Artificial Life and Robotics (2023) 28:710–717
https://doi.org/10.1007/s10015-023-00890-y

ORIGINAL ARTICLE

Development of keypads which use colors or shapes to prevent shoulder surfing

Ryo Masuzawa[1] · Kentaro Aburada[1] · Hisaaki Yamaba[1] · Tetsuro Katayama[1] · Naonobu Okazaki[1]

Received: 13 May 2022 / Accepted: 18 July 2023 / Published online: 2 August 2023

Abstract
In conventional smart phones and ATMs, a four-digit passcode is entered into a keypad, and the user confirms whether the passcode matches the keypad. However, there is a risk that a third party can easily steal the password by watching the code entry or analyzing the position of fingerprints left on the keypad. There are other solutions, such as biometric authentication or the use of special displays, but both of them are costly and difficult to implement. In this study, we propose a keypad that does not leave fingerprints on the screen, is low cost, and can be used to input passcodes without worry, even if someone is standing next to it. The proposed keypad uses cursors that are moved by directional keys to select numbers, making fingerprint analysis difficult. Because attackers do not know the color that the user has selected, they cannot know which cursor the user is moving. To verify the safety and convenience of this system, we conducted experiments on subjects in their 20 s and 50 s. The results showed that the average difference in authentication time from the conventional method was about 5 s, and the method was generally convenient. We conclude that our keypad system is secure, because no peeping attacks on a subject were successful in guessing the subject's passcode.

Keywords Keypad · Shoulder surfing · Lock screen · Smartphone

1 Introduction

Since smartphones have become widespread, the number of victims of social engineering attacks has been increasing every year. One of the most common methods of social engineering is shoulder surfing, in which a third party peeks at the screen during authentication and steals confidential information such as passcodes. This is one of the most common methods and has the highest number of victims, partly because it does not require any special technology. To increase not only security but also practicality, this paper proposes a keypad that can prevent peeping attacks with lower implementation cost and authentication time. In this authentication method, a color is registered as secret information in addition to the usual 4-digit passcode. The keypad has 3×3 squares, and each square is framed in a unique color. The positions of the digits are fixed, and the colored frames are moved by pressing the directional keys. A user enters each digit of his or her passcode by moving his or her registered color frame onto the digits and pressing the enter key (see Fig. 1). In addition, users with color blindness can also use the system by replacing the colors with shapes.

An experiment was conducted to verify the safety and convenience of our keypad system. Experiments were conducted on subjects in their 20 s and 50 s to see if there was a difference in authentication speed between older and younger subjects. We also measured the percentage of correct answers to see if the correct 4-digit numbers were typed in. In addition, to confirm the safety of the system, we asked the subjects to shoulder surf while another subject performed authentication.

This work was presented in part at the joint symposium of the 27th International Symposium on Artificial Life and Robotics, the 7th International Symposium on BioComplexity, and the 5th International Symposium on Swarm Behavior and Bio-Inspired Robotics (Online, January 25–27, 2022).

✉ Kentaro Aburada
aburada@cs.miyazaki-u.ac.jp

[1] University of Miyazaki, 1-1 Gakuen-Kibanadai-Nishi, Miyazaki 889-2192, Japan

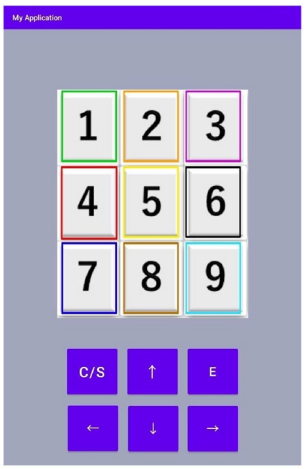

Fig. 1 Implementation screen of the proposed method

2 Related work

There are many studies on keypads that prevent shoulder surfing by third parties.

Qu and He proposed an anti-peep passcode keypad [1]. In their method, hybrid images that can be seen correctly from the distance between the user's eyes and the screen are introduced. Fuzzy logic was used to adjust the effect. By combining those two methods, only the user who is at an appropriate distance can enter the correct passcode. The hybrid image prevents third parties from peeking at the screen, and the fuzzy adaptive visual distance adjustment improves the user experience. One of the features of this method is that the only external device used is the internal camera of the smartphone, which makes it low-cost to apply and easy to disseminate.

Owada et al. proposed a method of entering secret information using a vision input device [2]. The authors developed a keypad that prevents shoulder surfing by a third party and also allows a physically handicapped person to log in easily by entering a passcode using an eye input device provided on the keypad. The authors used a method that gradually divides a normal keypad into separate parts using blinking motions, before finally narrowing it down to a single number. This method is claimed to have high peeking resistance and can be used by a wide range of users because the keypad is operated indirectly without using the hands.

Takeda proposed a user authentication scheme called "fakePointer" that can prevent shoulder surfing attacks with a video camera [3]. FakePointer uses a special pointer to select the numbers that make up the passcode. The fact that the selection is made using a pointer rather than directly with a finger is very similar to the method

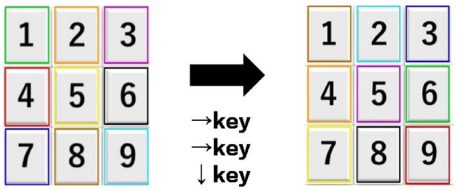

Fig. 2 Example of cursor movement

presented in this paper. The present study developed a new countermeasure against shoulder surfing attacks that does not prevent the attacker from seeing the passcode entry, but ensures a certain level of security even if the attacker sees the code entry.

In Hara and Sakurai's study [4], the security of two-step authentication is discussed. In their paper, biometrics is also cited as an example of a typical secure authentication method. However, their study also states that it is more costly than other authentication methods.

3 Proposed method

In this study, we developed a keypad that prevents prying eyes by combining a cursor with color and shape information, directional keys for moving it, decision keys for inputting information, and a conventional keypad.

3.1 Basic concept

In addition to the usual 4-digit passcode, we register a color as secret information. Users can choose their favorite color from nine colors: blue, green, brown, yellow, purple, orange, red, black, and light blue. In the initial state of the keypad, the numbers from 1 to 9 are arranged in a 3×3 tabular format in ascending order from the upper left corner. The colored frame surrounding each number is hereafter referred to as the color cursor. A user moves the color cursor over the number he or she wants to enter and taps the enter button to input the number in the color cursor instead of directly tapping numbers on the screen. For example, suppose the current keypad state is as shown on the left side of Fig. 2 and the color registered by the user is red. To enter 9 in this state, the user can tap the right arrow key twice and tap the down arrow key once to move the red cursor to 9 (right side of Fig. 2). He or she can then tap the enter key to complete the input. It is hard for attackers to identify the registered color of a user, because all other color cursors will move simultaneously in the direction of the user's pressed arrow key whenever the user moves his or her own color cursor.

In the conventional method, the passcode is selected directly with a finger. Therefore, if a third party sees the

user's fingertip at the moment of input, the passcode can be easily stolen. However, in this method, the user's finger is always on either the enter key or the directional key, and the attacker does not know which color the user has registered. Therefore, to the attacker, it appears as if various colors are moving instantaneously and randomly on the keypad while the cursor is moving, and they cannot know which color is the cursor.

The keypad in our system is connected to the top, bottom, left, and right edges of a device screen. In other words, if the color cursor is already positioned at the edge, any further attempts to move the cursor to the edge will move the cursor to the opposite side of the keypad. For example, if the user tries to move the cursor over number 3 further to the right, the cursor will move over number 1.

In addition, when the enter key is used to confirm the selected characters, if the cursor position does not change, it is easy for an attacker to discern the password. Therefore, we have devised a way to instantly change the position of all cursors in random directions when the enter key is pressed. Immediately after the enter key is tapped, the cursor position is automatically changed as if one of the four directional keys had been tapped, so that confidential information is not identified. The direction is set to be selected randomly (see Fig. 3). In other words, moving the cursor and inputting a digit look the same. Some studies have used winking or images to prevent shoulder surfing [5–7], but they have the disadvantage that the authentication method becomes very complex, thus reducing usability. In comparison, the present research is based on very simple principles, is not overly complicated, and does not restrict users.

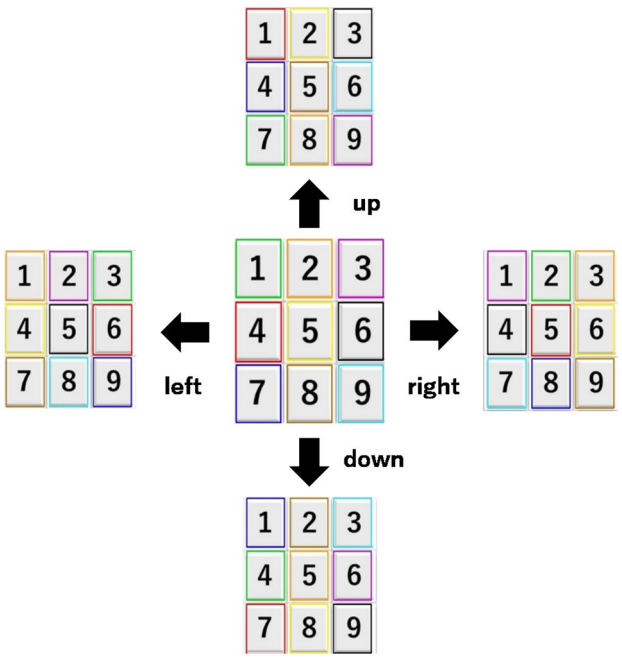

Fig. 3 Examples of movement up, down, left, and right

3.2 Layout design

The authentication method in which the user enters a few digits into a terminal and verifies that the digits match the registered passcode has been adopted in many devices that handle confidential information. Typical examples are PCs, smart phones, and ATMs. Because many of them have a single touch panel, we thought it would be practical to place the keypad, directional keys, decision keys, and other widgets on a single screen. Figure 1 shows the implemented screen of the proposed method. The goal of our research is to eventually develop an authentication method that can be applied to all devices that handle this type of authentication. For this purpose, all the parts are arranged so that they can be completed on one screen.

3.3 Role of each widget

The authentication method in this study is composed of a color cursor, a shape cursor, a directional key, a decision/enter (E) key, and a color/shape toggle (C/S) key, in addition to a keypad with numbers. The role of each widget is explained below.

3.3.1 Color cursor

The *color cursor* used in this research refers to the colored frame around each number. The user selects one of the nine colors in advance and registers it as secret information along with a 4-digit number. The user can move only the color cursor registered as secret information, and all other color cursors are dummies.

The user can enter any number by moving the self-designated color cursor over the number with the directional keys and pressing the E key. While the color cursor is moving, all color cursors move in the direction of the direction key pressed by the user. If the cursor that is already on the edge moves further out, it appears on the opposite side. In other words, all the numbers are connected up, down, left, and right, just like a map in a role-playing game. As an example, the cursor has been moved once to the left and twice up from the left in Fig. 2, and is shown on the right in Fig. 2. If you look at the green cursor in Fig. 2, you will see that before the move it was at 1, and after the move it is at 6. Moving the cursor once to the left moves the green cursor from 1 to 3. Next, moving the cursor up once moves the green cursor from 3 to 9. Then, moving the cursor up again, the green cursor moves from 9 to 6. This situation is shown in Fig. 2. This behavior in which a cursor that is already on the edge moves to the opposite side refers to the situation where the

green color cursor moves from 1 to 3 and from 3 to 9. This is commonly referred to as a torus structure, which is used in this keypad. The attacker does not know which of the nine colors the user has registered as secret information. Therefore, even if the attacker peeks at the user's screen, it will appear only that colors are randomly moving on the keypad.

3.3.2 C/S key

As explained in Section 1, the cursor can be one of nine colors. Users with color blindness who cannot distinguish between similar colors, such as blue and light blue, orange and red, and red and brown, cannot handle this color-based system. Therefore, by implementing a function to change the color information used for the cursor to shape information, users who have difficulty distinguishing colors will be able to use the alternative shape cursor. In addition, it can be used comfortably even when it is difficult to distinguish the color of the cursor due lighting conditions during use.

By tapping the C/S key, users can freely switch between the color cursor and shape cursor. Figure 4 shows the screen after switching cursors to the shape cursor. As with the color cursor, users who wish to use the shape cursor need to register their own shape cursor as confidential information in advance.

3.3.3 E key

When pressing the E key to enter a number, if the cursor stops moving once, the attacker can identify the timing of the entry, that is, know exactly when a number is being entered. Therefore, if the attacker happens to hit the color cursor that he or she has spotted, the password can be stolen by remembering the timing of the four times the user entered the numbers. Even if the color cursor that the attacker has spotted is wrong, if it is seen nine times, the password will be identified. To solve this problem, it is important to prevent the attacker from identifying the moment when the numbers are entered.

In our system, to prevent the attacker from identifying the moment of input, all cursors move once in one random direction, up, down, left, or right, the moment the E key is pressed. In other words, the E key not only inputs the number under the user's own cursor, but it also takes on the function of forcing the cursor to move once in any of the four directions at the same time. Because the cursor moves when the user is entering numbers, this prevents the attacker from knowing the timing of the input. Even if the attacker could identify the timing of the input by watching the user's finger and seeing the moment the E key is pressed, he or she would not be able to identify which number was selected because the location of the color cursor changes at the moment the E key is pressed. Unless both the color cursor and the E key are watched at the same time, the attacker will not be able to identify the number the user has entered.

A normal keypad often has a password entry field like "• • • •" that lets users check how many numbers they have just entered. However, if the password is seen by an attacker, there is a risk that it will give the attacker information about the timing of the user's input and how many characters have already been inputted. Therefore, it is not employed in our system.

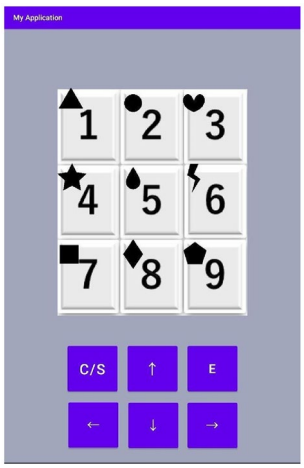

Fig. 4 Screen appearance after switching to the shape cursor

3.4 Comparison with other methods

In this section, we explain the advantages of our operating methodology over those of previous studies.

Qu and He's proposed method [1] cannot defeat an attacker who peeks at the screen from right beside it, because the optical illusion effect of fuzzy images cannot be expected for a person at the same distance from the screen. However, the proposed method in our study is not limited by the distance from the screen. In addition, our method is not as complicated as fakePointer [3], and the average authentication time is shorter.

Owada et al.'s work [2] does not require the user to use his or her hands, making authentication possible for people with hand impairments. In addition, because the authentication is performed using eye movements, it is also resistant to peeping. However, this authentication method is not easy for any person to use, because the difficulty of closing only one eye varies from person to person. In addition, there are concerns about cost and compatibility because of the need for a separate camera. In contrast, our study does not require any special skill and can be used with media that do not have a camera mounted.

3.5 Implementation

Our method was implemented using Kotlin for the Android version and Python for the PC version. In the proposed method, the white keypad area with numbers, the color cursor, and the shape cursor are displayed as an image, and the coordinates are used to determine which number is selected. The directional, E, and C/S keys were made into buttons and placed at the bottom of the screen to make them easy for users to use and difficult for attackers to see. To make it difficult for an attacker to determine which button users are pressing, all buttons are as close together as possible.

In the proposed method, because various colors are used for the color cursor, the background and buttons are set to be unified in darker shades to make them easier to see. When the correct passcode is entered, the word "SUCCESS" is displayed at the bottom of the screen using the makeText method of the Toast class, and the lock is released. If a different passcode is entered, "FAILED" is displayed in the same way to notify the user. An example of the display of the authentication result is shown in Fig. 5.

3.6 Authentication procedure

The authentication procedure of the proposed method is explained below using a concrete example.

We assume that the user's secret information is the color red, and the 4-digit passcode, is 4649.

3.6.1 Switch cursor

First, if needed, the user presses the C/S key to switch the cursor according to the situation. The default setting is to display a color cursor, so users with color blindness or in situations where it is very difficult to distinguish colors should use this button first to switch to a shape cursor.

3.6.2 Move the cursor

After deciding on the type of cursor they want to use, users then move the cursor they registered in advance to select numbers for input. In our example, the color is red and the passcode is 4649, so we first move the red color cursor to the location of 4.

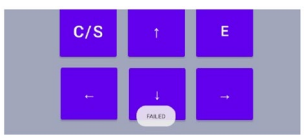

Fig. 5 Example of notification after a failure

3.6.3 Press the E key to enter the number

Once the position is fixed, a user can enter the number selected by the cursor by pressing the E key. Then, from the state after moving in four random directions, the user moves the cursor again to the top of the second digit, 6, and presses the E key. This process is repeated to enter the four digits. If the 4-digit number entered by a user matches the registered 4-digit passcode, the authentication is successful and the lock is released. Figure 3 shows an example of four patterns of movement when the E key is pressed with the red cursor at 4.

4 Experiments for evaluating convenience and safety

4.1 Purpose of the experiments

The purpose of the experiments was twofold. First, we evaluated whether the implemented keypad is easy to use, based on the percentage of successes and the completion time. Also, we evaluated the security of the keypad as a login method by comparing it with conventional keypads.

4.2 Experimental environment

The keypad in this study was implemented on a Lenovo TB-X306F tablet with the Android operating system.

For comparison with a conventional system, we used the standard keypad on the iPhone12 Pro Max. The conventional keypad on the iPhone is shown in Fig. 6.

4.3 Experimental procedure

The experimental procedure is described below.

4.3.1 Description

For each subject, we first explained the authentication procedure described in Sect. 3.5. Then, we explained the difference between the color cursor and the shape cursor, and the reason why the cursor moves randomly up, down, left, and right after input, using specific examples.

Fig. 6 iPhone12 keypad

4.3.2 Practice

Each subject was asked to practice the keypad used in this study until he or she felt sufficiently comfortable with it.

4.3.3 Login

Using the proposed keypad, each subject was asked to log in three times in a row using different passcodes. At this time, the experimenter recorded the time required from the time the cursor actually appeared to the time the login succeeded or failed.

4.3.4 Evaluation

After the measurement of each subject was completed, a questionnaire survey was conducted to evaluate the usability of the system. In this survey, we used the System Usability Scale (SUS), which is an index to measure the usability of a system.

4.4 System usability scale

The SUS [8, 9] was developed by Brooke in 1986 as an evaluation index for character-based PCs. Since then, it has also been used as an evaluation axis for cell phones, hardware, and interactive voice response. The following 10 statements were used in the evaluation:

(1) I would like to use this keypad often.
(2) I felt that this keypad was complicated enough to require explanation.
(3) I thought that this keypad is easy to use.
(4) I feel that I need an expert's support to use this keypad.
(5) I felt that the contents and navigation on this keypad were sufficiently consistent.
(6) I felt that there were many inconsistent parts in this keypad.
(7) I think most people will quickly figure out how to use this keypad.
(8) I felt that this keypad was very difficult to operate.
(9) I am confident that I can use this keypad.
(10) I think there are many things I need to know before I start using this keypad.

Odd-numbered statement: subtract 1 from the response number Even numbered statements: 5 minus the response number

All items were rated on a scale of 0 to 4, and the total number added together is multiplied by 2.5 to convert it to a scale of 0–100. If the score for each item is N1 to N10, the total score S can be expressed by equation 4.1.

$$S = \left(\sum_{i=1}^{10} N_i \right) \times 2.5. \tag{4.1}$$

The higher the value for each scale, the better the system is rated. The SUS scale has an average score of 68 from a survey by Sauro et al. [8], and a score of over 80.3 is required to be in the top 10% with excellent usability.

4.5 Results and discussion

Figure 7 shows the experimental results. Twenty-three subjects, identified as A to W, were asked to enter their passwords three times each using the proposed and conventional methods. Subjects E–W were in their 20 s, and subjects A–D were in their 50 s. The vertical axis of the graph shows the time taken for each subject to complete the input. The average completion time for the proposed method was 6.09 s, and the average completion time for the conventional method was 1.34 s. The difference is about 5 s, indicating that the proposed method takes more time than the conventional method. However, because it took less than 10 s on average, it is not expected to have a significant impact on convenience. The failure rate of the proposed method was 20.8% and that of the conventional method was 5.8%. The failure rate is considered to be higher, because the operation is more complex than that of the conventional method. However, because many subjects use the conventional authentication procedure frequently, the fast completion time and the high rate of successes are likely to be influenced by habituation. It is possible that the proposed method will also show better results than those of the current experiment when it is used

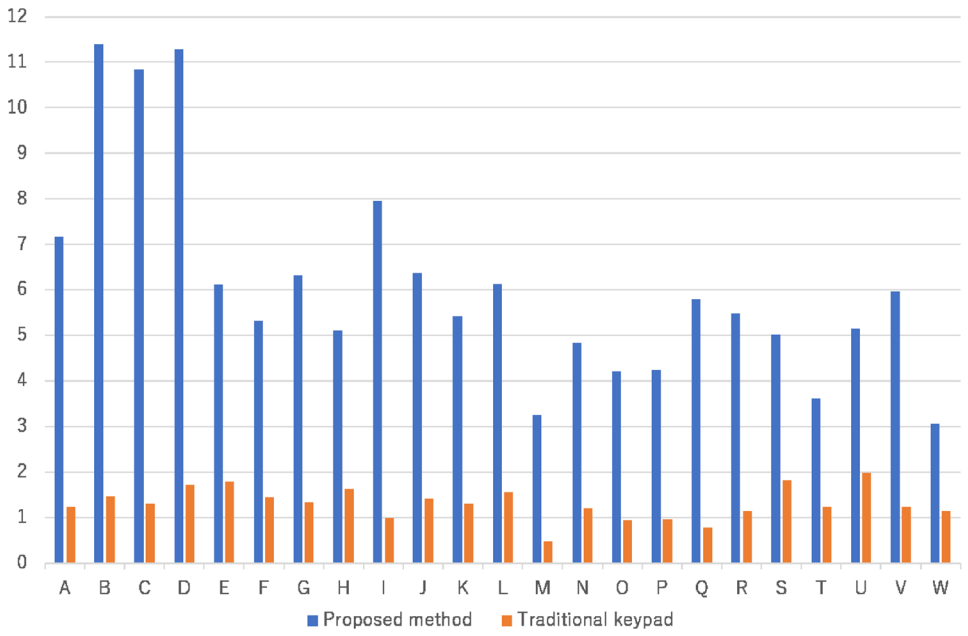

Fig. 7 Comparison of input time between the proposed and conventional keypads

for a long time. Comparing the average response times of the conventional method between subjects in their 20 s and 50 s, we found that subjects in their 20 s took an average of 5.23 s and subjects in their 50 s took an average of 11.15 s, indicating that older subjects tended to need a longer completion time. These results suggest that it may take more time for the elderly to understand and become accustomed to this system, which is more complicated than the conventional method.

All subjects were asked to play the role of an attacker, peeking at the screen where another person was typing and guessing the passcode. An experiment was conducted to verify the percentage of correct answers. As a result, no one peeked at the keypad of the proposed method and guessed the correct passcode. In the case of the conventional method, 100% of the subjects were able to discern the passcode. This shows that the proposed method is much more secure than the conventional method.

Based on the questionnaires of five subjects, the SUS score was 74% (Sect. 4.4), we can say that the score is higher than average because the average score is 68%. This resulted in high usability as well.

5 Summary and future tasks

In this study, we developed, implemented, and evaluated a keypad that uses color and shapes to resist shoulder surfing by third parties. Conventional keypads have the problem that passcodes can be easily stolen by a third party who peeks at them or analyzes the position of fingerprints left on the keypad.

Therefore, we developed a keypad that allows users to input passwords without leaving their fingerprints on the keypad and without the need to select numbers directly with their fingertips by indirectly selecting numbers with a cursor.

Experimental results confirmed that the

proposed method is more secure than conventional keypads and does not significantly impair convenience. In addition, the proposed method requires the user to memorize unique secret information different from the passcode, whereas the fakePointer method [3] requires the user to use the one selected by the system each time during authentication. In other words, it is simple and the time required for authentication is short. Therefore, this method is suitable for use in credit card transactions in stores and at ATMs, where a certain degree of speed and confidentiality are required at the same time, because it is more practical than the fakePointer method for these applications. However, if the user's color is somehow known to an attacker, there is a risk that the password will be deciphered the next time it is observed, unlike the fakePointer method. Therefore, as with conventional passwords, it is necessary to change the color information on a regular basis.

Future work is required to further improve the convenience and reduce the time needed to unlock the keypad, because it takes about 5 s more to unlock the new keypad than the conventional keypad. The proposed keypad is more complicated to use than a conventional keypad and, therefore, requires sufficient explanation and more time for children and the elderly to get used to it. Therefore, it is necessary to add a simpler screen structure and a navigation system that make it easier to understand the usage procedure.

Video attack resistance remains a major problem. If the screen of the user and the terminal are accurately recorded from behind, the video can be analyzed later to identify up to nine passcodes, and from there, the passcodes can be easily detected by a brute force attack. In the future, we would like to solve these problems and turn the system into a more practical one with improved convenience and safety.

Also, in the future, we would like to make it practical for use in all terminals that handle passcode authentication methods, such as ATMs and electronic payment terminals in stores.

Acknowledgements This work was supported by JSPS KAKENHI Grant Numbers JP21K11849, JP22K12013, and JP20K11812.

References

1. Hongchun Qu, Linsheng He (2020) "An anti-peep passcode keypad based on hybrid image and fuzzy adaptive visual distance adjustment," Chongquing University of posts and Telecommunications, IOP Conference Series: Materials Science and Engineering
2. Owada H, Kamitai D, Inoue C, Okamoto M (2019) A secret information input method using a sight input device. Proceedings of the Future Technologies Confference, pp. 936-943, February
3. Takeda Tetsuji (2008) fakePointer: a user authentication scheme that makes peeping attack with a video camera hard. IPSJ J. 49(9):3051–3061 (**In Japanese**)
4. Hara D, Sakurai K (2020) Current status and issues related to vulnerabilities of two-factor authentication (in Japanese). IPSJ SIG Technical Report. https://www.ipsj-kyushu.jp/page/ronbun/hinokuni/1009/Papers/B3-5.pdf. Accessed 28 Apr 2023
5. Thakare SV, Gore DV (2013) 3D security cloud computing using graphical password. Int J Adv Res Comput Commun Eng 2(1):945–949
6. Tanaka Ryosuke, Kashima Masayuki, Sato Kiminori, Watanabe Mutsumi (2015) The development of PIN code input system strong to multiple shoulder hacking. ITE Tech Rep 39(43):35–38 (**In Japanese**)
7. Ho PF, Kam YH-S, Wee MC, Chong YN, Por LY (2014) Preventing shoulder-surfing attack with the concept of concealing the password objects information. Sci World J 2014:12
8. Sauro J (2011) February 3, Measuring Usability with the System Usability Scale (SUS). https://measuringu.com/sus/ Accessed 03 Dec 2021
9. https://marketing-sphere.blogspot.com/2014/05/sussystem-usability-scale.html. Accessed 10 Dec 2021 (**In Japanese**)