Proposal of a Puzzle Authentication Method with Shoulder-surfin Attack Resistance

Mirang Park* Yoshihiro Kita* Kentaro Aburada† Naonobu Okazaki‡
*Kanagawa Institute of Technology
1030 Shimo-Ogino, Atsugi, Kanagawa 243-0292, Japan
†Oita National College of Technology
1666 Oaza-Maki, Oita 870-0152, Japan
‡University of Miyazaki
1-1 Gakuen-Kibanadai-Nishi, Miyazaki 889-2192, Japan

***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, in order to prevent data theft, it is necessary to lock and unlock terminals using a personal authentication method such as personal identificatio numbers (PINs). However, most existing authentication methods have a common problem, referred to as shoulder-surfing in which authentication information is covertly obtained by peeking over the shoulder of a user as he/she completes the authentication sequence. In this paper, we propose a puzzle authentication method that is very simple and sufficientl secure, even when the authentication sequence is being watched. This method uses a grid-based authentication scheme in which a user selects four out of 16 panels, and four out of 16 positions. We also implemented the proposed method on a mobile terminal and evaluated it through experiments and questionnaire surveys.**

I. Introduction

Due to increased computing capabilities, modern mobile terminals hold massive amounts of private and potentially sensitive user data. In many cases, additional remote data are accessible through applications on the mobile terminal. This is very convenient for the users but becomes problematic should they ever lose their phone or have it stolen. Many users are aware of this problem and thus want to protect access to their devices[1]

The display lock system is a function that changes the status of mobile terminals into a locked condition so that operations cannot be performed. In such devices, it is necessary to unlock the display lock 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 a 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.

Mobile terminals are equipped with their own display lock system that uses personal authentication methods such as passwords, personal identificatio numbers (PINs), and Android unlock pattern[2] in order to prevent data theft. However, most existing authentication methods are not resistant to covert observations. In order 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-surfin attack into consideration. Shoulder-surfin is the process in which authentication information is covertly and deliberately obtained by a person peeking over the shoulder of a user as he/she completes the authentication sequence. Therefore, the research and development of authentication methods that are resistant to shoulder-surfin is required.

Existing authentication methods[3]–[15] with shoulder-surfin attack resistance are indeed more secure against peeking, but they are hard to use because they involve complex operations and much information that must be remembered. Therefore, they are not used by most users of mobile terminals.

In this paper, we present a puzzle authentication that we designed to overcome shoulder-surfin attacks while improving usability. We aim to improve the usability and the operatively in a way that users can fin fun, such as puzzle games.

II. Related Work

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 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-surfin attack resistant authentication methods have been developed with stronger resistance than other existing authentication methods[7], [8], they are difficul to use with mobile terminals.

"fakePointer"[9] is an authentication scheme which has a double-layered user interface, and uses two pieces of authentication information: passwords and disposal one-time secret

978-1-4799-4224-4/14 $31.00 © 2014 IEEE
DOI 10.1109/NBiS.2014.87

information referred to as “answer indicator”. Although this method has high resistance to shoulder-surfin attacks, the user needs to remember both background information and passwords for every authentication operation.

“Draw-A-Secret” (DAS)[10], [11], such as applied to an Android unlock pattern, is purely graphical: the user draws a secret design (the password) on a grid. DAS introduces three techniques for protecting from shoulder-surfin attack: decoy strokes, disappearing strokes, and line snaking. However, even if the authentication operation is not directly observed, the information can be deduced from the locus of the finger inputting information on the mobile terminal screen[12].

“XSide”[13] is an authentication method for mobile touch-screen devices; XSide achieves both high usability and shoulder-surfin attack resistance by utilizing a touchscreen on the front as well as a touch-sensitive area on the back of the device for password entry. However, it is costly to prepare the special devices required for XSide.

Weinshall’s method[14] is one type of authentication scheme using a challenge-response protocol. It uses 80 pictures that are presented in a panel composed of an 8×10 regular grid. The grid’s rows and columns include the numbers 0, 1, 2, and 3. The users are asked to (mentally) compute a path, starting from the top-left picture in the panel. If the picture is registered as the password, move downward from the picture; otherwise move to the right of it. Finish when reaching the right-hand side or bottom of the grid, and input the fina number as authentication information. This method is unsuitable for mobile terminals, because a large display area is necessary for the grid.

“Secret Tap with Double Shift” (STDS)[15] is another authentication scheme using a challenge-response protocol, and it is our previously proposed method. It uses 16 icons presented in a panel composed of a 4×4 regular grid. The user registers information: four icons as passwords and two rules of movement as a common key between the user and the mobile terminal. The user selects an icon that is among the four specifie as passwords and two rules from the 16 displayed icons. STDS is a secure authentication scheme against shoulder-surfin attack. However, it has low usability due to the complex operations necessary.

III. Proposed Approach

A. Goals and Design Policy

We propose a puzzle authentication method having shoulder-surfin attack resistance. 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 analyzed by other individuals, even if the authentication operation is performed numerous times.
- Brute-force attack resistance
  Maintain the resistance strength at a value of 2^{-14}, which is sufficien to prevent the authentication process from being broken more easily than by a brute-force attack on a PIN or password. This policy follows the standard put forth in “NIST Special Publication 800-63-1 Electronic Authentication Guideline”[16].
- Usability
  Maintain a level of usability that permits operators to perform the authentication operation with ease and fun.

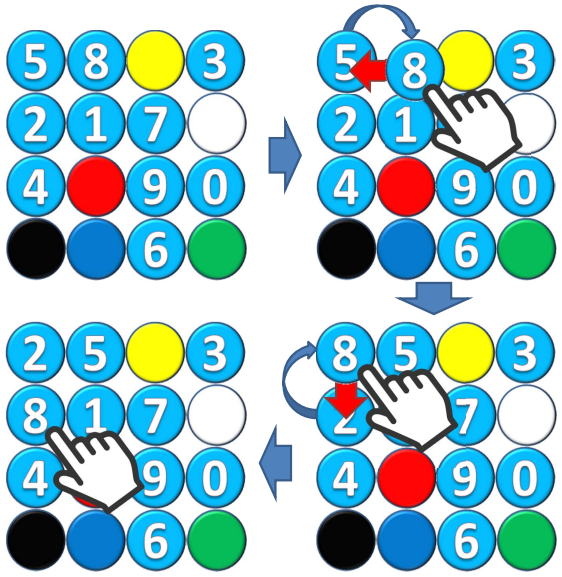

Fig. 1. Example of panel operations

B. Puzzle Authentication Scheme

We defin the following puzzle authentication scheme. This scheme uses a challenge-response protocol. The mobile terminal prepares an N-by-M array that includes random numbers from 0 to $N \times M$ (without duplication) as a challenge, and assigns to each user pass-numbers and pass-locations as common keys. Pass-numbers consist of N numbers from 0 to $N \times M$. Pass-locations are the element numbers of array, and also consist of N numbers from 0 to $N \times M$.

During authentication, the mobile terminal shows the array to the user. The user can swap any adjacent elements in an array freely. If the element numbers including a pass-number are the same numbers as pass-locations, then authentication is successful; otherwise authentication fails.

C. Example of Puzzle Authentication

Fig. 1 shows an example of panel operations. This example uses $N \times M = 4 \times 4 = 16$ panels: 0 to 9 and 6 colors. The 6 color panels are assigned the numbers from 10 to 15. These panels are placed randomly in the display area. The user registers four authentication panels and four locations.

When unlocking the display lock system, the user taps and slides any panel to place the four authentication panels at the four registered locations.

In the example of panel operations in Fig. 1, the user taps the panel ‘8’ and slides it to the panel ‘5’ location. The panel

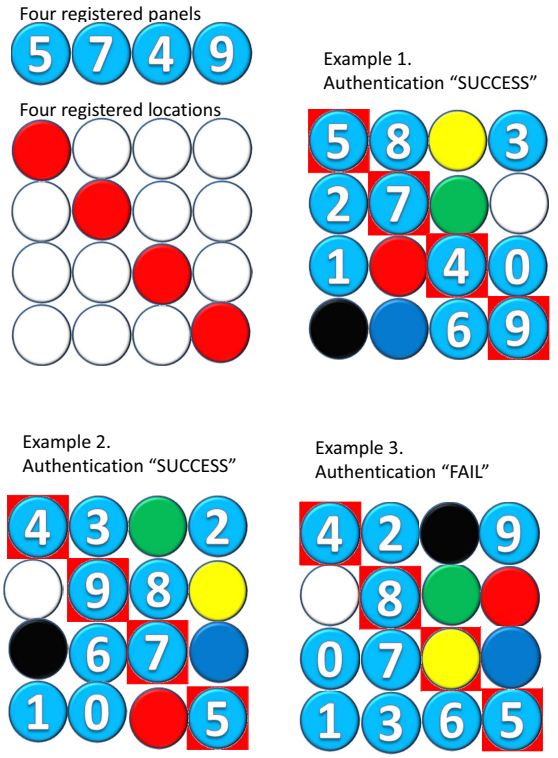

Fig. 2. Example of authentication

‘8’ is swapped with the panel ‘5’ to take its place. Then the user taps the panel ‘8’ and slide it to the panel ‘2’ location. The panel ‘8’ is swapped with the panel ‘2’ to take its place.

Fig. 2 shows an example of authentication. The user registered the four panels ‘5’, ‘7’, ‘4’, and ‘9’ as pass-numbers, and four locations (red panels) as pass-locations in Fig. 2. If the four panels are placed (in any order) at the pass-locations, authentication is successful; otherwise authentication fails.

D. Inprovement of Shoulder-surfin Attack Resistance

Min-entropy is a measure of the difficult that an attacker has to guess the most commonly chosen password used in a system[16], The min-entropy H is derived as the following mathematical expression.

$$H(bit) = -\sum_{i} P_i log_2 P_i$$

The value of resistance strength that NIST specifie is 2^{-14}. This value is transformed to min-entropy as follows:

$$\begin{aligned} H &= -\sum_{i=1}^{2^{14}} 2^{-14} log_2 2^{-14} \\ &= log_2 2^{14} \\ &= 14bits \end{aligned} \quad (1)$$

In the example in Fig. 2, N and M are 4. The numbers of combinations of pass-numbers and pass-locations are

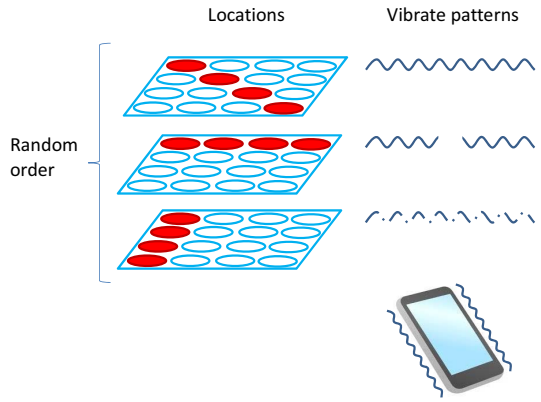

Fig. 3. Notificatio of pass-locations by vibration patterns

${}_{16}C_4 = 1,820$, and $P_i = 1,820^{-1}$. The min-entropy of puzzle authentication is derived as the following:

$$\begin{aligned} H &= -\sum_{i=1}^{1,820} 1,820^{-1} log_2 1,820^{-1} \\ log_2 2^{10} &< H < log_2 2^{11} \\ 10bits &< H < 11bits \end{aligned} \quad (2)$$

The min-entropy of our current method does not have the level of strength considered “comfortable”, which is to say that our method is weaker than existing methods for brute-force attack.

In addition, we should consider countermeasures to not only brute-force attacks but also shoulder-surfin attacks by camera. If the authentication displays and motions are recorded by camera, one needs to consider the following two cases[9]:

- Attacker has record data of the authentication displays and motions.
- Attacker has some record data of the user’s authentication motions.

It is dangerous to keep stolen authentication information. Therefore, authentication information are demanded the following two rules.

- Information that only the user knows.
- Information that is not permanently fi ed.

We propose a method to improve shoulder-surfin attack resistance. Fig. 3 shows the notificatio of pass-locations by vibration patterns. The user registers the patterns of pass-locations. As the device boots, the device vibrates and transmits the pattern of pass-locations to the user as vibration patterns. The user reads the vibration pattern, and places the passwords at the locations.

E. Implementation of Puzzle Authentication Method

We implemented the puzzle authentication method on mobile terminals equipped with the Android OS in order to evaluate our proposed method.

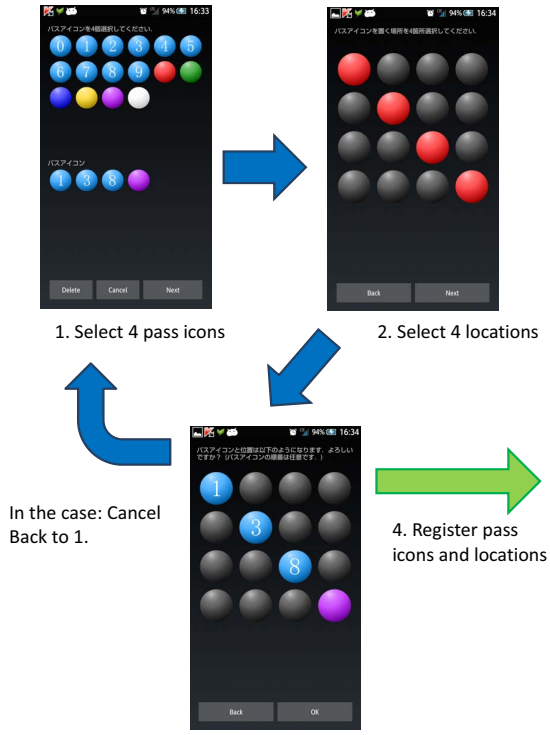

Fig. 4. Example of display of authentication information input

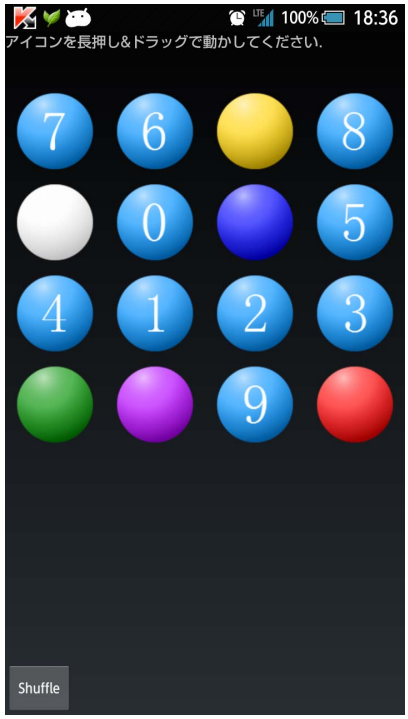

Fig. 5. Example of the display for input of the authentication information

Fig. 4 shows an example of registration of locations and the authentication panels. The user selects and taps four locations and four panels, and can confir the registration information by a confirmatio display when the user finishe the registration of the locations and panels.

Fig. 5 shows an example of the display for the input of the authentication information. The user taps and slides any of the panels, and places the four registered panels at the four registered locations. If all registered panels are located on registered locations, then authentication is successful; otherwise, authentication fails.

The bottom-left button, called the “Shuffle button, activates the rearranging function, which rearranges the elements of the array randomly, allowing unaccustomed users to swap the elements easily. This function is related to improving the usability.

IV. Evaluation and Discussion

A. Experiment on the Resistance to Covert Observation and Usability

The puzzle authentication was then examined in order to evaluate its resistance to covert observation and to confir its usability. The subjects were 15 students at Kanagawa Institute of Technology. This experiment was conducted as follows:

1) We confirme that the students knew how to use each authentication method, i.e., PINs, the Android Password Pattern, and the puzzle authentication method.
2) One student was then chosen at random to act 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.

In the case of PINs and the Android Password Pattern, all of the students were able to detect the registered panels and locations. In the case of the puzzle authentication method, none of students was able to detect the registered panels and locations. Thus, it is clear that the puzzle authentication method is resistant to covert observation attacks.

Next, we evaluated the usability of the puzzle authentication method by means of a questionnaire containing the following f ve questions:

- Comprehensibility
  Do you understand how to use the authentication method?
- Usability
  Do you feel that the authentication method is easy to use?
- Familiarity
  Do you feel that the authentication method will become easy to use after gaining experience?
- Security
  Do you feel that the authentication method is safe?

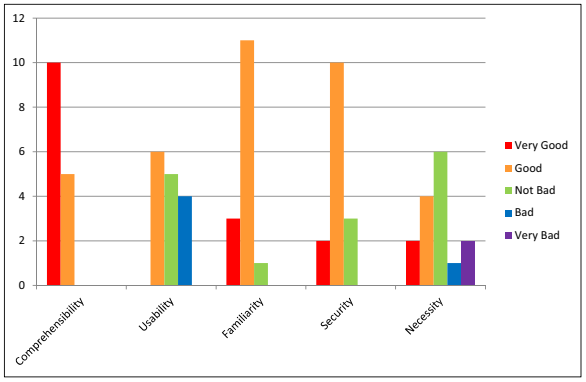

Fig. 6. Evaluation of usability by users (15 students)

- Necessity
  Do you want to use the authentication method every day?

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

Fig. 6 shows the evaluation of usability by 15 students as users. Comprehensibility, familiarity, and security were rated high, but usability and necessity received low ratings. Thus, it is necessary to improve the usability of the puzzle authentication method.

B. Rate of Successfully Broken Authentication via Brute-force Attack

We derived the strength of the reinforced proposed method as a countermeasure against brute-force attack. The number of pass-location patterns is L. L can be derived from the min-entropy of the proposed method as follows:

$$\begin{aligned} H > 10bits + L &= 14bits \\ L &= 4bits \\ &= 16 \end{aligned} \tag{3}$$

In order to maintain a comfortable security strength, the number of patterns of pass-locations needs to be 16 or more, but it is hard for users to remember so many patterns.

If N and M both increase from 4 to 5, then the combination of pass-numbers and pass-locations becomes ${}_{25}C_5 = 53,130$. The value of min-entropy is as follows:

$$\begin{aligned} H &= -\sum_{i=1}^{53,130} 53,130^{-1} log_2 53,130^{-1} \\ log_2 2^{15} &< H < log_2 2^{16} \\ 15bits &< H < 16bits \end{aligned} \tag{4}$$

Therefore, this method can achieve a comfortable level of strength. However, the usability of puzzle authentication would decrease because the information that users need to remember increases.

C. Evaluation of Shoulder-surfing Attack

Existing authentication methods are susceptible to penetration if the process can be recorded for later analysis. The puzzle authentication method is resistant to shoulder-surfing attacks, because the method uses two types of authentication information: panels and locations. Furthermore, the user is able to operate the panels without tapping the registered panels directly. Therefore, the puzzle authentication method is shoulder-surfing attack resistant as well.

However, because the user fixes the registry panels and locations, penetration becomes more likely if the authentication information is shown to other individuals, or if the authentication operation is recorded several times. While it is important to take anti-recording measures, it is rarely possible to record the authentication operation several times using a normal camera. Thus, it can be said that the puzzle authentication method is sufficiently resistant to shoulder-surfing attacks.

V. Conclusion

In this paper, we proposed a puzzle authentication method having shoulder-surfing attack resistance and improved usability. In order to enhance resistance to covert observation and recording attacks, the proposed method uses two types of authentication information: pass-numbers and pass-locations. We then implemented the puzzle authentication method and evaluated it experimentally. The results of our experiments indicate that the proposed method has a sufficient level of resistance to shoulder-surfing attacks.

In the future, we intend to investigate the following:

- Countermeasures to prevent authentication information leaks by numerous recording attacks.
- Countermeasures to prevent authentication information leaks by brute-force attacks.
- Usability improvement.

References

[1] Karlson, A.K., Brush, A.B., and Schechter, S.: Can I borrow your phone?: Understanding concerns when sharing mobile phones, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI2009), pp.1647-1650, 2009.

[2] Biddle, R., Chiasson, S., and P.C., van Oorschot: Graphical Passwords: Learning from the First Generation, Technical Report TR-09-09, School of Computer Science, Carleton University, 2009.

[3] Wazir, Z.K., Mohammed, Y.A., and 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] Lashkari, A.H., Zakaria, O.B., Farmand, S., and Saleh, R.: Shoulder Surfing Attack in Graphical Password Authentication, International Journal of Computer Science and Information Security, Vol.6, No.2, pp.145-154, 2009.

[5] Catuogno, L. and Galdi, C.: 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] Catuogno, L. and Galdi, C.: On the Security of a Two-Factor Authentication Scheme, Proceedings of the 4th Workshop on Information Security Theory and Practices (WISTP2010), pp.245-252, 2010.

[7] Wiedenbeck, S., Wates, J., Birget, J.C., Brodskiy, A., and Memon, N.: Design and Evaluation of a Shoulder-Surfin Resistant Graphical Password Scheme, Proceedings of the Working Conference on Advanced Visual Interfaces, pp.177-184, AVI'06, ACM, New York, USA, 2006.

[8] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N.: PassPoint: Design and Longitudinal Evaluation of a Graphical Password System, International Journal of Human-Computer Studies, Vol.63, Issues 1-2, pp.102-127, 2005.

[9] Takada, T.: fakePointer: An Authentication Scheme for a Better Security Against a Peeping Attack by a Video Camera, Proceedings of the 2nd International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM2008), 2008.

[10] Jelmyn, I., Mayer, A., Monrose, F., Reiter, M.K., and Rubin, A.D.: The Design and Analysis of Graphical Passwords, Proceedings of the 8th conference on USENIX Security Symposium, Vol.8, pp.1-8, 1999.

[11] Zakaria, N.H., Griffiths D., Brostoff, S., and Yan, J.: Shoulder Surfin Defense for Recall-based Graphical Passwords, Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS) 2011, No.6, pp.1-12, 2011.

[12] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., and Smith, J.M.: Smudge Attacks on Smartphone Touch Screens, Proceedings of the 4th USENIX Conference on Offensive Technologies, pp.1-7, 2010.

[13] Luca, A.D., Harbach, M., Zezschwitz, E.V., Maurer, M.E., Slawik, B., Hussmann, H., and Smith, M.: Now You See Me, No You Don't — Protecting Smartphone Authentication from Shoulder Surfers, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp.2937-2946, 2014.

[14] Weinshall, D.: Cognitive Authentication Schemes Safe Against Spyware, Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P), pp.295-300, 2006.

[15] Kita, Y., Sugai, F., Park, M., and Okazaki, N.: Proposal and its Evaluation of a Shoulder-Surfin Attack Resistant Authentication Method: Secret Tap with Double Shift, International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol.2, No.1, pp.48-55, 2014.

[16] NIST Special Publication 800-63-1 Electronic Authentication Guideline, National Institute of Standards and Technology, 2011.