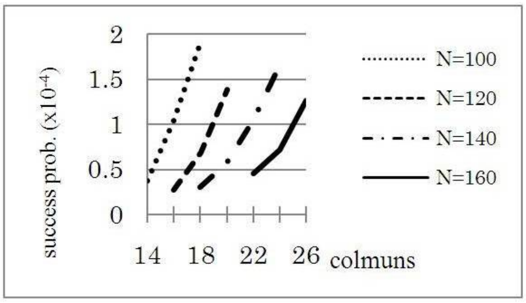


Fig. 2. Success probability of random attacks (L = 7)

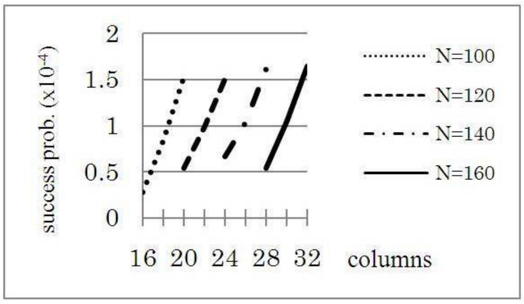


Fig. 3. Success probability of random attacks (L = 8)

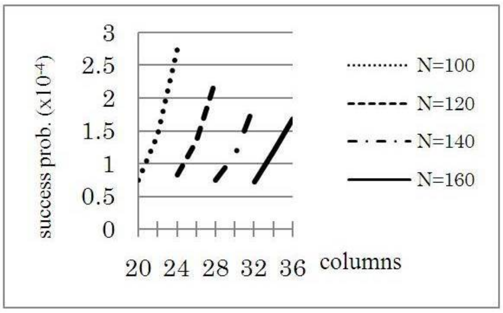


Fig. 4. Success probability of random attacks (L = 9)

The number of columns in the authentication interface and the pass-image length vary in the evaluation. The number of rows in the interface is fixed to four. When the number of columns increases, the number of images on the display also increases, thus increasing the success probability of random attacks.

A safe range of the number of columns against random attacks is summarized in Table 1. In the Table, each value is the maximum number of columns in which the success probability of random attacks does not exceed 1/10000.

Table 1. Safety range of columns

	L = 7	L = 8	L = 9
N = 160	~25	~29	~35
N = 140	~20	~25	~29
N = 120	~19	~22	~24
N = 100	~15	~18	~20

(2) Non-ordered pass-image

Figs. 5, 6 and 7 show the success probabilities of random attacks. Each value is also a mean value of the simulation conducted one million times.

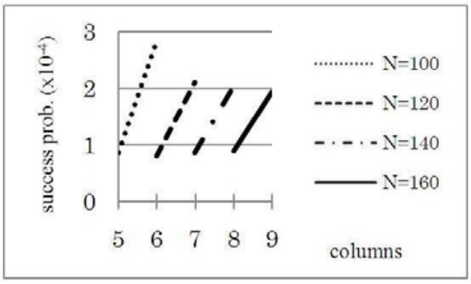


Fig. 5. Success probability of random attacks (L = 7)

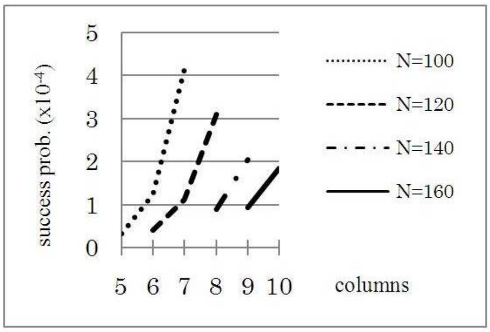


Fig. 6. Success probability of random attacks (L = 8)

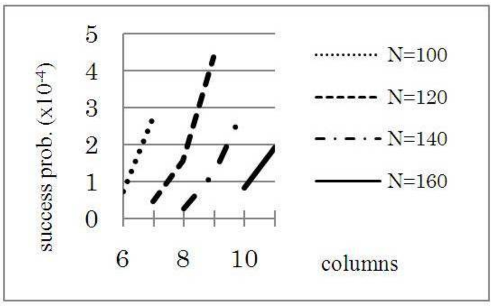


Fig. 7. Success probability of random attacks (L = 9)

The safe range of the number of columns in the authentication interface against random attacks is summarized in Table 2. Tables 1 and 2 indicate that the tolerance to random attacks using non-ordered pass-images is weaker than that using ordered pass-images. Authentication using non-ordered pass-images accepts any order of correct pass-images; in other words, it accepts a variety of pass-image sequences. Thus, the tolerance to random attacks is weaker.

In both tables, each value is the maximum number of columns in which the success probability of random attacks does not exceed 1/10000.

Table 2. Safe range of columns

	L = 7	L = 8	L = 9
N = 160	~8	~9	~10
N = 140	~7	~8	~8
N = 120	~6	~6	~7
N = 100	~5	~5	~6

5.2. *Video-recording attacks*

Video-recording attacks are quite serious: multiple authentication operations are assumed to be recorded, and it is possible to narrow down the pass-image candidates for attackers. In this study, we assume that two different authentication operations are recorded. We denote them as s_{11}, s_{12}, …, s_{1L} and s_{21}, s_{22}, …, s_{2L}, where L is the length of the pass-image sequence. For example, these authentication operations could be recorded on two successive days, and s_{12} would indicate the screen shot of yesterday's second pass-image selection. Also, s_{22} would indicate the screen shot of today's second pass-image selection.

Attackers analyze videos and attempt to obtain the pass-images as follows:

(1) Ordered pass-images

When ordered pass-images are used, the first pass-image must appear in the first authentication. Let the shots of the authentication interface in the first pass-image selection of each authentication be s_{11} and s_{21}. In both the shots, the first pass-image must appear. Similarly, the second pass-image must be included in both s_{12} and s_{22}. In this way, attackers analyze video and attempt to obtain the pass-images. If a sequence of the images obeys the following conditions, it is a possible pass-image candidate:

1) The sequence of the pass-images consists of L images. It is described as c_1, c_2, .., c_L.

2) The correct pass-image c_k must appear in both s_{1k} and s_{2k}.

3) For each image involved in the sequence of the pass-images, row restriction is satisfied for the first and second set of operations.

Through the aforementioned analysis, attackers may obtain several ordered pass-image sequences whose length is L. When attackers attempt to obtain the correct sequence of the pass-images, they will attempt each possible pass-image sequence. Thus, it is considered to satisfy the requirements described in section 2 when more than 10000 possible pass-image sequences exist.

(2) Non-ordered pass-images

When non-ordered pass-images are used, a candidate for the pass-image sequence must satisfy the following conditions:

1) The sequence of the pass-images consists of L images. It is described as $c_1,c_2,…,c_L$.

2) When an image from $c_1,c_2,…,c_L$ appears in $s_{11},s_{12},…,s_{1L}$ in this order, an image from $c_1',c_2',…,c_L'$ must appear in $s_{21},s_{22},…,s_{2L}$ in the order where $c_1',c_2',…,c_L'$ is a permutation of $c_1,c_2,…,c_L$.

3) For each image involved in $c_1,c_2,…,c_L$, row restriction is satisfied for the first set of operations $s_{11},s_{12},…,s_{1L}$. In addition, for each image involved in $c_1',c_2',…,c_L'$, row restriction is satisfied for the second set of operations $s_{21},s_{22},…,s_{2L}$.

Through the aforementioned analysis, attackers obtain several ordered pass-image sequences whose length is L. When attackers attempt to obtain the correct sequence of the pass-images, they use each possible pass-image sequence. However, assume two different pass-image sequences c_1, c_2, …, c_L and c_1', c_2', …, c_L', where $c_1',c_2',…,c_L'$ is a permutation of $c_1,c_2,…,c_L$. When attackers confirm that c_1, c_2, …, c_L is not a correct sequence of the pass-images, they need not attempt $c_1',c_2',…,c_L'$, because the order of the pass-images is not important in this case, and $c_1',c_2',…,c_L'$ is not a correct sequence of the pass-images. Thus, it is considered to satisfy the requirements described in section 4 when more than 10000 different pass-image candidates exist. In this context, candidates do not refer to sequences but to sets.

5.3. *Security against video-recording attacks*

(1) Security evaluation for ordered pass-images

Figs. 8, 9 and 10 show the number of pass-image candidates obtained through video analysis. Each value is a mean value of the simulation conducted 100 times.

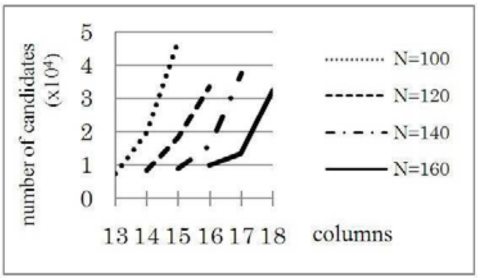


Fig. 8. Number of pass-image candidates (L = 7)

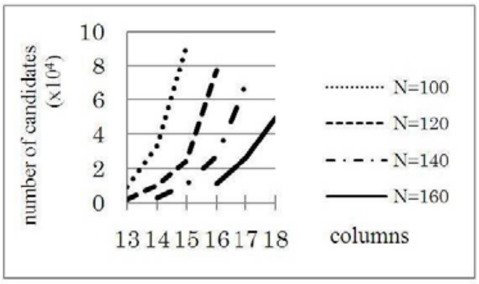


Fig. 9. Number of pass-image candidates (L = 8)

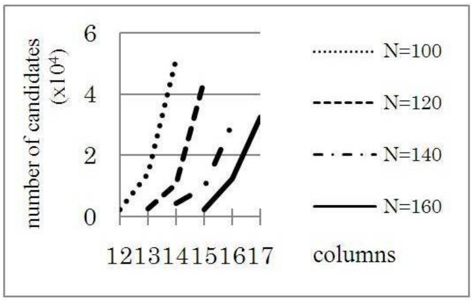


Fig. 10. Number of pass-image candidates (L = 9)

The results are briefly summarized in Table 3. For example, when the pass-image length is eight and the total number of images is 160, 16 or more columns are required in the authentication interface for the method to be tolerant to video-recording attacks.

Table 3. Safe range of columns

	L = 7	L = 8	L = 9
N = 160	17~	16~	16~
N = 140	16~	15~	16~
N = 120	15~	14~	14~
N = 100	14~	14~	13~

(2) Security evaluation for non-ordered pass-images

Figs. 11, 12 and 13 show the number of pass-image candidates obtained through video analysis. Each value is a mean value of the simulation conducted 100 times.

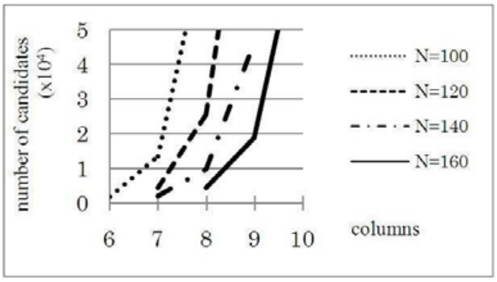


Fig. 11. Number of set of pass-image candidates (L = 7)

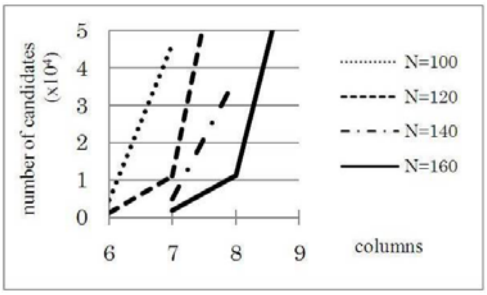


Fig. 12. Number of set of pass-image candidates (L = 8)

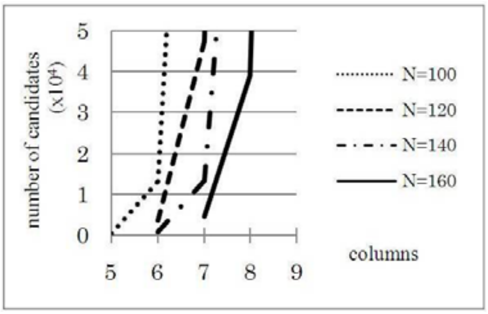


Fig. 13. Number of set of pass-image candidates (L = 9)

The results are summarized in Table 4. For example, when the pass-image length is eight and the total number of images is 160; eight or more columns are required in the authentication interface for the method to be tolerant to video-recording attacks. The numbers of columns are rather small compared with Table 3. For example, when the length of the pass-image is eight, a pass-image candidate must appear in the same order in twice the operations for ordered pass-images. On the other hand, the authentication system accepts many pass-image sequences consisting of the same eight pass-images for non-ordered pass-images. Thus, even if the authentication interface includes a small number of images (columns), many pass-image candidates exist.

Table 4. Safe range of columns

	L = 7	L = 8	L = 9
N = 160	9~	8~	8~
N = 140	9~	8~	7~
N = 120	8~	7~	7~
N = 100	7~	7~	6~

5.1. *Security against both types of attacks and discussion*

The range of columns in the authentication interface for acceptable tolerance to both types of attacks is shown in Tables 5 and 6.

Table 5. Safe range of columns (ordered pass-images)

	L = 7	L = 8	L = 9
N = 160	17 ~ 25	16 ~ 29	16 ~ 35
N = 140	16 ~ 20	15 ~ 25	16 ~ 29
N = 120	15 ~ 19	14 ~ 22	14 ~ 24
N = 100	14 ~ 15	14 ~ 18	13 ~ 20

Table 6. Safe range of columns (non-ordered pass-images)

	L = 7	L = 8	L = 9
N = 160	-	8 ~ 9	8 ~ 10
N = 140	-	8	7 ~ 8
N = 120	-	-	7
N = 100	-	-	6

The values in Table 5 are higher than those in Table 6, which implies that authentication with ordered pass-images requires many columns in the interface for the method to be tolerant to video-recording attacks. Many columns indicate a wide interface that is considered unsuitable for use.

Authentication with non-ordered pass-images is considered to be superior to that with ordered pass-images in terms of the interface.

6. Usability of the Method

In this section, we evaluate and discuss the usability of the proposed pass-image authentication method. We asked our colleagues to use the authentication method. We discovered that some colleagues found the selection and memorizing of eight images to be a difficult task.

If photographs captured by each user are used as pass-images, memorizing them is much easier, but it is known that this poses a security concern because it is possible to narrow down the pass-image candidates by paying attention to the photographer's preference and the conditions under which the photographs were taken.

Another solution is to memorize the images associated with a specific story. However, it is difficult to choose a comprehensive story using just eight images.

For the pass-image authentication, it is necessary to collect many pictures. Pictures may be classified into several categories. If a user selects two pictures in each category, this is considered to be a relatively straightforward task for most users. Moreover, to select some image pairs regardless of the category may be acceptable for users. For example, after imaging a story 'after 5 o'clock in the afternoon, go to a restaurant by jet and eat seafood', a user can select two photo pairs such as {office building photo, night-scene photo}, {jet photo, seafood photo}.

7. Usage Guidelines

We consider the following two usage guidelines (UG) for the proposed method:

UG 1:

- The length of the pass-image sequence is eight.
- Four category images are used for authentication. A user registers two pass-images in each category, beforehand.
- For authentication, two pass-images in the same category are continuously used. Thus, 2k-th and (2k + 1)-th pass-images must fall in the same category.
- Row restriction for the pass-images must be satisfied.
- The attackers have the same information as normal users. Therefore, they know the correct category of each image.

UG 2:

- The length of the pass-image sequence is eight.
- A user registers four different pass-image pairs, beforehand, where each pair consists of two pass-images.
- For authentication, two pass-images in the pair are continuously used. Thus, 2k-th and (2k + 1)-th pass-images must fall in the same pair.
- Row restriction for the pass-images must be satisfied.
- The attackers have the same information as normal users. However, they do not have any information on pass-image pairs which are personally defined by each user.

Assume {a1, a2}, {b1, b2}, {c1, c2} and {d1, d2} are pairs of user selected pass-images. In UG1, a1 and a2 must be involved in the same category. On the other hand, in UG2, a1 and a2 must be involved in the pair personally designated by a user. The same holds for b1 and b2, c1 and c2 or d1 and d2. For an intuitive description, the difference of UG1 and UG2 is whether the attackers know the correct category or not, when the term ‘pair’ is understood as a ‘category’ in UG2. In the authentication procedure, the order of a1 and a2 is irrelevant. This is a characteristic point compared with textual passwords.

The following are examples of acceptable pass-image sequences in the authentication process: <a1,a2,c2,c1,b1,b2,d2,d1> or <d1,d2,c1,c2,b1,b2,a2,a1> or ......

Table 7. Safe range of columns (UG1)

	Columns	Number of pass-image candidates $(\times 10^4)$	Success rate of random attacks [after pass-image insertion] $(\times 10^{-6})$	Number of operations per one selection [after correct pass-image insertion] (number of insertion)
N = 160	13	2.0	7 [49]	3.2 [2.8](1)
	14	4.9	26 [67]	3.1 [2.7](1)
	15	8.3	46	3.0
	16	37	74	2.9
	17	94	92	2.8
N = 140	13	4.4	27 [94]	3.0 [2.6](1)
	14	21	50	2.9
N = 120	11	1.1	25 [89]	3.0 [2.6](1)
	12	3.6	69	2.9

Table 8. Safe range of columns (UG2)

	Columns	Number of pass-image candidates $(\times 10^4)$	Success rate of random attacks [after pass-image insertion] $(\times 10^{-6})$	Number of operations per one selection [after correct pass-image insertion] (number of insertion)
N = 160	8	1.1	0 [75]	4.5 [2.8](3)
	9	6.8	0 [27]	4.1 [3.1](2)
	10	32	0 [51]	3.8 [2.9](2)
	11	180	2 [67]	3.6 [2.8](2)
	12	770	5 [24]	3.4 [3.0](1)
	13	over 1000	12 [49]	3.2 [2.8](1)
	14	over 1000	23	3.1 [2.7](1)
	15	over 1000	41	3.0
	16	over 1000	72	2.9
N = 140	8	3.2	1 [32]	3.9 [3.0](2)
	9	19	3 [60]	3.6 [2.8](2)
	10	102	5 [76]	3.5 [2.7](2)
	11	317	7 [32]	3.3 [2.9](1)
	12	over 1000	20 [67]	3.1 [2.7](1)
	13	over 1000	40	3.0
	14	over 1000	66	2.9
N = 120	7	1.1	0 [37]	4.0 [3.0](2)
	8	12	2 [63]	3.6 [2.7](2)
	9	62	6 [21]	3.4 [2.9](1)
	10	210	16 [56]	3.2 [2.8](1)
	11	870	27 [93]	3.0 [2.7](1)
	12	over 1000	66	2.9
N = 100	7	4.0	3 [78]	33.6 [2.7](2)
	8	30	12 [47]	3.3 [2.8](1)
	9	210	30 [78]	3.0 [2.7](1)
	10	960	72	2.9

These usage guidelines are considered to be rather easy to follow; however, whether the authentication method following these guidelines is tolerant to both types of attacks is unclear.

The results of the security evaluation are shown in Tables 7 and 8. Each table shows a safe range of columns in the authentication interface for UG1 or UG2.

In both tables, the average button operation frequency is shown on the right. In Ku(2005), keystrokes per character (KSPC) on a mobile terminal are discussed and the operation frequency is considered as a measure to evaluate the user interface. Moreover, in this study, to reduce KSPC, the fourth insertion of a pass-image in the display is considered. This is achieved by inserting a pass-image in the authentication display when the display does not include a correct pass-image. The insertion is adopted when it is safe for random attacks. The number of KSPC can be reduced, and hence, can improve the usability.

In Table 7, for example, when the total number of images is 120 (N = 120) and the number of columns in the authentication display is 11, 11000 candidates are obtained by analyzing two sets of user's authentication operation videos. Also, it has a tolerance to random attacks because the success rate of random attacks is 70 × 10^{-6}. As this case has enough tolerance to random attacks, the pass-image insertion can be adopted. When one pass-image insertion is adopted, the tolerance to random attacks is still under 10^{-4} and KSPC can be reduced from 3.0 to 2.6. In Table 8, on the other hand, when N = 120 and the number of columns is 11, 870 × 10^{-4} candidates are obtained and KSPC is similar to that in Table 7.

In Tables 7 and 8, the values of tolerance to random attacks are similar. However, the values of tolerance to video-recording attacks are different. It is clear that information on the correct category is helpful to narrow down the pass-image candidates. Therefore, UG2 is considered to be superior to UG1 from the viewpoint of tolerance to video-recording attacks. From Table 8, it follows that in the cases of 10 or 12 columns with N = 140, and in the case of 9 columns with N = 100, the authentication is considered to have enough tolerance and usability.

So far, there was no published authentication method which satisfies the following:

- An authentication method that uses pass-images instead of textual passwords that is tolerant to random and video-recording attacks even if the operation is video recorded twice.
- A method whereby any additional information except pass-images should not be registered beforehand. In the case of other methods, sometimes users are required to memorize additional information, such as the correct place in the interface for each pass-image or pass-text.

A user's authentication operation must be satisfied by the 'row restriction' described in section 6. It may be also described in the authentication interface for the user's help. There is no need to memorize it.

8. Conclusion

This study proposed a user authentication method that uses pass-images instead of textual passwords. Fundamental characteristics of the authentication method are clarified, and the proposed authentication method is shown to be tolerant to random and video-recording attacks even if the operation is video recorded twice. The method does not require a user to register additional information except pass-images.

In the discussion of usability, usage guidelines for eight pass-images are proposed. In addition, it is shown to be tolerant to both random and video-recording attacks when authentication is used in accordance with the guidelines.

Detailed evaluations from the view point of the ease of memorizing pass-images and failure rates in accordance with spending time will be included in a further study.

References

Banno (2007) : The recent trend, the forensic science technology of the living body authentication technology, vol.12, no.1, pp.1-12

Dhamija, R.; Perrig, A. (2000) : Déjà vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, pp.45-58

Hirakawa, Y.; Take, T.; Ohzeki, K. (2011) : Pass-Image Authentication Method Tolerant to Video-Recording Attacks, FedCSIS2011, pp.767-773, 2011

Ku, W.; Tsaur, M. (2005) : A Remote User Authentication Scheme Using Strong Graphical Passwords, IEEE Local Computer Networks, LCN'05 (2005)

MacKenzie, I. S. (2002) : KSPC (keystrokes per Characters) as a Characteristic of Text Entry Techniques, Proc. Mobile HCI '02, LNCS-2411, Berlin, pp.405-416, Springer-Verlag (2002)

Mitsubishi Tokyo UFJ Bank (2005) : A bank report about that the camera was put on secretly at the ATM machine by some person. http://www.bk.mufg.jp/info/ufj/ufj_20051101.html

NEC (2006) : The service of the investigation of the detectaphone and the sneak shot receptacle http://www.necf.jp/solution-service/office/hiddenmic-camera/

Pering, T.; Sundar, M.; Light, J.; Want, R. (2003) : Photographic Authentication through Untrusted Terminals, IEEE Pervasive Computing, vol.2, no.1, pp.30-36

Roth, V.; Richter, K.; Freidinger, R. (2004) : A Pin-Entry Method Resilient Against Shoulder Surfing', CCS'04, pp.236-245

Sakurai, Yoshida, Bunaka, (2004) : Mobile authentication method, Computer Security Symposium 2004, pp.625-630

Secom Co., Ltd. (2006) : It begins' the ATM sneak shot damage prevention service 'by the offer' http://www.secom.co.jp/corporate/release/2006/nr_20060814.html

Sobrado, L.; Birget, J. (2002) : 'Graphical passwords', The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4

Suo, X.; Zhu, Y.; Owen, G. S. (2005) : Graphical Passwords: A Survey, 21st Annual Computer Security Applications Conference, ACSAC 2005

Takada, T.; Koike, H. (2003) : Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images, LNCS2795. Human-Computer Interaction with Mobile Devices and Services, pp.347-351

Takada, T. (2007) : fakePointer2: The proposal of the user interface to improve safety to the peep attack about the individual authentication, Cryptography and Information Security Symposium, SCIS2007

Takada, T. (2008) : fakePointer: The authentication technique which has tolerance to video recording attacks', IPSJ transaction, vol.49, no.9, pp.3051-3061

Une, M.; Matsumoto, T. (2005) : About the fragilitas about the living body authentication: It studies mainly a fragilitas about the counterfeiting of a stigma by the finance, vol.24, no.2, pp.35-84

Yokohama Bank (2005) : A bank report about that equipment for the sneak shot was installed in the unmanned agency (the ATM out of the store). http://www.boy.co.jp/info/pdf/9.pdf

Zhao, H.; Li, X. (2007) : S3PAS: A Scalable Shoulder-Surfing Resistant Textual-graphical Password Authentication Scheme', IEEE Advanced Information Networking and Applications Workshops 2007, pp.467-472