International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 48-55
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method: Secret Tap with Double Shift

Yoshihiro Kita* Fumio Sugai** MiRang Park*
Naonobu Okazaki**
* Kanagawa Institute of Technology,
1030 Shimo-Ogino, Atsugi, 243-0292, Japan.
y.kita@ccy.kanagawa-it.ac.jp, mirang@nw.kanagawa-it.ac.jp
** University of Miyazaki,
1-1 Gakuen-kibanadai nishi, Miyazaki 889-2192, Japan.
tf12006@student.miyazaki-u.ac.jp, oka@cs.miyazaki-u.ac.jp

ABSTRACT

Recently, mobile terminals such as smartphones have come into widespread use. Most of such mobile terminals store several types of important data, such as personal information. Therefore, it is necessary to lock and unlock terminals using a personal authentication method such as personal identification numbers (PINs) in order to prevent data theft. However, most existing authentication methods have a common problem referred to here as "shoulder-surfing", in which authentication information is covertly obtained by a person watching "over-the-shoulder" of a user as he/she completes the authentication sequence. In the present paper, a new icon-based authentication method that is simple but sufficiently secure even when the authentication sequence is being watched is proposed. The proposed method is implemented on a mobile data terminal and is evaluated through experiments and questionnaire surveys.

KEYWORDS

Graphical authentication, Mobile terminals, Shoulder-surfing attack.

1 INTRODUCTION

Recently, mobile terminals such as smartphones have come into widespread use. Most such mobile terminals store numerous types of important data, such as personal information. As a result, mobile terminals are equipped with their own display lock system that uses a personal authentication method such as personal identification numbers (PINs) in order to prevent data theft. However, most existing authentication methods are not resistant to covert observations. In other words, when a mobile terminal is unlocked using authentication information in public, authentication information may be disclosed to other individuals. Moreover, existing authentication methods do not take shoulder surfing into consideration. Shoulder surfing is the process in which authentication information is covertly and deliberately obtained by a person watching over-the-shoulder of a user as he/she completes the authentication sequence. Therefore, the research and development of an authentication method that is resistant to shoulder surfing is required.

In this paper, we propose a shoulder-surfing-attack-resistant authentication method that uses icons and a touch-panel liquid crystal display. The proposed method is resistant to covert observation, recording, and brute-force attacks. We then explain how we implemented and evaluated this authentication method experimentally.

2 BACKGROUND

2.1 Display Lock System Security

Security using the display lock system has become widespread. The display lock system is a function that changes the status of mobile terminals that have been leftidle into a locked condition so that operations cannot be performed. In such devices, it is necessary to unlock the display lock system using personal authentication information such as password input, in order to change the terminal status so that normal operations can be performed. This system is designed to prevent leakage and alteration of the information within the mobile terminals.

Mobile terminals are normally locked when put in a pocket or bag. The frequency of the authentication will increase whenever a user uses the mobile terminals. Therefore, it is important to consider the usability of an authentication method.

2.2 Existing Authentication Methods with Covert Observation Resistance

Because it is important to take measeres against covert observation in order to prevent authentication information from being stolen, covert observation re-

sistant authentication methods have been devised. Such methods do not expose the authentication information during entry, even if other individuals try to view the input process. Additionally, it should be noted that the risk of covert observation is not restricted to direct observation by other individuals, camera recordings also pose a threat. Therefore, it is necessary to make the authentication process more complex in order to prevent authentication information from being stolen even if cameras and/or other individuals observe the information input process numerous times.

There are two types of shoulder-surfing attack: direct observation attacks, in which authentication information is obtained by a person who is directly monitoring the authentication sequence, and recording attacks, in which the authentication information is obtained by recording the authentication sequence for later analysis.

2.3 Related Research

2.3.1 Android Password Pattern

The Android password pattern, which has high-usability due to its intuitive input method, is one type of recall-based graphical password system[1] and is used worldwide.

However, this authentication method has weak points to all attack methods. For example, it is not resistant to shoulder-surfing attacks[7], Therefore, if authentication entry is covertly observed even once, the password can be stolen. Furthermore, even if the authentication operation is not directly observed, the information can be deduced from the locus of the fingers inputting information on the mobile terminal screen[2].

2.3.2 Graphical Password Methods for Mobile Terminals

There are numerous graphical password methods[3, 4, 5], but many of them face the same difficulties. For example, instead of trying to guess the authentication information, a dedicated adversary could try to capture it by observing the legitimate user over the his/her shoulder when he/she logs into the system. However, in contrast with covert observation by transitory human observers (who face limitations such as poor memories, and limited computational abilities), a more serious problem is attacks by camera-equipped adversaries. In such situations, an adversary that has illegal access to security camera recordings, or who has placed a secret camera where he/she can view authentication inputs, can record any number of user-terminal interactions, and over time, extract the secret authentication data bit by bit. This attack method has a high probability of success[6].

While shoulder-surfing attack resistant authentication methods have been developed with stronger resistance than other existing authentication methods[7, 8]. However, they are difficult to use with mobile terminals.

3 PROPOSED APPROACH

3.1 Goals and Design Policy

We propose a shoulder-surfing-attack-resistant authentication method that uses icons and a touch-panel liquid crystal display. This authentication method is named "Secret Tap method. ''

The goals and design policy are described as follows.

- Covert observation resistance

  Maintain the resistance strength at a level that prevents the authentication information from being revealed to other individuals, even if the authentication operation is performed numerous times.

- Recording attack resistance

  Maintain the resistance strength at a level that prevents the authentication information from being analyzed by other individuals even if the authentication operation is fully recorded.

- Brute-force attack resistance

  Maintain the resistance strength at a level that prevents the authentication process from broken more easily than by a brute-force attack on a four digit PIN. This policy follows the standard put forth in ISO 9564-1[9].

- Usability

  Maintain a level of usability that permits operators to perform the authentication operation with ease.

3.2 Proposed Method 1: Secret Tap Method

Figure 1 shows the Secret Tap method authentication process. This method places 16 randomly selected icons in the display area, which is a 4×4 square. The user selects the authentication icon from the 16 icons and taps the selected icon. The user repeats this operation for a predetermined number of registry icons. If all of the selected icons are correct authentication icons, the authentication is successful and the mobile terminal is unlocked.

To this method, we propose adding a shift function as a way to increase shoulder-surfing attack resistance. The shift function is described as follows:

1. The user sets the shift value and icons as authentication information beforehand.

2. The 16 icons are divided into four areas, referred to as the first through fourth quadrants, as shown in Figure 1.

Figure 1. Authentication of Secret Tap method.

3. The authentication icons are the four icons in the quadrant that are rotated counterclockwise by the value of the shift from the quadrant the includes the registry icon.

4. The user taps one of the authentication icons.

For example, when the shift value is +2, the quadrant including the registry icon is the third quadrant in Figure 1. The first quadrant is shifted from the third quadrant. The user taps one of the four icons in the first quadrant as an authentication icon. When this process is used, the authentication information cannot be stolen, because the user does not have to tap the registry icons directly.

However, this authentication method has a high potential for being broken by brute-force attack because only four of the 16 displayed icons are actual authentication icons. Furthermore, while this weakness by remedied by increasing the number of registry icons, this would require users need to remember more registry icons, and thus reduce the usability of the method.

3.3 Proposed Method 2: Secret Tap with Double Shift Method

In this section, we propose an authentication method that is resistant to both shoulder-surfing and brute-force attacks. This authentication method is named "Secret Tap with Double Shift (STDS) method."

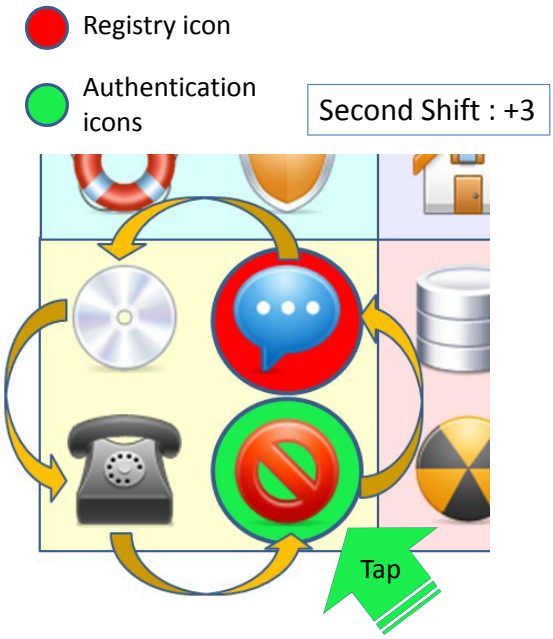

Figure 2. 2nd shift function of the STDS method, which shifts the registry icon in the quadrant.

The STDS method uses two shift types. The "first shift," which refers to the shift of icons between quadrants is the same as described in the Secret Tap method above, while the "second shift," refers to shifting the position of an icon within the quadrant.

Figure 2 shows the second shift function of the STDS method whereby the registry icon shifts within the quadrant. The second shift process is described as follows:

1. The user sets the values of the shift and icons in the same manner as Secret Tap method.

2. The four icons are arranged within the quadrant, as shown in Figure 2.

3. The authentication icon is rotated counterclockwise by the value of 2nd shift from the registry icon in this quadrant.

4. The user taps this icon.

Figure 3 shows an example of the STDS method in use. The registry icon is the upper-left icon in third quadrant. The first shift is '+2,' and the second shift is '+1.' First, the icon is rotated counterclockwise two quadrants from the registry icon as following the value of the first shift. Next, the icon is rotated counterclockwise among the quadrant icons by the value of second shift. Thus, the shifted icon is the authentication icon.

Since the authentication icon is still one of the 16 displayed icons, the STDS method can maintain a high level of resistance to brute-force attack without having to increase the number of input icons.

Figure 3. The example of using STDS method.

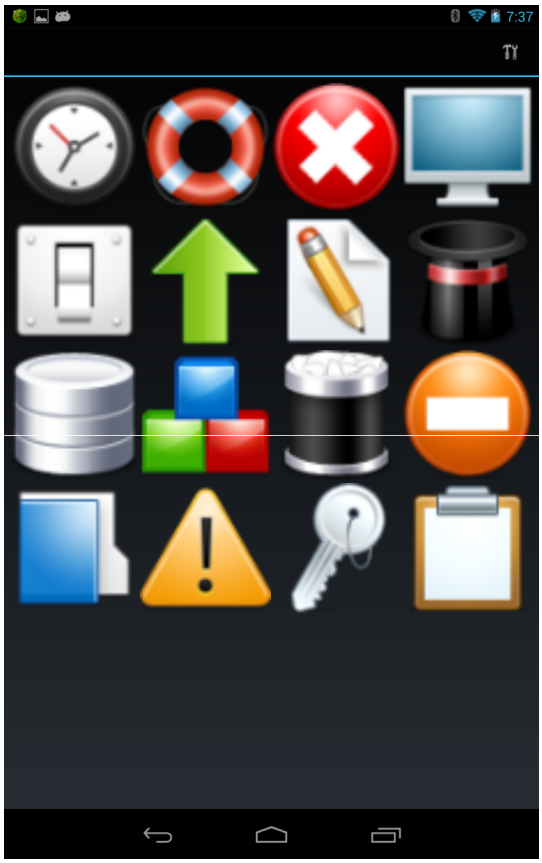

Figure 4. Implementation of a common authentication display in each method.

3.4 Implementation of the Secret Tap Method and the STDS Method

3.4.1 Basic Functions

We then applied the Secret Tap and STDS methods to mobile terminals equipped with the Android OS in order to evaluate their resistance to shoulder-surfing attacks. Figure 4 shows the implementation of the common authentication displays for each method. The user taps an authentication icon in this authentication display only a number of times equal to the number of the registry icons. If the authentication is successful, the user can exit the application or change to the registry icon selection display. If the authentication is unsuccessful, the user is directed to reattempt authentication. Figure 5 shows a common display of the registry icons selection. The user can select his/her favorites from more than 50 potential registry icons. The maximum number of registry icons that can be selected is 10.

Figure 6 shows a common display of the first shift selection. The user taps the upper-right menu (value of shift function) in the action bar, which changes this display. The shift types have five value levels: "Any Shift," "Shift +0," "Shift +1," "Shift +2," and "Shift +3." The user can select the shift value, and then register the value to tap. "Any Shift" has no-fixed value, and can be altered by the user at any time.

An example of "Any Shift" is shown in Figures 7 and 8. Figure 7 shows the situation: the first shift is "Shift +1," and the second shift is "Any Shift." Because the first shift is "Shift +1," the authentication quadrant is moved one quadrant from the quadrant that includes the registry icon. Since the second shift is "Any Shift," all the icons that are included in the destination quadrant are displayed as authentication icons. This method is the same as the "Secret Tap" method described in section 3.2.

Figure 8 shows the situation: first shift is "Any Shift," and the second shift is "Shift +1." Because the first shift is "Any Shift," all quadrants are authentication quadrants. The authentication icons are rotated counterclockwise from the upper-right of each quadrant.

If the first shift and second shift are both "Any Shift," the values of both shifts become "Shift +0" automatically.

Therefore, use of the "Any shift" value not only reduces user burden, attackers are foiled by the user ' s seemingly arbitrary selections. However, this function decreases resistance to brute-force attacks and requires additional measures, such as increasing the number of registry icons. The registry icons are only displayed once because it is necessary to maintain high resistance to recording attacks. Thus, since the registry icons cannot be inferred from a single record-

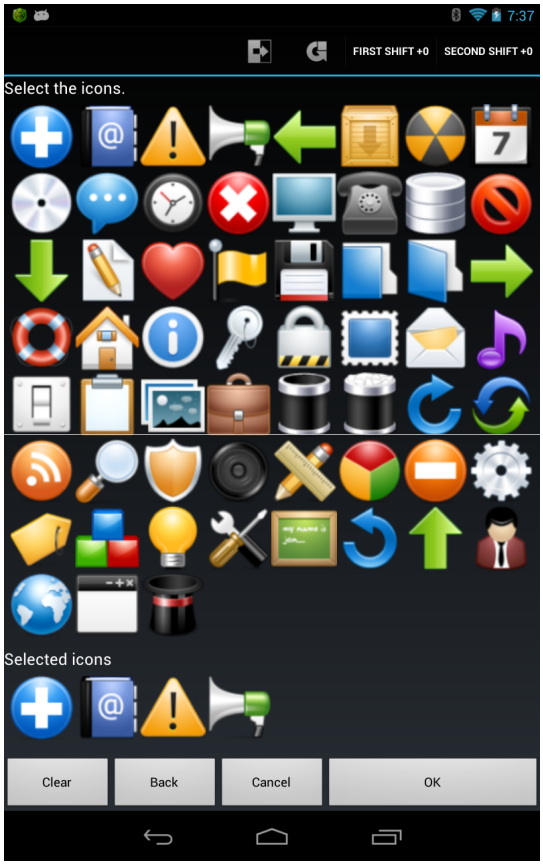

Figure 5. Common display of the registry icon selection.

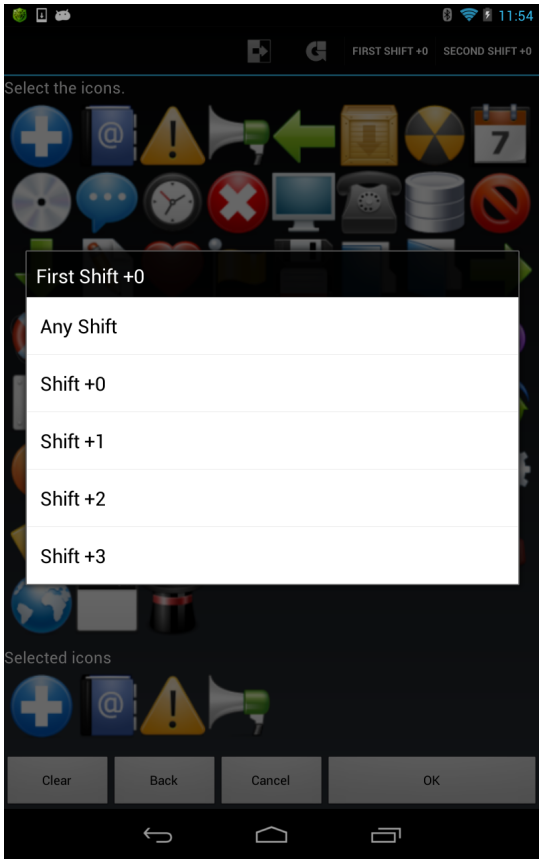

Figure 6. Common display of the value selection of shift function.

ing, such attacks can be resisted while continuing to use a small number of registry icons.

3.4.2 Fake Mode Implementation

To further boost resistance to recording attacks, we implemented the "Fake Mode" concept, an example of which is shown in Figure 9. This mode uses the vibrate function of mobile terminals. More specifically, if the mobile terminal vibrates during entry, the user is prompted to tap different icons than he or she would tap for actual authentication. This frustrates observers attempting to identify the authentication icons.

However, because this mode also decreases resistance to brute-force attacks, other measures such as increasing the number of registry icons, are also required.

4 EVALUATION

4.1 Rate of successfully broken authentication via brute-force attack

Figure 10 shows the rate of breakable authentication by brute-force attack. The target methods are PINs, Android Password Pattern, the Secret Tap method, and the STSD method. The horizontal axis indicates the numbers of input icons or characters. The vertical axis indicates the rate of successfully broken authentication via brute-force attack. The rate of 1/10,000(0.0001) is emphasized by a red line in this graph.

The number of input icons or characters necessary for the Secret Tap method is confirmed to be greater than 1/10,000 when the number of input icons is seven, and the rate of the STDS method is greater than 1/10,000 when the number of input icons is four, which is the same as for a PIN. Moreover, the resistance is higher than that of the Android Password Pattern. Thus, it can be seen that only the STDS method achieves our aimed for level of resistance to brute-force attack.

4.2 Experiment to Evaluate the Resistance to Covert Observation and Usability

The Secret Tap and STDS methods were then examined in order to evaluate their resistance to covert observations and to confirm their usability. The subjects were eight students of the Kanagawa Institute of Technology.

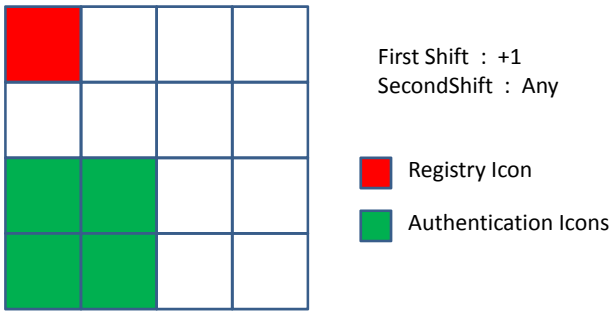

Figure 7. Example of the Any value of Second Shift.

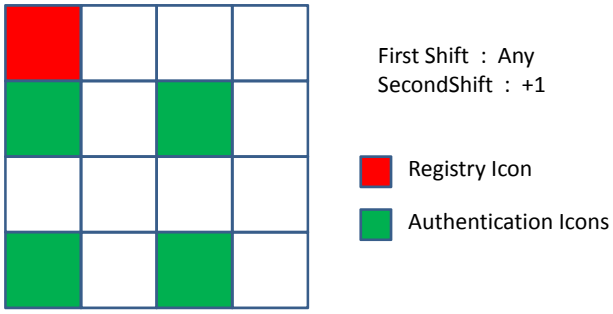

Figure 8. Example of the Any value of First Shift.

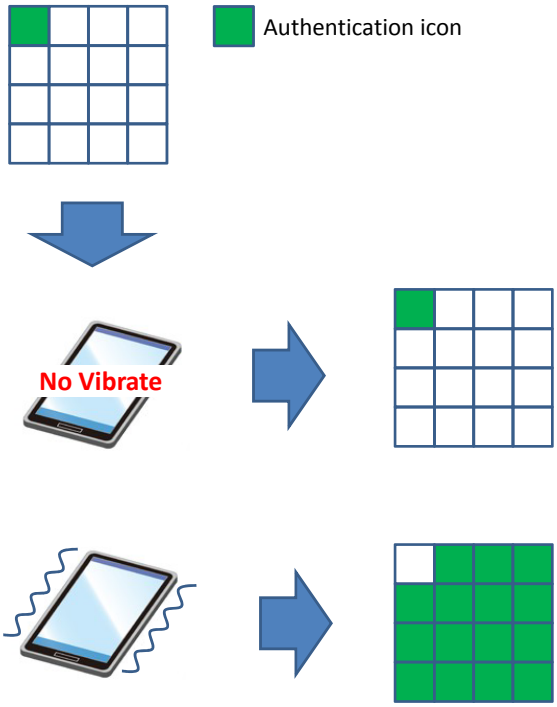

Figure 9. Example of "Fake Mode."

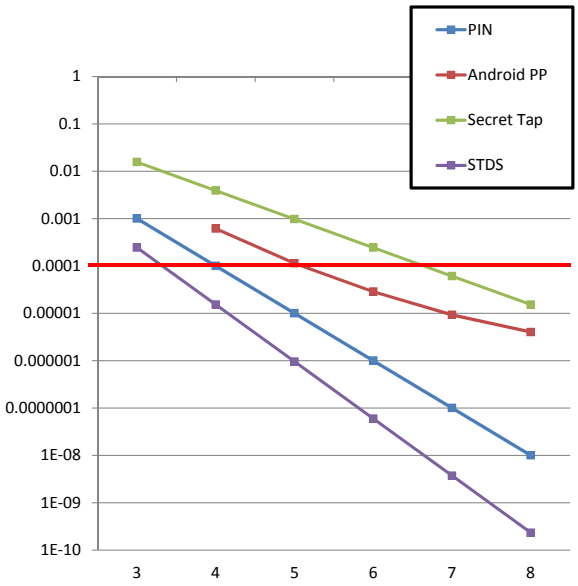

Figure 10. Rate of successfully broken authentication via brute-force attack.

4.2.1 Experiment 1: Investigation of the suitable number of registry icons

The upper limit to the number of icons that can be remembered was investigated before experimentation in order to determine the maximum number of registry icons that would still permit ease of use. This experiment was conducted as follows:

1. 1 to 10 icons, which were selected at random from 50 icons, were presented to the eight participating students.
2. The students were then presented with a display showing all 50 of possible choices, and given 15 seconds to choose the presented icon(s).

Table 1 shows the numbers of students that are able to remember all of the presented icons. All of the students were able to remember up to five icons.

However, it was found that six or more icons were difficult to remember. Thus, it was determined that five was the most suitable number of registry icons.

4.2.2 Experiment 2: Evaluation of the resistance to multiple covert observation attempts

We then evaluated the resistance to covert observations several times by experiment. The subjects were the same eight students that participated in the experiment discussed in Section 4.2.1 above. This experiment was conducted as follows:

1. First, we confirmed the students knew how to use each authentication method, i.e., PINs, Android Password Pattern, Secret Tap method, and STDS method.
2. One student was then chosen at random to act

Table 1. Numbers of students who can remember all shown icons

Number of shown icons	1	2	3	4	5	6	7	8	9	10
Number of students	8	8	8	8	8	6	3	1	0	0

Table 2. Numbers of students who cauld detect the registry icons

Detected icons	0	1	2	3	...	All
PINs	0	0	0	0	...	8
Android PP	0	0	0	0	...	8
Secret Tap method	6	1	1	0	...	0
STDS method	8	0	0	0	...	0

as the user.

3. The user set the authentication information and performed the authentication operation in the presence of the other students.
4. The other students attempted to detect the authentication information by covertly observing the authentication operation.

The numbers of registry icons, characters, and points of contact required in order to resist a brute-force attack are as follows:

- PINs: 4 numbers
- Android Password Pattern: 7 points of contact
- Secret Tap: 7 icons
- STDS: 4 icons

Table 2 shows the number of students who detected the registry icons. In the cases of PINs and Android Password Pattern, all of the students were able to detect the authentication information. However, in the cases of the Secret Tap and the STDS methods, none of the students were able to completely detect the authentication information. Thus, it is clear that our two proposed methods are resistant to covert observation attacks.

Next, we evaluated the usability of the methods by means of a questionnaire containing the following five questions:

- Comprehensibility

  Do you understand how to use the authentication method?

- Usability

  Is this authentication method is easy to use?

- Familiarity

  Will this authentication method become easier to use after gaining experience?

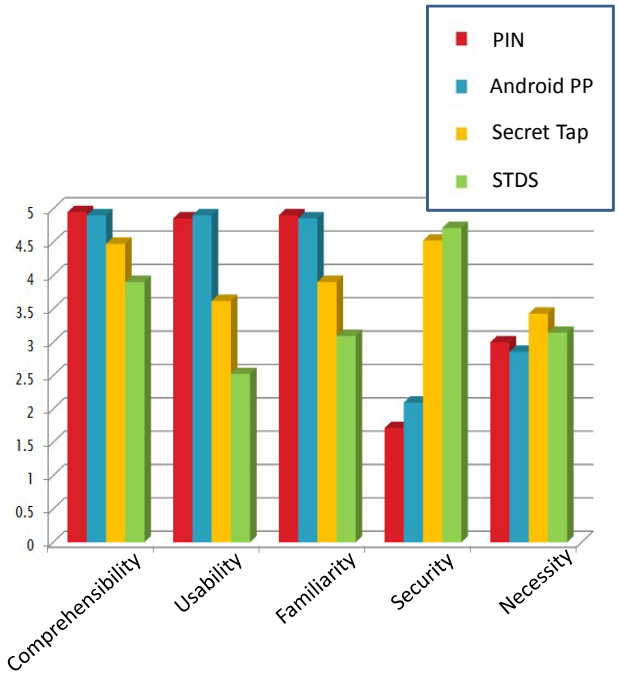

Figure 11. Evaluation of usability by user (students)

- Security

  Is this authentication method safe?

- Necessity

  Is this authentication method necessary?

For each method, the five questions were evaluated using the following rank scale (1: Very bad, 2: Bad, 3: Not bad, 4: Good, 5: Very good).

Figure 11 shows the results of the usability evaluation. The data are averages for each rank. The rankings of comprehensibility and necessity were the same for each method. In the cases of PIN and Android Password Pattern input, the usability and familiarity were good, but the security was poor. In the cases of the Secret Tap method and the STDS method, the usability and familiarity were poor, but the security was good.

Thus, as shown in Figure 11, even though the two proposed methods were designed to have acceptable levels of usability, the subjects reported both their usability and familiarity to be poor. This indicates that it will be important to improve the usability of the proposed methods in the future.

4.3 Evaluation of the Resistance to Recording Attack

Existing authentication methods are susceptible to penetration if the process can be recorded for later analysis. The proposed authentication methods are resistant to shoulder-surfing attacks because, when the proposed shift function is used, the user does not tap the registry icon directly and the registry icons are only displayed once. Therefore, the proposed methods are recording-attack resistant as well.

However, because the user fixes the registry icons and the value of the shift, penetration becomes more likely if the authentication information is shown to other individuals, or if the authentication operation is recorded several times. However, while it is important to take anti-recording measures, it is a rarely possible to record the authentication operation several times using a normal camera. Thus, it can be said that the proposed methods are sufficiently resistant to shoulder-surfing attacks.

5 CONCLUSION

In this paper, we proposed a shoulder-surfing-attack-resistant authentication method using icons and a touch-panel liquid crystal display. In order to enhance resistance to covert observation and recording attacks, this method has two shift functions, i.e., the first shift and the second shift. We then implemented the proposed methods and evaluated them experimentally. The results of our experiments indicate the proposed methods have a sufficient level of resistance to shoulder-surfing attacks.

In the future, we intend to investigate the following:

- Countermeasures to prevent numerous recording attacks.

  Because the user fixes the registry icons and the shift value, penetration of the authentication information is more likely if other individuals are allowed to observe the input operation, or if it is recorded several times. Thus, it is important to take anti-recording measures.

- Usability improvement.

  Currently, users believe that this authentication operation, which utilizes two shift functions, is difficult to use. The solution to this problem lies in developing a method that allows the authentication information input and operation to be performed more simply. However, if the authentication information is simplified, security is reduced. Therefore, it will be important to improve both the usability and security of the authentication method.

REFERENCES

[1] Biddle, R., Chiasson, S., van Oorschot, P.C.: Graphical passwords: Learning from the first generation. Technical report TR-09-09, School of Computer Science, Carleton University (2009).

[2] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge attacks on smartphone touch screens, Proceedings of the 4th USENIX conference on Offensive technologies. pp. 1-7. WOOT'10, USENIX Association, Berkeley, CA, USA (2010).

[3] Wazir, Z.K., Mohammed, Y.A., Yang, X.: A Graphical Password Based System for Small Mobile Devices, International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, pp.145-154, (2011).

[4] Arash, H.L., Omar, B.Z., Samaneh, F., Rosli, S.: Shoulder Surfing Attack in Graphical Password Authentication, International Journal of Computer Science and Information Security, Vol. 6, No. 2, pp.145-154, (2009).

[5] Luigi, C., Clemente, G.: A Graphical PIN Authentication Mechanism with Applications to Smart Cards and Low-Cost Devices, Proceedings of the 2nd IFIP WG 11.2 international conference on Information security theory and practices: smart devices, convergence and next generation networks, pp.16-35, (2008).

[6] Luigi, C., Clemente, G.: On the security of a two-factor authentication scheme, Proceedings of the 4th Workshop on Information Security Theory and Practices (WISTP 2010), pp.245-252, (2010).

[7] Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme, Proceedings of the working conference on Advanced visual interfaces. pp. 177-184. AVI '06, ACM, New York, NY, USA (2006).

[8] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: PassPoint: Design and lingitudinal evaluation of a graphical password system, International Journal of Human-Computer Studies, Vol. 63, Issues 1-2, pp.102-127, (2005).

[9] International Organization for Standardization: ISO 9564-1:2011 Financial services – Personal Identification Number (PIN) management and security – Part 1: Basic principles and requirements for PINs in card-based systems, (2011).