Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks

Y. Hirakawa

***Abstract*—The user authentication is widely used in the automatic teller machines (ATMs) and many Internet services. Recently, the crimes that ATM passwords are stolen using a small charge-coupled device (CCD) cameras have increased. In addition, in the mobile environment, there is a high risk of observation attacks that steal passwords, because many people possess devices such that camera-equipped mobile phones and miniature cameras.**

In this paper, we propose the authentication methods that are secure against the brute-force and video recording attacks. In the article, a video-recording attack is defined as an attacker's analysis of videos, in which a user's password entry operations are recorded once or twice, in order to obtain the user's password.

We propose a basic method and an improved method. In the basic method, a user must provide the correct entry position of each password beforehand. On the other hand, in the improved method, a user does not need to provide any information beforehand, other than the password.

The relative security of the two proposed methods is then evaluated.

***Index Terms*—Observation attacks, password authentication method.**

I. Introduction

User authentication is widely used in automatic teller machines (ATMs) and many Web services. A four-digit PIN or a text password is commonly used for user authentication. In Japan in October 2005, an ATM password was stolen by means of wireless charge-coupled device (CCD) camera recording. The criminal group had set up many cameras at ATMs in Tokyo. The bank's investigation revealed that shots were sneaked in more than 60 ATMs in the metropolitan area [1], [2].

Biometric authentication technology and sneak-shot camera-detection technology are methods [3]-[6] for solving this problem. However, because there are many ATMs installed in the country, and the above solutions require additional equipment, the problem is still not solved.

In this article, we propose an authentication method that is secure against observation attacks. Also, the security of the proposed authentication method is evaluated against brute-force and video-recording attacks.

The remaining sections of this article are organized as follows: Chapter II describes the requirements to the password authentication method. Chapter III describes existing techniques. Chapter IV describes the proposed basic method and its evaluation. Chapter V describes the proposed improved method and its evaluation. Chapter VI provides discussions, and Chapter VII summarizes this article.

Manuscript received May 22, 2013; revised August 13, 2013.

Y. Hirakawa is with the Information Science Engineering Department, Shibaura Institute of Technology, Tokyo, Japan (e-mail: hirakawa@shibaura-it.ac.jp).

II. Requirements

We assume the use of text passwords at ATM. The safety of the password is evaluated from the following two viewpoints:

A. Bruce-Force Attack

This denotes the success rate of a random attack. Because a PIN of four-digits is used so far at ATMs, we adopt as a requirement for a random attack, a success rate of less than 1/10000.

B. Video-Recording Attack

Currently, many cell phones and hand-held device contain a camera feature. In addition, wireless CCD cameras are inexpensive. Therefore, the risk of sneak shots is increasing.

Sometimes in an ATM, password authentication is conducted more than once. Therefore, we should be concerned about multiple video recordings of the password input operation.

There is no clear standard for the success rate of video-recording attacks. However, by consensus, the success rate of an attack is given as 1/10000, which indicates the safety of the random attack. In the same way, we adopt as a requirement for a video-recording attack, a success rate of less than 1/10000.

In this article, we assume that the password entry operation will be recorded twice on a video. Also, the requirement is interpreted that more than 10000 password candidates are obtained after analyzing the recorded videos.

III. Related Work

Some existing reports discuss shoulder surfing and other observation attacks.

A password authentication technique, called Pin-Entry, which uses numeric key entry, is proposed [7]. In the display, a white or black background is randomly displayed. A user does not designate a password, but selects white or black of as the password's background color. To enter a password entry of 1 digit, a user designates background color by the different color-pattern with four times. This method is safe against shoulder surfing. However, if the input operation is recorded on a video, the password can still be easily found out.

In [8], an interface for the text password 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 recorded on a video, the password can still be easily found out.

In [9] and [10], an authentication method called fakePointer 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 the background mark, such as diamond, square, circle, octagon, of the displayed numeric password. At the time of authentication, a user presses the enter button, which adjusts the password according to the background mark. If the "answer selection information" can be safely retrieved before each authentication, there is a tolerance to video attacks by recording twice. However, the mentioned studies do not discuss how to retrieve it safely.

A text-password entry interface called mobile authentication is proposed [11]. In this method, all the selectable texts are arranged in a square. Each text has a background color. For example, each password is numeric or alphabetic, and the texts are arranged in 6×6 square in which six colors are used. Each color appears only once in each row. The color pattern of a row is the permutated color pattern of another row. In this method, a user provides a password and the correct background colors beforehand. During password entry, the user changes the background color of a pass-character until it matches the correct background color, and then presses the enter button. This technique has the restriction that all available texts must be displayed in the square, but this method is secure against a video attack by recording twice. The comparison of the methods is described in the Discussions section.

Next, we review the methods which use a pass-image instead of a text-password.

In [13], a method called Déjà vu is proposed. In this method, a user selects five pass-images beforehand from thousands of images produced by the computer. During authentication, the 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 mentioned in [13] and [14] are not safe against shoulder surfing because the user specifies a pass-image during the authentication operation.

In AWASE-E method [15], 25 images including one correct pass-image, are usually displayed on the screen similar to the methods in [13] and [14], but this method allows the display of a screen in where there is no pass-image. If the pass-image is not present on the screen, a user must select the "no pass-image button". Although this technique increases ambiguity, its safety when sneaking a shot is not clear.

IV. The Basic Method and Its Security

A. Outline of the Basic Method

In the basic method, we assume that the following information is provided beforehand:

1) Password

In this article, a text password is discussed. The available text sets are numeric (10 characters), alphabetic (26 characters), or alphanumeric (36 characters).

2) Correct column position of the password

Let us assume that the password is "WAKE" and its correct column position is "1 4 4 1". This means that the correct position of "W" is the first column, the correct position of "A" is the fourth column, and so on. The proposed method is named Random Board. An illustration of its interface is shown in Fig. 1. The interface has the following features:

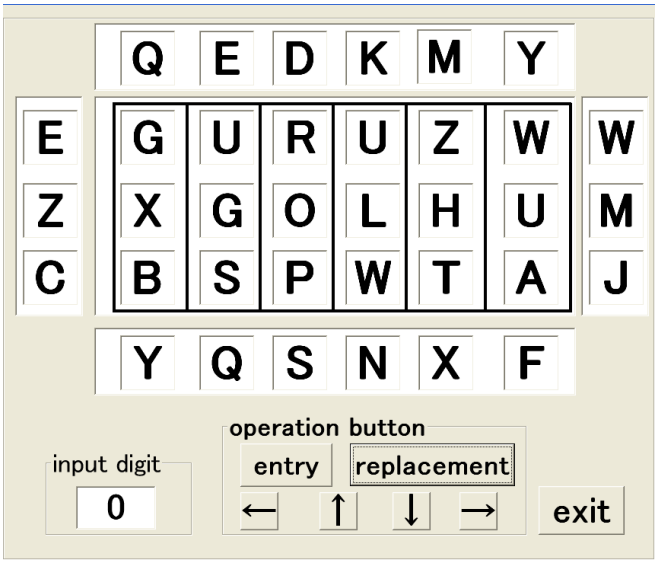

Fig. 1. Interface of random board.

- Text-display: The available texts are displayed in a D×W square. An example display of 3×6 is shown in Fig. 1.
- Modification function of text display: The entire text that is displayed in the square moves one position left, right, up, or down by pressing the operation button. The area that is surrounded by the broken line is a preindication area and shows the text available around the square. In addition, when the text that the user wants to enter is not in the display, the user presses the "replacement" button to display a new set of texts.
- Password input function: The user enters a password by using the "entry" button when the text of the password is placed in the correct column.

The following example demonstrates the operation of the Random Board: Assume that the password is "WAKE," as mentioned before, and that the correct column positions are "1 4 4 1". When the display for the first pass-text entry is shown, as Fig. 1, the user presses the "entry" button if he is searching for "W". By pressing the "←" button once, the user shifts its position to the first column, which is a correct position. Because only a column position is specified, the first pass-text may be placed in any row in the first column.

B. Security Evaluation

The security of the basic method is evaluated. Because the method specifies only the correct column position for each pass-text, it has ambiguity and has a tolerance for shoulder

surfing attacks and the video-recording attacks that record more than once.

1) Security against random attacks

Assume that the D row × W column display is used in the authentication interface, the number of available text for a password is N, and password length is L. In this case, the success probability p of a random attack is described as follows:

$$p = \{1 - \{(N\text{-}1)/N\}^D\}^L$$

Table I--Table III show values for p when N=10, 26, and 36. The values of p > 0.0001, shown by the grayed area, indicate a greater success probability of a random attack. The success probability p does not depend on the number of columns W.

TABLE I: SUCCESS PROBABILITY OF RANDOM ATTACK (N=10)

	L=1	L=2	L=3	L=4	L=5	L=6
D=1	0.100000	0.010000	0.001000	0.000100	0.000010	0.000001
D=2	0.190000	0.036100	0.006859	0.001303	0.000248	0.000047
D=3	0.271000	0.073441	0.019903	0.005394	0.001462	0.000396
D=4	0.343900	0.118267	0.040672	0.013987	0.004810	0.001654
D=5	0.409510	0.167698	0.068674	0.028123	0.011517	0.004716
D=6	0.468559	0.219548	0.102871	0.048201	0.022585	0.010582

TABLE II: SUCCESS PROBABILITY OF RANDOM ATTACK (N=26)

	L=1	L=2	L=3	L=4	L=5	L=6
D=1	0.038462	0.001479	0.000057	0.000002	0.000000	0.000000
D=2	0.075444	0.005692	0.000429	0.000032	0.000002	0.000000
D=3	0.111004	0.012322	0.001368	0.000152	0.000017	0.000002
D=4	0.145196	0.021082	0.003061	0.000444	0.000065	0.000009
D=5	0.178073	0.031710	0.005647	0.001006	0.000179	0.000032
D=6	0.209685	0.043968	0.009219	0.001933	0.000405	0.000085

TABLE III: SUCCESS PROBABILITY OF RANDOM ATTACK (N=36)

	L=1	L=2	L=3	L=4	L=5	L=6
D=1	0.027778	0.000772	0.000021	0.000001	0.000000	0.000000
D=2	0.054784	0.003001	0.000164	0.000009	0.000000	0.000000
D=3	0.081040	0.006567	0.000532	0.000043	0.000003	0.000000
D=4	0.106567	0.011356	0.001210	0.000129	0.000014	0.000001
D=5	0.131384	0.017262	0.002268	0.000298	0.000039	0.000005
D=6	0.155512	0.024184	0.003761	0.000585	0.000091	0.000014

2) Security against video attacks by recording once

Because attackers do not know the password and its correct column positions, they are not able to predict a password candidate set by analyzing the recorded video, if it is recorded only once.

3) Security against video attacks by recording twice

Next, we discuss the security of video attacks that record twice. For example, this means that today's and yesterday`s password input operation of the same user are recorded by the video. Even if the number of password candidates is large, the number of the password candidates decreases sharply by analyzing the two recorded videos because all the pass-characters are placed in their same respective columns in both the videos.

To achieve secure authentication, the following procedure is used:

- To maintain the tolerance of a random attack, the number of rows D in the interface is decided using Table I - Table III.
- As the number of columns W increases, the number of password candidates increases. Thus, by keeping the number of rows fixed to the value decided by the above procedure, the number of columns is increased until the number of the password candidates exceeds 10000.

Table IV - Table VI are based on simulation results, where the displayed texts of each password entry operation are generated randomly, and the common password candidates are counted. In a simulation, the number of candidates is obtained by considering the average of 100 trials. When the average exceeds 10000, the proposed method is considered secure.

In the Tables, the following notations are used:

D: Number of rows in the authentication interface

mN: Minimum number of texts available for the password to maintain tolerance to random attacks

mW: Minimum number of columns in the interface to maintain tolerance to video-recording attacks

TABLE IV: SECURE RANGE (N=10)

	L=4		L=5		L=6		L=7		L=8	
	mN	mW	mN	mW	mN	mW	mN	mW	mN	mW
D=1	10	100+	7	95	5	55	4	39	4	31
D=2	20 x		13 x		9	16	7	11	6	10
D=3					13 x		11 x		9	5
D=4									11 x	

TABLE V: SECURE RANGE (N=26)

	L=4		L=5		L=6		L=7		L=8	
	mN	mW	mN	mW	mN	mW	mN	mW	mN	mW
D=2	20	80	13	42	9	28	7	22	6	17
D=3	29 x		18	19	13	13	11	10	9	8
D=4			24	11	17	8	14	6	13	5
D=5			30 x		22	5	17	4	16	3
D=6					26	4	23	3	19	2
D=7					33 x		27 x		23	2
D=8									26	2
D=9									29 x	

TABLE VI: SECURE RANGE (N=36)

	L=4		L=5		L=6		L= 7		L=8	
	mN	mW	mN	mW	mN	mW	mN	mW	mN	mW
D=2	20	99	13	56	9	36	7	28	6	22
D=3	29	40	18	26	13	16	11	13	9	10
D=4	39 x		24	14	17	10	14	8	13	6
D=5			30	9	22	7	17	5	16	4
D=6			38 x		26	5	23	4	19	3
D=7					33	4	27	3	23	2
D=8					38 x		30	2	26	2
D=9							34	2	29	2
D=10							38 x		32	1
D=11									35	1
D=12									38 x	

In the case N=10 and L=6, when D=2 (two rows are displayed in the authentication interface), the minimum length of the texts that composes a password must be equal to or more than 9 (mN=9) to be secure against a random attack.

In other words, it means that a password composed of numbers (except 0) is sufficient. The tolerance to the random attack becomes stronger when the type of the text used changes from numeric to alphanumeric. In addition, the Table indicates that in order to be tolerant to a video attack, the number of columns in the authentication interface should be equal to or more than 16 (mW=16).

In the case of N=10 and L=6, three-row interface is not safe. This is because to be tolerant to a random attack, more than 13 texts are needed (13x). The Table suggests that a numeric password is not safe in this case.

There is also a description "100+" in the Table, which means that the columns are more than 100. This condition is not considered in the simulation.

If there are too many columns in the interface, it has a usability problem. Thus, the password length should be equal to or more than 6 in the case of N=10, and should be equal to or more than 5 in the case of N=26 or N=36.

V. The Improved Method

In the preceding chapter, we have proposed a password authentication method that has tolerance to random attacks and the video attacks by recording twice. However, in this method, users must additionally provide the correct columns beforehand, which cause inconvenience to them. Therefore, in this chapter we discuss improvements to the basic method.

A. Outline of the Improved Method

To maintain the tolerance to random and video-recording attacks, the following rules are adopted to introduce more ambiguities:

- The user presses the enter button to place the first pass-text in any position.
- Assume that during the authentication operation, the user presses the enter button for the (k-1)-th pass-text placing it in the i-th row and the j-th column. Then, the correct place of the k-th pass-text is from the i-th row to the (i+d)-th row, and from the j-th column to the (j+w)-th column. The values of d and w are predefined in the method for secure authentication.

A	Q	B	M	J	R
D	W	L	S	Q	Z
P	G	K	Y	C	O
V	M	I	T	H	L

Fig. 2. Display of the first pass-text entry.

Fig. 2 shows the interface when d=3 and w=3. Assume that the password is "WAKE" and the user presses the enter button for the first pass-text entry when the display is the same as Fig. 2. In this case, the gray colored area is a correct position for the second pass-text "A". If the correct position is from the 3rd row to the 5th row in three-row interface, it is interpreted that correct row is any one of the 3rd, 4th, and 1st row.

In this method, generally, security depends on the size of the correct range (d row × w column) and the size of interface display (D row × W column). Although the small size of d×w and D×W can be used to achieve tolerant to random attacks, the small size has low tolerance to video-recording attacks.

B. Security Evaluation

1) Security against random attacks

The success rate of random attack is shown in Table VII - Table IX.

The success rate of random attack is different from the one that is obtained by calculating the success rate for each pass-text independently and then calculating the product. If multiple k-th pass-text exist in the range of correct position, the allowable correct position of (k+1)-th pass-text is wider than the calculated range. Hence, the security is evaluated using simulations. Texts displayed on the authentication interface are generated randomly, and the success rate of random attacks is calculated by assuming the correct password is all 0. The simulation is performed 1000000 times for each simulation condition. When the number of times the password was authenticated correctly was less than 100, the simulation condition is secure.

TABLE VII: Secure Range of D×W (N=10)

	L=10		*L=11*		*L=12*		*L=13*	
d×*w*	*min*	*max*	*min*	*max*	*min*	*max*	*min*	*max*
3	1000	96	1200	340	1300	1200	1500	3500
4	120	10	100	30	90	70	70	200
5		5*x*	13	6	8	11	6	28
6				6*x*		6*x*	6	7

TABLE VIII: Secure Range of D×W (N=26)

	L=8		*L=9*		*L=10*	
d×*w*	*min*	*max*	*min*	*max*	*min*	*max*
5	950	380	1000	2000	1100	lots
6	260	100	280	550	240	2400
7	110	50	100	170	70	800
8	48	20	30	70	11	240
9	18	11	9	32	9	90
10	12	10*x*	10	16	10	40
12				12*x*	12	14

TABLE IX: Secure Range of D×W (N=36)

	L=7		*L=8*		*L=9*		*L=10*	
d×*w*	*min*	*max*	*min*	*max*	*min*	*max*	*min*	*max*
5	2500	500	3000	4800	3700	lots	4600	lots
6	860	160	900	1300	960	lots	1000	lots
7	380	90	340	480	310	3000	300	lots
8	170	36	140	200	110	1000	70	4200
9	90	20	60	90	40	400	25	2000
10	48	14	27	42	14	200	10	900
12		12*x*	12	16	12	45	12	160
14				14*x*	14	22	14	55

In the Tables, following notations are used:

d×w: Width of the correct position of pass-text (not valid for the first pass-text)

min: Minimum size of D×W in authentication interface to be tolerant to video-recording attacks

max: Maximum size of d×w to be tolerant to random attacks

lots: Value greater than 10000

The success rate of random attacks is reflected in the *max* column in Table VII – Table IX. For example, in the case of

$L=12$ and $d\times w=5$ in Table VII, the value is 11 in the *max* column. This indicates that the success rate of random attacks is less than 0.0001 when the value $D\times W$ is equal to or less than 11.

2) Security against video attacks by recording twice

There is tolerance to video-recording attacks if there is a large amount of ambiguity. Thus, large values are used for $D\times W$ and $d\times w$ so that the interface is tolerant to video-recording attacks.

The evaluation results are shown in Table VII – Table IX in the *min* column. For example, in the case of $L=12$ and $d\times w=5$ in Table VII, the value in the *min* column is 8. This indicates that the number of password candidates obtained by analyzing two recorded videos is less than 10000 when the value of $D\times W$ is less than 8. Therefore, in this case, it has tolerance to both random attacks and video-recording attacks when the value of $D\times W$ is between 8 and 11.

The criterion for evaluating security in this simulation is the same as the one used in the basic method. From the results shown in Table VII -Table IX, it can be seen that to have tolerance to random attacks and video-recording attacks, a numeric password must be at least 12 characters long, an alphabetic password must be at least nine characters long, and an alphanumeric password must be at least eight characters long.

VI. Discussion

First, we compare our proposed method with the method in [11]. The method in [11] and the basic method in this article are very similar from the viewpoint of performance. However, in the method [11], all of the available texts are displayed as squares on the authentication interface. In the case of a four-character password, the number of columns should be equal to or more than 10 for tolerance to random attacks, and the number of rows should be equal to or more than 9 for tolerance to video-recording attacks. Therefore, the number of available pass-texts is equal to or more than 90 for tolerance to both the attacks. Also, in the case of five-character password, the number of columns should be equal to or more than 7 and the number of rows should be equal to or more than 6. Therefore, the method [11] is not used when four or five length alphanumeric password is used.

Also, in the method [11], the user needs to provide the password and its correct color pattern beforehand. It is desirable to use a method that does not require any additional information provided beforehand, such as the improved method described in this article. However, the feasibility of such a requirement is not clear for the method [11].

The comparison of each authentication method is shown in Table X.

In the fakePointer method, the procedure to retrieve the "answer selection information" must be secure against attacks. This procedure must be done before each authentication. Thus, it is reflected in "repeated authentication" column in Table X. If a user can retrieve the "answer selection information" safely, it is also applicable to mobile authentication and the basic method in this article.

As shown in Table X, the improved method discussed in this article is the only method that can be used for repeated authentication and that has tolerance to both random attacks and video attacks recorded twice, without any additional information provided beforehand.

TABLE X: Comparison of Authentication Method

	secure against shoulder surfing	Secure against video attack recording twice	repeated authentication	no additional information provided beforehand
Pin Entry	O	×	O	O
S3PAS	O	×	O	O
fakePointer	O	O	×	O
Mobile authentication	O	O	O	×
Random Board	O	O	O	×
Improved Random Board	O	O	O	O

VII. Conclusion

We propose the Random Board as a password authentication method that has a tolerance to random attacks and video-recording attacks. We adopt as a requirement, a success rate of less than 1/10000 for random attacks and less than 1/10000 for video analysis attacks by recording the authentication operation twice. The specific authentication interface in which to fill the requirement is shown. We propose two types of Random Boards. The basic method requires that correct password entry positions be provided beforehand, whereas the improved method does not require such information.

We demonstrated that the method has tolerance to both random attacks and video attacks by recording twice by using a four-character or longer alphanumeric password in the basic method, and an eight-character or longer alphanumeric password in the improved method. The improved method proposed in this article is the only method that can be used for repeated authentication and that has tolerance to both random attacks and video attacks recorded twice, without any additional information provided beforehand.

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. [Online]. Available: 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). [Online]. Available: http://www.boy.co.jp/info/pdf/9.pdf

[3] M. Une and 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.* [Online]. Available: http://www.secom.co.jp/corporate/release/2006/nr_20060814.html

[6] NEC. The service of the investigation of the detectaphone and the sneak shot receptacle. [Online]. Available: http://www.necf.jp/solution-service/office/hiddenmic-camera/

[7] V. Roth, K. Richter, and R. Freidinger, "A Pin-Entry Method Resilient Against Shoulder Surfing," *CCS'04*, pp. 236-245, Oct. 2004.

[8] H. Zhao and 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, "fakePinter: 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," in *Proc. Cryptography and Information Security Symposium, SCIS2007*, 2007.
[11] Sakurai, Yoshida, and Bunaka, "Mobile authentication method," in *Proc. Computer Security Symposium 2004*, pp. 625-630, Oct. 2004.
[12] X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey," in *Proc. 21st Annual Computer Security Applications Conference, ACSAC 2005*, 2005.
[13] R. Dhamija and A. Perrig, "Déjà vu: A User Study Using Images for Authentication," in *Proc. 9th Usenix Security Symposium*, pp. 45-58, Aug. 2000.
[14] RealUser. [Online]. Available: http://www.realuser.com/
[15] T. Takada and 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.
[16] L. Sobrado and J. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.
[17] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic Authentication through Untrusted Terminals," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 30-36, 2003.
[18] W. Ku and M. Tsaur, "A Remote User Authentication Scheme Using Strong Graphical Passwords," *IEEE Local Computer Networks, LCN'05*, 2005.
[19] Y. Hirakawa and K. Fujita, "A study of password authentication against shoulder surfing," *SISY2008*, 2008.

Y. Hirakawa received his BS, MS, and PhD degrees in 1978, 1980, and 1994 from Kobe University, respectively. He engaged in Nippon Telegraph and Telephone Research Center until 2004. Since 2005, he is a professor at the Information Science Engineering Department, Shibaura Institute of Technology, Tokyo, Japan.

His interests include ad hoc communication networks, p2p communications, security, and Internet application services. Dr. Yutaka Hirakawa is a member of IEEE computer society, IEICE (The Institute of Electronics, Information and Communication Engineers) Japan, and IPSJ (Information Processing Society Japan).