

# Pass-Image Authentication Method Tolerant to Video-Recording Attacks

Yutaka Hirakawa

Shibaura Institute of Technology 3-7-5, Toyosu, Koto-ku, Tokyo, 135-8548 Japan

Email: hirakawa@sic.shibaura-it.ac.jp

Motohiro Take

Shibaura Institute of Technology 3-7-5, Toyosu, Koto-ku, Tokyo, 135-8548 Japan

Email: m108075@sic.shibaura-it.ac.jp

Kazuo Ohzeki

Shibaura Institute of Technology 3-7-5, Toyosu, Koto-ku, Tokyo, 135-8548 Japan

Email: ohzeki@sic.shibaura-it.ac.jp

**Abstract**—User authentication is widely used in automatic teller machines (ATMs) and Internet services. Recently, ATM passwords have been increasingly stolen using small charge-coupled device cameras.

This article discusses a user authentication method in which graphical passwords instead of alphabetic ones are used as passwords in order for it to be tolerant to observation attacks. Several techniques for password authentications 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 article proposes a user authentication method that is tolerant to attacks when a user's pass-image selection operation is video recorded twice. In addition, usage guidelines recommending eight pass-images are proposed, and its security is evaluated.

## I. INTRODUCTION

User authentication is widely used in automatic teller machines (ATMs) and many Internet services. A four-digit personal identification number (PIN) or a textual password is commonly used for user authentication. In Japan in October 2005, an ATM password was 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 operation was captured by hidden cameras at more than 60 ATMs in the metropolitan area [1][2].

Biometric authentication technology and sneak shot camera detection technology are possible solutions [3][4][5][6] to this problem. However, because there are many ATMs installed around the world and the aforementioned solutions require additional equipment, the problem is still not solved.

In this article, 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 elderly and younger people. Thus, authentication using pass-images might become a widely accepted method. In addition, this article 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.

The remainder of this article is organized as follows: Chapter II describes the requirements of the pass-image authentication method. Chapter III briefs the existing techniques. Chapter IV explains the proposed authentication

method and Chapter V reports its security evaluation. Chapter VI discusses the usability of the method. Chapter VII describes the usage guidelines and Chapter VIII summarizes the article.

## II. REQUIREMENTS

We assume the use of pass-images at ATMs. The security of the authentication method is evaluated from the following two viewpoints:

### (1) Random attack

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

### (2) Video-recording attack

Currently, 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.

At an ATM, password authentication may be conducted more than once; for example, in the case of 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 for a video-recording attack.

## III. RELATED WORK

Few studies on the authentication methods that use pass-texts have discussed observation attacks [7][8][9][10][11][12].

In [7], 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 [8], an interface for the textual password called S3PAS is proposed. Many characters are displayed on the interface. A user designates three points where a pass-character is in-

cluded in the triangle. This method is also safe against shoulder surfing; however, if the input operation is video recorded, the password can be easily discovered.

In [9] and [10], an authentication method called fake-Pointer is proposed, which uses numeric key entry. 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 information.

A textual password entry interface called mobile authentication is proposed in [11]. 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  $10 \times 5$  square in which 10 colours are used. Each colour appears only once in each row. The colour pattern of a row is the permuted 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 restriction 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 [13], a method called Déjà vu is proposed. In this method, a user selects five pass-images beforehand from numerous images produced by the computer. During authentication, a user selects a pass-image from 25 images displayed on the screen. Because a mechanically produced image is difficult for a user to memorize, [14] proposes the use of facial images as pass-images.

The techniques described in [13] and [14] are not safe against shoulder surfing because a user specifies a pass-image using a keyboard or mouse.

In [15], a method using graphical passwords is proposed. This method is similar to that described in [8]. This method is ambiguous, and security evaluation against shoulder surfing is not sufficient.

In the AWASE-E method [16], 25 images including one correct pass-image are displayed on the screen similar to those described in the methods in [13] and [14]; 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 not sufficient.

Thus, there is no report on a pass-image authentication method tolerant to video-recording attacks where user operations are video recorded multiple times.

## IV. PROPOSED AUTHENTICATION METHOD

### A. 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 analyses the recorded video. To this end, providing secret information beforehand, such as correct position of each pass-image in the interface, is one solution, which is analogous to the technique used in [11]. 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.

### B. Authentication interface

When the password is “ffchopin”, it is an example of 8-length alphabetic password. Each character is chosen from 26 alphabetic characters. In this article, pass-images are used instead of characters. We assume there are  $N$  different images. And each pass-image is chosen from these  $N$  images. The password generally consists of number of pass-images. When the password is composed of eight pass-images, we use the description that the length of pass-images is eight. We use  $L$  to indicate the length of pass-images.

We proposed the authentication interface shown in Fig. 1. In the authentication interface, depth ( $D$ )  $\times$  width ( $W$ ) images are randomly selected and displayed.



A display example with 4 $\times$ 7 images

Fig. 1 Authentication Interface

For authentication operation, a user presses the following:

- 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.

### C. Row restriction of each pass-image

In this article, 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 placing 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 placing the  $k$ -th pass-image in the  $d_k$ -th row, where  $d_k$  is not equal to  $d_1, d_2, \dots, d_{k-1}$ .
- For the  $k$ -th ( $k > 4$ ) pass-image, a user must press the selection button placing the pass-image in the  $d_{k-4}$ -th row.

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.

## V. SECURITY EVALUATION

There are different ways to consider authentication using the 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 evaluation, we assume the following two schemes:

- 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. The 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. The authentication must be achieved  $L$  times with each different pass-image.

### A. 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 random attack is very small.

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

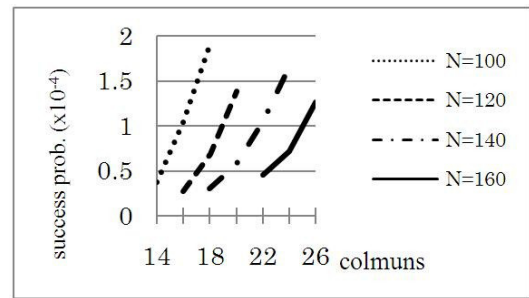


Fig. 2 Success probability of random attacks ( $L = 7$ )

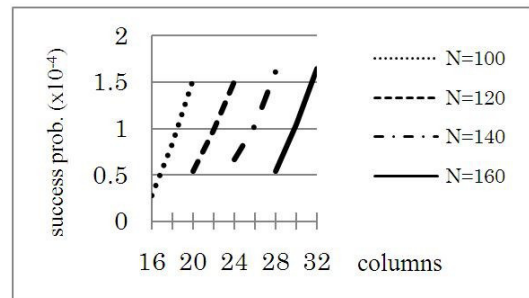


Fig. 3 Success probability of random attacks ( $L = 8$ )

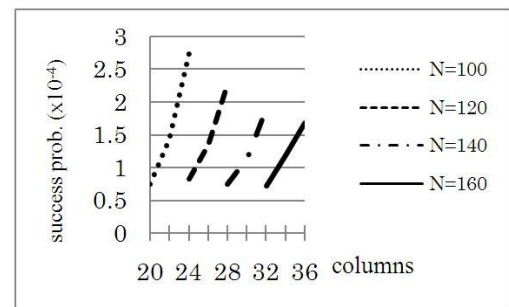


Fig. 4 Success probability of random attacks ( $L = 9$ )

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.

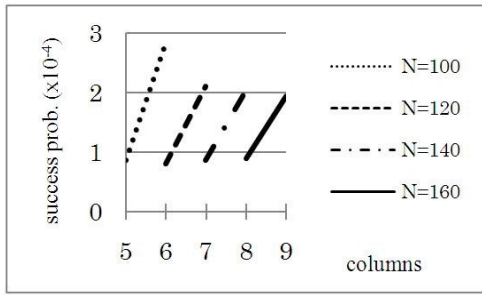
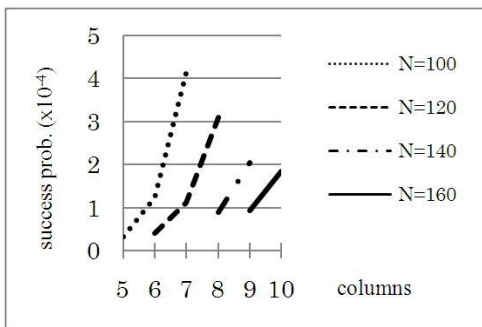
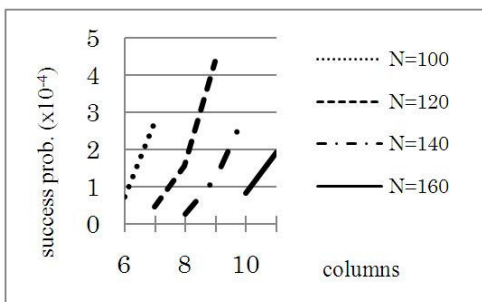
A safe range of the number of columns against random attacks is summarized in Table I. In the table, each value is the maximum number of columns in which the success probability of random attacks does not exceed  $1/10000$ .

TABLE I  
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 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 II. 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 II.  
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

## B. Video-recording attacks

Video-recording attack is very serious; attackers record users' password input operation by using video cameras. In addition, multiple authentication operations are assumed to be recorded. As the first step, we assume that two different authentication operations are recorded in this article. We denote them as  $s_{11}, s_{12}, \dots, s_{1L}$  and  $s_{21}, s_{22}, \dots, s_{2L}$ , where  $L$  is the length of the pass-image sequence. For example, these authentication operations could be recorded yesterday and today, respectively, and  $s_{12}$  would indicate the screen shot of yesterday's second pass-image selection.

Attackers analyse 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 analyse video and attempt to obtain the pass-images. If a sequence of the images follows 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  $c_1, c_2, \dots, c_L$ .
- 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 obtained 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. Thus, it is considered to satisfy the requirements described in Chapter II 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  $c_1, c_2, \dots, c_L$ .
- 2) When image  $c_1, c_2, \dots, c_L$  appears in  $s_{11}, s_{12}, \dots, s_{1L}$  in this order, image  $c'_1, c'_2, \dots, c'_L$  must appear in  $s_{21}, s_{22}, \dots, s_{2L}$  in the order where  $c'_1, c'_2, \dots, c'_L$  is a permutation of  $c_1, c_2, \dots, c_L$ .
- 3) For each image involved in  $c_1, c_2, \dots, c_L$ , row restriction is satisfied for the first set of operations  $s_{11}, s_{12}, \dots, s_{1L}$ . In addition, for each image involved in  $c'_1, c'_2, \dots, c'_L$ , row restriction is satisfied for the second set of operations  $s_{21}, s_{22}, \dots, s_{2L}$ .

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, assuming two different pass-image sequences  $c_1, c_2, \dots, c_L$  and  $c_1', c_2', \dots, c_L'$ , where  $c_1', c_2', \dots, c_L'$  is a permutation of  $c_1, c_2, \dots, c_L$ , when it is clarified that  $c_1, c_2, \dots, c_L$  is not a correct sequence of the pass-images, attackers need not try with  $c_1', c_2', \dots, c_L'$ , because the order of the pass-images is not important in this case, and  $c_1', c_2', \dots, c_L'$  is not a correct sequence of the pass-images. Thus, it is considered to satisfy the requirements described in Chapter IV when more than 10000 possible pass-image candidates exist.

### C. Security against video-recording attacks

#### (1) Security evaluation for ordered pass-images

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

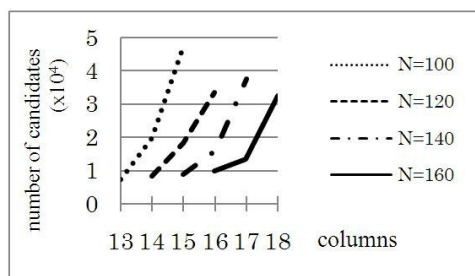


Fig. 8 Number of pass-image candidates (L = 7)

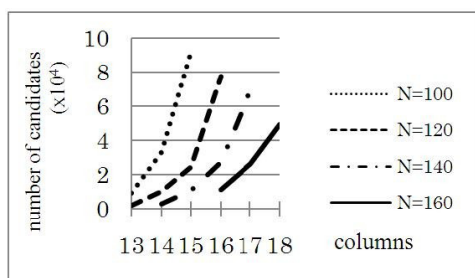


Fig. 9 Number of pass-image candidates (L = 8)

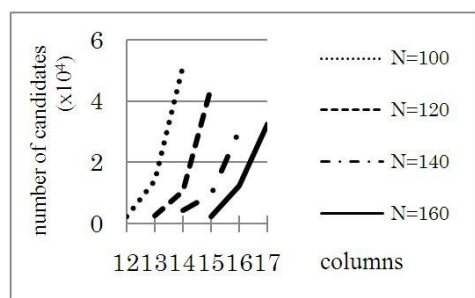


Fig. 10 Number of pass-image candidates (L = 9)

The results are briefly summarized in Table III. 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 III.  
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 the pass-image candidates obtained through video analysis. Each value is a mean value of the simulation conducted 100 times.

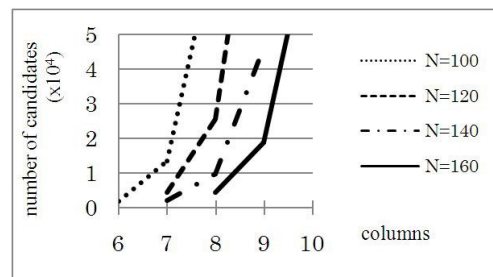


Fig. 11 Number of set of pass-image candidates (L = 7)

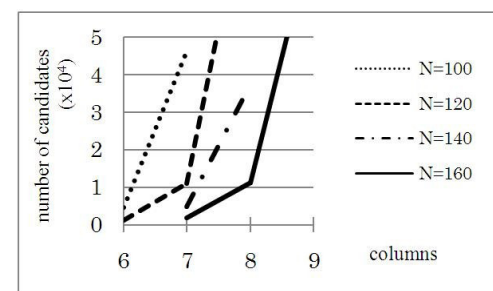


Fig. 12 Number of set of pass-image candidates (L = 8)

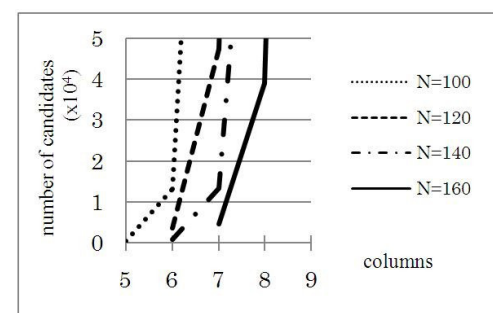


Fig. 13 Number of set of pass-image candidates (L = 9)

The results are summarized in Table IV. 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.

TABLE IV.  
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~

#### D. Security against both attacks and discussion

The range of columns in the authentication interface for the method to be tolerant to both types of attacks is shown in Tables V and VI.

TABLE V.  
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 VI.  
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 V are higher than those in Table VI, 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.

#### VI. USABILITY OF THE METHOD

In this section, we evaluate and discuss the usability of the proposed pass-image authentication method. We prepared several photo images in eight categories, which included photographs of animals, scenery, vehicles and food. We asked our colleagues to use the authentication method. We faced a difficulty when some colleagues found selecting and memorizing 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 there is a problem in security because it is possible to narrow down the pass-image candidates paying attention with photographer's preference and conditions of taking photographs.

Another solution is to memorize the images by using a story. However, this was ruled out in the discussion of the evaluation results in this article.

We attempt to solve this problem in the following section.

#### VII. USAGE GUIDELINES

Considering the suggestions of our colleagues, we introduced usage guidelines for the proposed method summarized as follows:

- The length of the pass-image sequence is eight pass-images.
- Four category images are used for authentication. A user selects two pass-images in each category.
- 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.

These usage guidelines are rather easy to follow; however, whether the authentication method following these guidelines is tolerant to both types of attacks is unclear. We assume that attackers have the same information as normal users; for example, they know the correct category of each image.

The results of security evaluation are shown in Table VII. It shows a safe range of columns in the authentication interface.

TABLE VII.  
SAFE RANGE OF COLUMNS

	columns	Number of pass-image candidates	Success rate of random attacks ( $\times 10^{-6}$ )	Number of operations per one selection
N = 160	10	$1.4 \times 10^4$	0	3.8
	11	$5.2 \times 10^4$	2	3.6
	12	$1.6 \times 10^5$	6	3.4
	13	$3.2 \times 10^5$	14	3.2
	14	$1.8 \times 10^6$	17	3.1
	15	$4.0 \times 10^6$	26	3.0
N = 140	16	$9.5 \times 10^6$	61	2.9
	10	$3.0 \times 10^4$	5	3.5
	11	$9.9 \times 10^4$	6	3.3
	12	$3.6 \times 10^5$	26	3.1
	13	$1.3 \times 10^6$	44	3.0
N = 120	14	$3.4 \times 10^6$	57	2.9
	15	$1.1 \times 10^7$	90	2.8
	9	$1.6 \times 10^4$	4	3.4
	10	$1.0 \times 10^5$	18	3.2
N = 100	11	$2.8 \times 10^5$	31	3.0
	12	$8.1 \times 10^5$	71	2.9
	9	$5.1 \times 10^4$	31	3.1
	10	$2.4 \times 10^5$	75	2.9

In the table, the average button operation frequency is shown on the right. In [19], keystrokes per character (KSPC) on a mobile terminal are discussed and the operation frequency is considered as a measure to evaluate the user interface.

For example, when 100 images are used (25 images for each category), authentication is tolerant to both random and video-recording attacks in the case of a 9- or 10-column and 4-row interface. Also, the value of KSPC is relatively small and easy to use.

Conventionally, there is no authentication method which satisfies followings:

- The authentication method, that uses pass-images instead of textual password, is tolerant to random and video-recording attacks even if the operation is video recorded twice.
- Any additional information except pass-images should not be registered beforehand. In a case of other method, 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 the "row restriction" described in Chapter IV. But it may be described in the authentication interface for user's help. It is no need to memorize it.

In this article, we use random selection and describe statistical data. In the case where  $N = 100$  and 4-row 10-column display is used in the authentication interface, the average number of pass-image candidates is  $2.4 \times 10^3$ , where the standard deviation is  $9.7 \times 10^4$ . Assuming the values as normally distributed, a 95% confidence interval is  $1.9 \times 10^4 \pm$  the mean value. A 99% confidence interval is  $2.6 \times 10^4 \pm$  mean value.

#### VIII. CONCLUSION

This article proposed a user authentication method that uses pass-images instead of textual password. 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.

#### REFERENCES

- [1] The Mitsubishi Tokyo UFJ bank, '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](http://www.bk.mufg.jp/info/ufj/ufj_20051101.html)
- [2] Bank of Yokohama, '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>

- [3] M. Une, T. Matsumoto, '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 (2005)
- [4] Banno, 'The recent trend, the forensic science technology of the living body authentication technology', vol.12, no.1, pp.1-12 (2007)
- [5] Secom Co., Ltd., 'It begins' the ATM sneak shot damage prevention service 'by the offer'  
[http://www.secom.co.jp/corporate/release/2006/nr\\_20060814.html](http://www.secom.co.jp/corporate/release/2006/nr_20060814.html)
- [6] NEC, 'The service of the investigation of the detecta-phone and the sneak shot receptacle'  
<http://www.necf.jp/solution-service/office/hidden-mic-camera/>
- [7] V. Roth, K. Richter, R. Freidinger, 'A Pin-Entry Method Resilient Against Shoulder Surfing', CCS'04, pp.236-245 (Oct 2004)
- [8] H. Zhao, X. Li, 'S3PAS: A Scalable Shoulder-Surfing Resistant Textual-graphical Password Authentication Scheme', IEEE Advanced Information Networking and Applications Workshops 2007, pp.467-472 (2007)
- [9] T. Takada, 'fakePointer: The authentication technique which has tolerance to video recording attacks', IPSJ transaction, vol.49, no.9, pp.3051-3061 (Sep 2008)
- [10] T. Takada, 'fakePointer2: The proposal of the user interface to improve safety to the peep attack about the individual authentication', Cryptography and Information Security Symposium, SCIS2007 (2007)
- [11] Sakurai, Yoshida, Bunaka, 'Mobile authentication method', Computer Security Symposium 2004, pp.625-630 (Oct 2004)
- [12] X. Suo, Y. Zhu, G. S. Owen, 'Graphical Passwords: A Survey', 21<sup>st</sup> Annual Computer Security Applications Conference, ACSAC 2005 (2005)
- [13] R. Dhamija and A. Perrig, 'Déjà vu: A User Study Using Images for Authentication', 9<sup>th</sup> Usenix Security Symposium, pp.45-58 (Aug, 2000)
- [14] RealUser: <http://www.realuser.com/>
- [15] L. Sobrado, J. Birget, 'Graphical passwords', The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4 (2002)
- [16] T. Takada, H. Koike, '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 (2003)
- [17] T. Pering, M. Sundar, J. Light, R. Want, 'Photographic Authentication through Untrusted Terminals', IEEE Pervasive Computing, vol.2, no.1, pp.30-36 (2003)
- [18] W. Ku, M. Tsaor, 'A Remote User Authentication Scheme Using Strong Graphical Passwords', IEEE Local Computer Networks, LCN'05 (2005)
- [19] I. S. MacKenzie, 'KSPC (keystrokes per Characters) as a Characteristic of Text Entry Techniques', Proc. Mobile HCI '02, LNCS-2411, Berlin, pp.405-416, Springer-Verlag (2002)