PAPER Special Section on Enriched Multimedia — Potential and Possibility of Multimedia Contents for the Future —

Shoulder-Surfing Resistant Authentication Using Pass Pattern of Pattern Lock

So HIGASHIKAWA[†*], **Tomoaki KOSUGI**[†*], **Shogo KITAJIMA**[†], ***Nonmembers***, ***and*** **Masahiro MAMBO**[††], ***Member***

SUMMARY We study an authentication method using secret figures of Pattern Lock, called pass patterns. In recent years, it is important to prevent the leakage of personal and company information on mobile devices. Android devices adopt a login authentication called Pattern Lock, which achieves both high resistance to Brute Force Attack and usability by virtue of pass pattern. However, Pattern Lock has a problem that pass patterns directly input to the terminal can be easily remembered by shoulder-surfing attack. In this paper, we propose a shoulder-surfing resistant authentication using pass pattern of Pattern Lock, which adopts a challenge & response authentication and also uses users' short-term memory. We implement the proposed method as an Android application and measure success rate, authentication time and the resistance against shoulder surfing. We also evaluate security and usability in comparison with related work.

key words: *shoulder surfing, authentication, pattern lock, android application*

1. Introduction

Recently, many people have portable devices such as smart phones, which have been improved to be small-sized and lighter. At the same time, the risk of loss or theft has been increased. If attackers steal mobile devices, they can impersonate the owners and access to private information such as privacy-sensitive pictures stored in the personal mobile devices. Thereby, to counter the attack and privacy invasion, mobile devices generally have some authentication systems such as PIN, Text Password, Pattern Lock, and Fingerprint Authentication. On Pattern Lock, which is one of these systems, users input a figure with a single-stroke sketch as a secret. In comparison with PIN which uses several numbers, Pattern Lock has more secret combinations and the secret is easy to memorize and input. Although the system has high usability, a slight peep into the input screen helps an attacker to obtain the secret pattern. For these reasons, authentication systems on mobile devices have been required to be resistant against shoulder surfing and some methods have been proposed in [4], [5], [8].

In this paper, we propose an authentication system which has high affinity with Pattern Lock and the resistance against shoulder surfing attack. Moreover, we execute experiments regarding usability and safety.

Manuscript received April 5, 2017.
Manuscript revised August 25, 2017.
Manuscript publicized October 16, 2017.

[†]The authors are with the Graduate School of Natural Science and Engineering, Kanazawa University, Kanazawa-shi, 920–1192 Japan.
[††]The author is with the Institute of Science and Engineering, Kanazawa University, Kanazawa-shi, 920–1192 Japan.
[*]Presently, with the NTT Data Hokuriku Corporation.

DOI: 10.1587/transinf.2017MUP0012

2. Related Knowledge

2.1 Shoulder Surfing

Shoulder surfing is an attack by peeping an authentication screen of devices. We consider human eyes or cameras to be the attackers. Features of the attack by human eyes are as follows.

- The attack is involved by memorizing and processing ability of the attacker.
- If the attacker could not specify the secret with a single peep, he attempts to narrow down the candidates with other trials.

Features of the attack by cameras are as follows.

- The authentication screen is recorded, so the attacker can do close analysis with the video.
- If the attacker could not specify the secret with the video of one authentication, he attempts to narrow down the candidates with the videos of other trials.

Monitoring cameras have been improved to be small-sized, so an authentication screen can be recorded without users' awareness. As an actual occurrence, an ATM of a big bank was recorded by artfully concealed cameras [6], [7]. Furthermore, the situation would be more possible in which we must carry out authentication with the peep by attackers. Therefore, countermeasures have been strongly required.

2.2 Pattern Lock and Pass Pattern

In advance, a user sets a pass pattern such as Fig. 2 with a one-stroke sketch, which is stored to be the secret of Pattern Lock. The user reproduces the pattern on the authentication and the system confirms the correspondence to judge. Pass patterns must fulfill the following rules:

- A pattern contains more than 3 dots.
- Each dot can be chosen up to one time.
- Passing over a dot is allowed if the dot was already chosen.

Pattern Lock has 389,112 secret combinations, which is more than 10,000 of PIN. Besides, its secret information

Copyright © 2018 The Institute of Electronics, Information and Communication Engineers

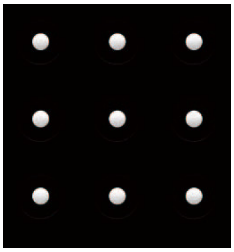

Fig. 1 Selectable dots

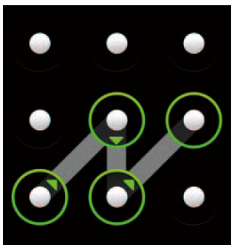

Fig. 2 An example of pass pattern

appears to be a diagram which a user can easily memorize. In contrast, Pattern Lock has no resistance against shoulder surfing.

3. Related Work

We introduce related work [2], [4], [5], [8] which can be resistant against shoulder surfing. These methods need no additional devices.

3.1 Matrix Authentication

Matrix Authentication [2] is a challenge & response authentication system which uses position and order as a secret. In advance, the system shows 4 tables in a horizontal line, each of which has 16 boxes in a 4-by-4 matrix. Then, a user choose more than 7 boxes out of 64. The chosen position and order is stored as "image password." When the authentication is started, 64 boxes are showed similarly as the above registration phase and each box has a random one-digit number. The user enters the numbers which are located in the same position as the image password. In this way, the input number array is a one-time password, so an attacker can not acquire any information of the secret by peeps. The possibility of Brute Force Attack on Matrix Authentication is more than $1/10^8$, whereas it has more than 64^8 secret combinations. Matrix Authentication may be resistant against shoulder surfing by eyes, but it has not been clarified [2]. Thus, we conduct experiments to investigate the resistance in Sect. 6.3.

3.2 STDS

STDS [5] is a challenge & response authentication system which uses icon images and shifts. A user registers some icons as a secret in advance. When the authentication is started, 16 icons are randomly located in a 4-by-4 matrix for each digit. One of these icons corresponds to the secret icon. In addition, shift information as transferring to other positions is showed. The user selects the proper icons considering the shift information and repeats the procedure for the rest digits.

Moreover, if the user activates "Any Shift Mode," shift information becomes selectable by the user beforehand. In this mode, the system has the resistance against one peep by recording. However, since the number of acceptable icons rises, the possibility of false authentication may also increase from $1/65536$ to $1/256$.

Furthermore, this system has "Fake Mode" for stronger resistance. If the mode is activated, the device gives out vibration on some digits. Then, the user must select an artificial icon. In this mode, the system is stronger against recording peeps than in Any Shift Mode. On the other hand, the usability gets lower for artificial procedures.

3.3 FakePointer

FakePointer [8] is a challenge & response authentication system which generates selection information for each authentication. This system is resistant against multiple peeps by recording, however, sharing information in secrecy with the user is not an easy task. Thereby, this system can not be widely applied to versatile devices.

3.4 CCC

CCC [4] is a challenge & response authentication system which has an interface like a knob of safes. A user inputs some numbers regarding a cursor and the PIN the user already registered. The correct position of the cursor is notified by the vibration. This system is resistant against peeps by recording. According to the paper, no attackers of 10 could specify the secret by shoulder surfing and the success rate was 91%. Nevertheless, it took 34.34 second for one authentication of 4-digit PIN in average, which should be shorter.

3.5 Comparison among Related Work

We show the comparison of features in Table 1. We indicate especially superior features in blue and inferior ones in red. As regards the resistance against shoulder surfing, O denotes that it has higher resistance than Pattern Lock and X denotes the contrary. Also, - means an unidentified value.

We conducted experiments to clarify the success rate and authentication time of Pattern Lock and Matrix Authentication. 4 university students tried each authentication. On Pattern Lock, they set a pass pattern of each digit and executed the authentication for 10 times on one pattern. On Matrix Authentication, they set a 8-digit password image and executed the authentication for 10 times. The values in Table 1 are the average of 10 authentications.

Table 1 Comparison among Related Work

		Pattern Lock	Matrix	STDS	fP	CCC
Safety	Candidates for Brute Force Attack	389,112	More than 10^8	65,536	10,000	10,000
	Resistance against Shoulder Surfing by eyes	X	-	O	O	O
	Resistance against Shoulder Surfing by cameras	X	X	O (up to 1 time)	O	O
Usability	Srcret Information users must memorize	Patterns	Positions	Icons and Shift Information	PIN	PIN
	Accept Probability [%]	86.2	82.5	85.0	94.4	91.0
	Authentication Time [sec.]	2.48	13.41	7.14	17.35	34.34
	Another Physical Device	X	X	X	X	Vibration
	Another Secure Channel	X	X	X	O	X

Matrix Authentication has no resistance against peeps by recording, but has much many secret combination. STDS is resistant against peeps by eyes although it is resistant against one peep by recording. Moreover, the system requires short time to execute and no secure connection to share the secret. On the other hand, users must remember a set of icons and shift information, so the system has not come into wide use. FakePointer has the resistance against peeps by recordings, but users are required to share secret information with the system in advance for each authentication. CCC requires long time to execute and vibrate functions whereas it also has the resistance against peeps by recordings.

4. Basic Design

We design a basic authentication method which is resistant against shoulder surfing and conduct experiments. Considering the results, we show an improved authentication as a proposed method in Sect. 5.

4.1 Design Principle

We set the principle of our proposed method as follows:

- Resistant against peeps by eyes
- Compatible with Pattern Lock: no additional secret information is needed

For the first principle, we let our method have the resistance in a way that attackers cannot narrow down candidates less than a certain value with some peeps. For the second principle, we let our method use secret information of Pattern Lock. Therefore, users can selectively execute the method: they use Pattern Lock if there seems no peeps or switch to the challenge & response mode in a crowded place. In addition, we utilize advantages of Pattern Lock. We attempt to let our method be handy to input and use no secure connection to share secrets.

For these goals, we adopt the challenge & response method of Matrix Authentication in Sect. 3.1. Specifically, our system shows numbers which are located as the dots of Pattern Lock. Then a user inputs the corresponding numbers on a table.

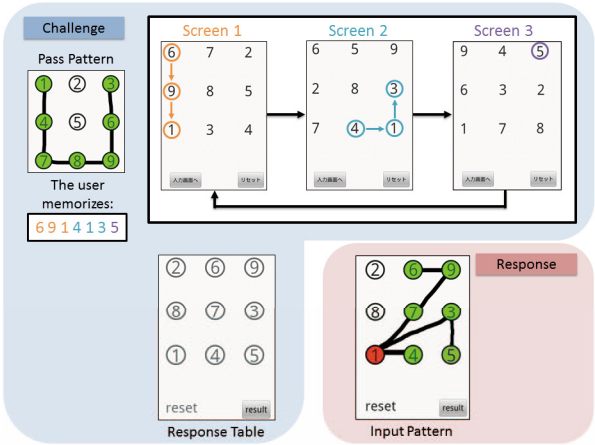

Fig. 3 Screens on the basic authentication

4.2 Authentication Procedure

Beforehand, a user sets a pass pattern in Pattern Lock. Just before the user begins the authentication, he judges whether the resistance against shoulder surfing is necessary for authentication. The system can be switched to use the challenge & response authentication, otherwise it operates as Patten Lock. The procedure of the challenge & response authentication is as follows.

1. Random numbers of 1-9, each one is chosen once, are showed in a 3-by-3 matrix. (Screen 1 of Fig. 3)
2. The user memorizes the numbers corresponding to 1st, 2nd, and 3rd dots of the pass pattern.
3. New random numbers are showed similarly as Step 1. (Screen 2 of Fig. 3)
4. The user memorizes the numbers of 4th, 5th, and 6th similarly as Step 2.
5. New random numbers are showed similarly as Step 1. (Screen 3 of Fig. 3)
6. The user memorizes the numbers of 7th, 8th, and 9th similarly as Step 2.
7. If the user forgets the numbers, get back to Step 1.
8. New random numbers are showed similarly as Step 1.
9. The user successively traces the numbers of Step 2, 4, and 6.
10. If the response is correct, the device becomes unlocked.

The numbers in response are colored by the times of being traced in the order of green, red, blue, yellow, orange, and purple. This coloring allows users make sure of the track. Besides, we make the numbers of response randomized so that attackers can not memorize a track as a figure with ease. Furthermore, we impose users memorizing three numbers in each table in challenge. If the system shows one table and they memorize up to 9 numbers at a time, the table can be seen by attackers for a long time so the secret may be easily specified. For this reason, we restrict the time per table to be memorized.

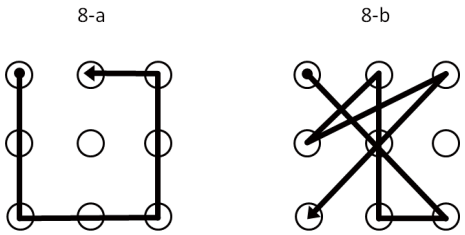

Fig. 4 Pass pattern examples (simple and complicated)

Table 2 Success rate and authentication time in the basic design

Pass pattern	Success rate (%)	Authentication time (sec)					
		Average	Max		Min		Standard deviation
			Max	Min	Max	Min	
Simple	82.86	20.63	168.15	9.90	30.31	4.45	9.05
Complicated	87.14	19.99	155.16	8.86	35.35	4.50	9.26
Average	85.00	20.31	161.65	9.38	34.35	4.47	9.15

In challenge, the same number sometimes appears continuously in the number array which the user memorizes. In such a case, the user inputs the number only once and omits other successive duplicated numbers (the case of degeneracy defined in Sect. 4.4). For example, in Fig. 3, if 3 appears at the position of 5 in Screen 3, then 3 seems to be the number to be traced just after the number array 413 in Screen 2. However, 3 appears only once in the screen for the response and the successive numbers 33 cannot be traced. Thus the successive numbers 33 are treated as one digit 3. In response, users sometimes trace numbers on the edge of a table. As the example from 9 to 1 on Fig. 3, if there is another number between two numbers to be traced, the user must additionally trace the middle number (the case of expansion defined in Sect. 4.4 and 7 in this example). Consequently, the response numbers can be varied to be longer, which prevents attackers from specifying the secret.

4.3 Experiment

4.3.1 Usability

We produce an authentication system which requires the procedures in Sect. 4.2 and execute experiments to evaluate the usability. Hereafter, digit of pass pattern denotes the number of dots on the pass pattern without counting the same dot multiple times. Each of examinees (7 university students), who before starting the experiment, practice multiple times with some pass patterns selected by themself, is given the same fixed pass patterns in each digit (4-9). The examinees try the authentication 10 times for each of the fixed i-digit pass patterns where $i \in \{4, .., 9\}$. An order of digit is randomly assigned in 4-9 because a simple order may affect the result. We measure the result (success/failure) and the time for the authentication and challenge. For each digit, the examinees arrange two patterns: simple and complicated as shown in Fig. 4 to measure the influence of pattern complexity.

We show the result in Table 2 and Fig. 5. In Table 2, we

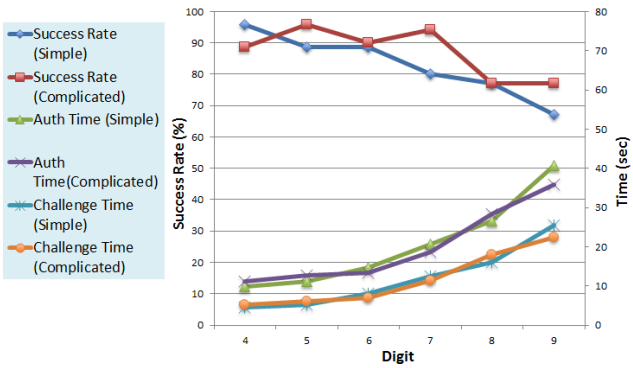

Fig. 5 The result of authentication experiment

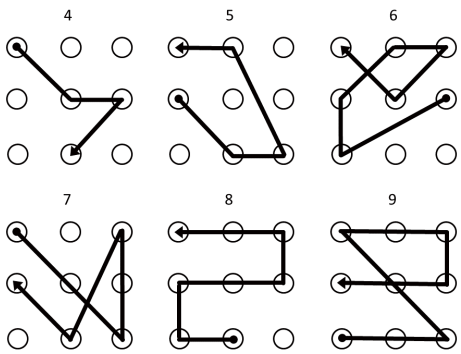

Fig. 6 Pass patterns for shoulder-surfing attack experiment

denote max and min of maxs and mins. The experiments of 7 examinees produced 7 max values and 7 min values. Max of maxs is the max value of all examinees. Min of maxs and others of mins are similar.

For the result, there is no typical difference in the simple patterns and the complicated patterns. As Fig. 5, the authentication time increases by 28 sec in between 4 and 9 digit and the success rate decreases by 20% likewise.

4.3.2 Resistance against Shoulder Surfing

An examinee sets one pass pattern for each digit and some examinees (5 university students) try to specify the secret pattern with multiple peeps. We show the patterns used in this experiment in Fig. 6. Shoulder-surfing attack was conducted following these conditions:

- Try to peep up to 10 times for each pattern
- Try to peep diagonally behind the user
- Can take a short note after each authentication
- Have a knowledge of general attacks and can elaborate another strategy

We suppose our algorithm is disclosed to the public, so attackers know how to conduct shoulder-surfing attack for this authentication. If an attacker finished 10 peeps for one pattern or he specified one candidate which most possibly corresponds to the pass pattern, we let him show the pattern to check the correspondence.

Table 3 The result of shoulder-surfing attack experiment

Digit	Attackers				
	A	B	C	D	E
4	S(10,4)	F(5,3)	S(9,4)	S(5,4)	S(5,4)
5	F(10,1)	F(10,1)	F(10,0)	S(9,5)	S(9,5)
6	S(7,6)	S(10,6)	S(10,6)	S(10,6)	F(10,3)
7	F(10,4)	F(10,3)	F(10,6)	S(10,7)	F(10,2)
8	F(8,6)	F(10,3)	F(10,4)	F(10,5)	F(10,6)
9	S(9,9)	F(10,4)	F(10,2)	S(6,9)	F(10,7)

Table 4 The average number of possible patterns for a number array

Digit	4	5	6	7	8	9	Total
Ave. No. of Candidates	1.16	1.14	1.13	1.11	1.06	1.03	1.10

We show the result in Table 3. After showing a proposed scheme in Sect. 5, we also show the result for the proposed scheme in Table 7. S denotes that the attacker succeeded to specify the secret pattern and F denotes the contrary. In addition, (u, n) denotes that the attacker tried u peeps and partly specified n digits of the pass pattern. According to the result, attackers need more than 4 peeps to specify a secret pattern.

4.4 Degeneracy and Expansion

We examine the difference of resistance against Brute Force Attack between the basic design in Sect. 4 and Pattern Lock.

In challenge, multiple successive numbers are put together to be one digit, which we call "Degeneracy." In response, if two numbers the user is tracing has another number in the middle, he must trace the numbers linearly and the middle number is added, which we call "Expansion." (See examples of degeneracy and expansion in Sect. 4.2) Due to these effects, some false patterns would generate the number array which can be accepted. Therefore, we evaluate the number of possible patterns for a certain number array. To this end, we at first fix a number array for a given pass pattern with a certain digit by randomly selecting challenge. Then we count the number of patterns whose number array for the same challenge is accepted by the same randomly selected response. We execute the experiment for 40 different pass patterns with every 4 to 9 digit.

We show the average number of possible candidates counted by the experimet in Table 4. In almost all of authentications, the number of possible patterns which generate a number array which can be accepted is 1 or 2. Since these patterns contain the real pass pattern, the number of false patterns is up to 1. This may be because almost all of possible false patterns do not follow the rules "Each dot can be chosen up to one time" and "Passing over a dot is allowed if the dot was already chosen" in Sect. 2.2. Accordingly, the possibility of Brute Force Attack is approximately $1/353738$, so the resistance is not nearly lowered. Furthermore, although degeneracy and expansion make our method stronger against shoulder surfing, usability is reluctantly sacrificed. For this reason, we consider confining these effects to enhance usability and propose an improved method in Sect. 5.

5. Proposed Method

The main idea of our proposed method is that given a pass pattern of user, random numbers are located on challenge screen 1, 2, 3 in a way not causing degeneracy and a number array is determined. Also given the number array, random numbers are located on response screen without causing expansion. By the random number generation rules, the user is free from any special operation associated with degeneracy and expansion. Users just proceed the procedure in Sect. 4.2. We modify the generation algorithm as follows:

- Generate random numbers of 1-9, each one is chosen once, in a 3-by-3 matrix.
- Derive a number array to be input by checking the pass pattern with the matrix.
- If degeneracy is occurred, get back to Step 1.
- Generate new random numbers similarly as Step 1.
- If expansion is found by checking the number array with the matrix, get back to Step 8.

The whole procedure of the proposed challenge & response authentication is as follows.

1. Random numbers of 1-9, each one is chosen once, are showed in a 3-by-3 matrix. (Screen 1 of Fig. 3)

1'. Derive a number array to be input by checking the pass pattern with the matrix. If degeneracy is occurred, get back to Step 1.

2. The user memorizes the numbers corresponding to 1st, 2nd, and 3rd dots of the pass pattern.
3. New random numbers are showed similarly as Step 1. (Screen 2 of Fig. 3)
4. The user memorizes the numbers of 4th, 5th, and 6th similarly as Step 2.
5. New random numbers are showed similarly as Step 1. (Screen 3 of Fig. 3)
6. The user memorizes the numbers of 7th, 8th, and 9th similarly as Step 2.
7. If the user forgets the numbers, get back to Step 1.
8. Generate new random numbers similarly as Step 1.

8'. If expansion is found by checking the number array with the matrix, get back to Step 8.

9. New random numbers are showed similarly as Step 1.
10. The user successively traces the numbers of Step 2, 4, and 6.
11. If the response is correct, the device becomes unlocked.

6. Experiment

6.1 Usability

We execute experiments to evaluate the usability similarly as Sect. 4.3.1. All of their examinees are different from those for the basic design in Sect. 4.3.1. For the result in

Table 5 Success rate and authentication time in the proposed method

Pass pattern	Success rate (%)	Authentication time (sec)					
		Average	Max		Min		Standard deviation
			Max	Min	Max	Min	
Complicated	78.10	13.08	47.36	26.66	5.75	4.04	7.10

Table 6 Wilcoxon rank sum test

Digit	4	5	6	7	8	9
p-value ($\times 10^{-5}$)	3.697×10^{-8}	9.802×10^{-3}	9.920	15.81	197.2	6577

Table 7 The result of shoulder-surfing attack

Digit	Attacker				
	P	Q	R	S	T
4	S(5,4)	S(4,4)	S(6,4)	S(5,4)	F(10,3)
5	S(8,5)	S(8,5)	S(10,5)	F(10,4)	S(7,5)
6	S(8,6)	F(10,5)	S(8,6)	F(10,3)	S(4,6)
7	S(10,7)	S(8,7)	S(9,7)	S(10,7)	F(10,1)
8	F(10,5)	S(9,8)	F(10,4)	F(10,2)	F(10,3)
9	F(10,6)	F(10,4)	F(10,3)	F(10,2)	S(10,9)

Sect. 4.3.1, we perceived that pattern complexity does not effect authentication time, so we use only complicated patterns as pass patterns. Examinees are 7 university students.

We show the result in Table 5. Authentication time is shortened by 7 sec on average. The max value in all examinees is also reduced to 47 sec.

There are 70 data obtained from 10 (traials) $\times$ 7 (examinees) for each of the basic design and the proposed scheme. We have conducted the U-test for them and its result is shown in Table 6 where the p-value is less than. Therefore, the data used in our analyses itself can be considered as reliable.

We have also requested examinees to answer a questionaire about usability. 5 examinees have answered. For a question about how many digits of pass patterns are easy to use, three examinees answer 7 digits and other number is 5 digits by one examiner and 4 digits by one examinee. For a question about improving points, one examinee, who mentions 7 digits in the previous question, answers that if the pass pattern is selected by oneself, it is easier to memorize it and to use the system. Other examinee, who also mentions 7 digits, points out that the use of 3 challenge screens is unfamiliar.

6.2 Resistance against Shoulder Surfing

We execute experiments to evaluate the resistance against shoulder surfing similarly as Sect. 4.3.2. Examinees are 4 university students.

We show the result in Table 7. Notation is same as Sect. 4.3.2. We can realize that attackers need more than 4 peeps to specify a secret pattern.

In comparison with the basic design in Sect. 4, we estimated that the attack would be easy since degeneracy and expansion do not occur. Nevertheless, according to an examinee's opinion, i.e. attacker's opinion, it becomes rather hard to memorize the challenge matrix especially for long pass patterns due to shorter authentication time. In fact, we can observe that the whole of 9-digit pass pattern is identified by several attackers after at least 6 peers from Table 3 while the whole is identified by only one attacker after 10 peers from Table 7. Except the attacker, at most 6 digits of the 9-digit pass pattern are identified by all of other attackers even after 10 peers.

Table 8 The result of shoulder-surfing attack in Matrix Authentication

Digit	Atacker				
	A	C	F	H	I
8	F(10,5)	F(10,0)	F(10,1)	F(10,6)	F(10,1)
9	F(10,3)	F(10,2)	F(10,5)	F(10,4)	F(10,0)

6.3 Resistance against Shoulder Surfing on Matrix Authentication

To compare the resistance against shoulder surfing, we also conduct experiments of Matrix Authentication. Condition is same as Sect. 4.3.2 and examinees are 5 university students.

We show the result in Table 8, which signifies no one succeeded to specify image passwords, so the method has the high resistance against shoulder surfing by eyes.

7. Considerations

7.1 Comparison with Other Related Methods

We show the comparison in features of the proposed method and other related methods in Table 9. Values are colored in purple if superior to the proposed method or in orange if inferior, likewise.

According to the table, the proposed method has the resistance against shoulder surfing by eyes and has as many pass pattern candidates as Pattern Lock. However, the resistance is restricted to several peeps by eyes and further peeps may reveal pass patterns which should be secret.

Compared to Matrix Authentication, our method is inferior in the resistance against Brute Force Attack, in contrast, superior in success rate and authentication time. According to the result in Sect. 6.3, Matrix Authentication has the high resistance against peeps by eyes. On the other hand, we examine the difficulty to memorize secrets. We let 5 university students set a 9-digit pass pattern of and an 8-digit image password and check how many digit they remember after 1, 6, and 24 hours.

We show the result in Table 10, which means pass patterns are easier to memorize than image passwords. This may be because it is hard to memorize image passwords which are constructed out of 64 boxes and can be as an enclave. In contrast, we can perceive pass patterns as figures with a single-stroke sketch. Therefore, Pattern Lock is superior to Matrix Authentication on easiness of remembering secrets. Additionally, our method can work as Pattern Lock is there seems no peeps, so users can easily unlock devices without challenge & response authentication.

Table 9 Comparison of features

		Pattern Lock	Matrix	STDS	fP	CCC	Proposed Method
Safety	Candidates for Brute Force Attack	389,112	More than 10^8	65,536	10,000	10,000	353738
	Resistance against Shoulder Surfing by eyes	X	O	O	O	O	O (for several times)
	Resistance against Shoulder Surfing by cameras	X	X	O (up to 1 time)	O	O	X
Usability	Srcret Information users must memorize	Patterns	Positions	Icons and Shift Information	PIN	PIN	Patterns
	Accept Probability [%]	86.2	82.5	85.0	94.4	91.0	84.2
	Authentication Time [sec.]	2.48	13.41	7.14	17.35	34.34	10.15
	Another Physical Device	X	X	X	X	Vibration	X
	Another Secure Channel	X	X	X	O	X	X

O: Satisfied/Necessary
X: Not satisfied/Unnecessary

Table 10 Easiness to remember secrets

Time passed (Hour)	Pass pattern					Image password				
	A	B	C	D	E	A	B	C	D	E
1	9	9	9	9	9	8	8	8	8	8
6	9	9	9	9	9	8	6	8	0	8
24	9	9	9	9	9	8	6	8	0	8
Result	O	O	O	O	O	O	X	O	X	O
Success rate	100%					60%				

O: Easy to remember secrets
X: Not easy to remember secrets

Compared to STDS, our method is superior in the resistance against Brute Force Attack, but has no resistance against peeps by recording and requires longer authentication time. Nevertheless, users must reproduce a set of icons and shift information, which is quite hard to remember.

Compared to fakePointer and CCC, our method inferior in the resistance against peeps by recording and success rate. However, it deals more secret combinations and no additional hardwares, which produces high applicability.

7.2 Risk of Selecting Authentication Mode

The proposed method can be switched to Pattern Lock or challenge & response authentication. Users produce the decision whether there is the possibility of shoulder-surfing attack with recognition of surroundings, which is not always true. Particularly, if there seems a subtle possibility of attack, the decision depends on users' policy on security. If users intend to take the lowest risk, they should invariably use challenge & response authentication.

Users may forget the usage if they rarely use challenge & response authentication. As countermeasures, we consider switching to challenge & response authentication by compulsion in a certain period of time [9] or show an instruction such as "Memorize corresponding 3 numbers."

7.3 Psychological Consideration on Memory

According to [9], [10], in psychology, using temporary memory is thought to be deeply involved with cognitive operation and short-term memory is called working memory.

In the working memory model of Baddeley, working memory is composed with the phonological loop, which stores linguistic memory, the visuospatial sketchpad, which stores visual memory, and the central execution part, which controls these systems. Numbers are interpreted linguistically and handled in the phonological loop. In contrast, figures and handled in the visuospatial sketchpad.

With regard to memorizing numbers, he lets examinees memorize some numbers, and immediately after, the examinees are requested to reproduce the numbers in the order shown to them. Then they could reproduce 5 to 9 numbers as a short-term memory. It has been thought that not only numbers but also characters and words have this tendency. On the other hand, he lets examinees memorize some simple figures and then he show figures which are partly altered to let them point out the changes. Through the experiment, he showed that they could remember only about 3 figures [11]. From these results, humans is prone to be able to easily memorize numbers than figures with respect to the short-term memory. Hence, we consider that converting pass patterns to one-time passwords is a psychologically rational process.

8. Conclusion

We proposed an authentication using secret information of Pattern Lock. The proposed authentication keeps the compatibility with Pattern Lock as well as increases the resistance against shoulder surfing by eyes. We executed experiments to show high usability and attack resistance. Our method requires no additional secret information, which allows users to use Pattern Lock if there seems to be no possibility of shoulder-surfing attack.

For future tasks, we should ensure the resistance against more than 3 peeps or attack by recording. Additionally, experiments to examine a tendency of people younger or elder than around 20 years old are expected.

References

[1] A. De Luca, E.V. Zezschwitz, N.D.H. Nguyen, M.-E. Maurer, E. Rubegni, M.P. Scipioni, and M. Langheinrich, "Back-of-Device Authentication on Smartphones," Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI'13), pp.2389–2398, 2013.
[2] CSE, What is the Matrix Authentication (online), https://www.cseltd.co.jp/products/smx/, 2015.01.26.
[3] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication Usable in Front of Prying Eyes," Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI'08), pp.183–192, 2008.
[4] M. Ishizuka and T. Takada, "CCC: Shoulder Surfing Resistant Authentication System by Using Vibration," IPSJ Interaction 2014, pp.501–503, 2014.
[5] Y. Kita, N. Okazaki, H. Nishimura, et al., "Implementation and Evaluation of a User Authentication System Resistant against Shoulder Surfing," The IEICE Trans. Inf. & Syst. (Japanese Edition), vol.J97-D, no.12, pp.1770–1784, 2014.
[6] Bank of Tokyo-Mitsubishi UFJ, Secret Photographing in the ATM of our Bank (online), http://www.bk.mufg.jp/info/ufj/ufj_20051227_1.html, 2015.01.26.

[7] Security NEXT, Damage by Secret Photograhing in the ATM of Yokohama Bank (online), http://www.security-next.com/002953, 2015.01.26.
[8] T. Takada, fakePointer, "A User Authentication Scheme that Makes Peeping Attack with a Video Camera Hard," IPSJ Journal, vol.49, no.9, pp.3051–3061, 2008.
[9] Edited by K. Shiomi, "Cognitive Psychology with Conversation, Sec. 3 Memory (Written by M. Ogishi), Psychology with Conversation Series 3, Nakanishiya Publishing, 2006.
[10] Edited by Y. Takano, "Cognitive Psychology 2 Memory," Tokyo University Publishing, 1995.
[11] E.K. Vogel, G.F. Woodman, and S.J. Luck, "Storage of Features, Conjunctions, and Objects in Visual Working Memory," Journal of Experimental Psychology: Human Perception and Performance, vol.27, no.1, pp.92–114, 2001.
[12] P.C. van Oorschot and J. Thorpe, "On predictive models and user-drawn graphical passwords," ACM Transactions on Information and System Security, Vo.10, no.4, pp.1–33, 2008.
[13] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith, "Smudge attacks on smartphone touch screens," Proc. 4th USENIX Conference on Offensive Technologies, Article no.1-7, 2010.

So Higashikawa graduated Toyama University, Japan, in 2012 and finished the master course of Division of Electrical Engineering and Computer Science, Graduate School of Natural Science and Technology, Kanazawa University, Japan, in 2015. He engaged in research on secure authentication systems. He is currently working at NTT Data Hokuriku Corporated.

Tomoaki Kosugi graduated School of Electrical and Computer Engineering, College of Science and Engineering, Kanazawa University, Japan, in 2015 and finished the master course of Division of Electrical Engineering and Computer Science, Graduate School of Natural Science and Technology, Kanazawa University, Japan, in 2017. He engaged in research on privacy protection systems. He is currently working at NTT Data Hokuriku Corporated.

Shogo Kitajima graduated School of Electrical and Computer Engineering, College of Science and Engineering, Kanazawa University, Japan, in 2017 and is currently a master course student of Division of Electrical Engineering and Computer Science, Graduate School of Natural Science and Technology, Kanazawa University, Japan. He has been engaged in research on secure systems using edge computing.

Masahiro Mambo received a B.Eng. degree from Kanazawa University, Japan, in 1988 and M.S.Eng. and Dr.Eng. degrees in electronic engineering from Tokyo Institute of Technology, Japan in 1990 and 1993, respectively. After working at Japan Advanced Institute of Science and Technology, JAIST, at Tohoku University and at University of Tsukuba as assistant, associate and associate professor, respectively, he joined Kanazawa University in 2011. He is currently a professor of Faculty of Electrical and Computer Engineering, Institute of Science and Engineering. His research interests include information security, software protection and privacy protection.