Examination of personal authentication method achieving shoulder-surfi
ing resistance by combining mouse operation and number matrix

Kensuke Sakamoto¹, Makoto Nagatomo¹, Naonobu Okazaki², and Mirang Park¹a)
¹ Kanagawa Institute of Technology,
1030 Shimo-Ogino, Atsugi, Kanagawa 243–0292, Japan
² University of Miyazaki,
1–1 Gakuen-Kibanadai-Nishi, Miyazaki, Miyazaki 889–2192, Japan
a) mirang@nw.kanagawa-it.ac.jp

Abstract: Currently, personal authentication is used in many areas, and typically involves password authentication with a keyboard, but authentication information is easily leaked by shoulder surfing. We previously proposed an authentication method using mouse operation, which can be used with shared PCs and in public places. However, its usability was low. Thus, here we propose an improved method that can be performed by operating a mouse to manipulate cells of a number matrix displayed on a screen. We implemented the proposed method and conducted experiments on its usability and shoulder-surfi
ing resistance. Questionnaire results showed that the usability of the proposed method is improved, and no shoulder surfer could obtain complete authentication information.

Keywords: personal authentication, shoulder-surfi
ing resistance, computer mouse

Classification: Multimedia Systems for Communications

References

cursors to secure on-screen password entry,” CHI2013, pp. 2399–2402, 2013. DOI:10.1145/2470654.2481331


1 Introduction

In public places, such as offices and cyber cafés, a keyboard is generally used for password authentication on a PC. This method has the problem of being vulnerable to another person obtaining authentication information by peeking at the monitor during authentication. This is called a “shoulder-surfing attack”. Users can prevent shoulder-surfing attacks by hiding authentication operations, but it is difficult to hide the keyboard during authentication.

Thus, researchers are currently looking for personal authentication methods with shoulder-surfing resistance [1]. SECUREMATRIX [2] is an authentication method that uses information in 4×4 matrices. The user selects positions by entering numbers on the keyboard. The positions are not revealed if the numbers are leaked due to random numbers in the matrices. However, positions can leak if the keyboard and display are viewed at the same time.

CursorCamouflage [3, 4] is an authentication method in which a user inputs alphanumeric characters using a software keyboard. During the authentication phase, dummy cursors are displayed in addition to the real cursor. However, the authentication information can leak because a shoulder surfer can also detect the real cursor.

We previously proposed a personal authentication method using mouse operations with shoulder-surfing resistance [5]. However, the method did not have high usability. Therefore, in this paper, we propose an improved method using a number matrix in addition to mouse operations. We implemented the improved method to investigate usability, improvement of authentication time by familiarization, and shoulder-surfing resistance.

2 Proposed method using mouse operations and number matrix

2.1 Overview

Here we describe our personal authentication method using mouse operations. The input interface is a common three-button mouse, and the output interface is an N×N matrix. Authentication information comprises positions. The user moves from the initial position to the registered positions by mouse clicks during the authentication phase. In the pattern method [5], the current position is not displayed on the monitor in order to strengthen it against shoulder-surfing attacks. However, it is difficult for users to discern the current cursor position. In contrast, the proposed method displays the current position on the monitor by displaying numbers in a matrix. The registration and authentication procedures of the proposed method are as follows:
Registration phase:
1. A $N \times N$ number matrix is displayed.
2. The user clicks the positions that he or she wants to register.
3. Numbers from 1 to $N^2$ are displayed (for each position).
4. The user clicks the number corresponding to each position.

Authentication phase:
1. A $N \times N$ number matrix is displayed with the same size as that used in the registration phase.
2. The user finds the registered number on the matrix.
3. The user moves the registered number to the registered position by mouse operations. All numbers on the matrix are moved in the same direction when the user clicks a mouse.
4. The user selects the current position by clicking the left or right button and the wheel button together. The numbers on the matrix move in the direction indicated by the click.
5. The user repeats steps 3 and 4 according to the number of digits registered.
6. After selecting the final registered position, the user camouflages it by moving the current mouse position several times.

2.2 Implementation of proposed method
We implemented the proposed method using Java in Eclipse for Windows 10. We set the size of the matrix to $5 \times 5$ and the number of digits to 3, as implemented in [5]. Thus, the number of possible combinations of the authentication information was $25P_3 \times 25 = 345,000$. Fig. 1 shows a movie of the registration and authentication phases. In the registration phase, the user selects positions and a number using the cursor moved by mouse operation. In the authentication phase, the registered positions, current positions, and specified positions are surrounded by blue, yellow, and purple squares, respectively, to make them easy to identify in Fig. 1. In practice, these squares are not colored.

3 Experiment and discussion
We performed experiments to confirm the usability, measure the variation in authentication time due to familiarization, and evaluate shoulder-surfing resistance.

Fig. 1. Registration and authentication instruction video
A laptop with a 15.6-inch monitor and a Microsoft Mobile Mouse 3500 were used in all experiments. Note that the subjects operated the mouse under a desk while sitting on a chair.

3.1 Usability testing
We performed comparative experiments between the pattern method and proposed method. Subjects were 40 university students, and performed authentication five times in both methods. We measured the authentication time and success rate during authentication. In addition to these items, all subjects answered a questionnaire about comprehensibility, usability, familiarity, security, and needs. These topics were evaluated on a scale from 1 to 5.

Experimental results showed that it took 30.7 sec on average for a subject to complete authentication for the first time using the proposed method. This is about 6 sec more than that measured for the pattern method. However, authentication with the proposed method took almost the same time as that for the pattern method on the second and subsequent attempts. The average of fifth attempts was about 15.0 sec for both methods.

Authentication success rates were 66% and 87% in the pattern method and the proposed method, respectively. The reason for this is that the user can more easily discern the current position using the number matrix. Hence, we can conclude that the proposed method is easier to use than the pattern method.

Fig. 2(a) shows the results from the questionnaire. Scores for all the items in the proposed method are higher than those for the pattern method. In particular, usability is improved and user needs are better satisfied. In addition, the level of security is not reduced, even though the current cursor positions are visible.

3.2 Variation of authentication time by familiarization
We conducted experiments to determine whether familiarization during actual use would change the time required for authentication. To perform this test, 33 of the 40 original subjects performed authentication five times a day on six days over two weeks.

Fig. 2(b) shows the average authentication success time and the standard deviation for all the subjects for each day. On the first day, the average authentication time and standard deviation were about 18 sec and 6.3 sec, respectively, and the authentication time variation was large. However, on the sixth day, the average authentication time and the standard deviation were 10 sec and 2.6 sec, respectively. Thus, we found that the authentication time decreases by familiarization.

3.3 Shoulder-surfing resistance testing
We conducted experiments to evaluate the shoulder-surfing resistance of the proposed method. This experiment was conducted in an ideal environment where the shoulder-surfers could clearly see the authentication screen and hear the mouse clicks. The subjects were 15 of those from the usability testing. In the proposed method, there is a possibility of the registered number leaking if the number can be guessed, for example, if the user adopts his or her birthday as the registered number. Therefore, we performed two kinds of experiments that assumed that the registered
number is leaked or is not leaked (hereafter called experiments A and B). The experimental procedure was as follows:

1. We formed teams consisting of five people each and chose a single user from each team. Shoulder surfers were the other people on the team.
2. The user registered three positions and a number. Shoulder surfers were not allowed to see the monitor during registration.
3. The user performed 10 successful authentications. Shoulder surfers observed each authentication and tried to detect the registered positions and number. In experiment B, the user gave their registered number to the other people on the team.
4. Another team member was chosen to be the user.
5. Steps 2–4 were repeated until everyone in the team was a user once.

Table I shows the specific leakage rate for each digit. In experiment A, no surfer could identify all three positions, even though the current positions were displayed. In experiment B, the identification rate was higher than that in experiment A. Therefore, the proposed method has shoulder-surfing resistance. In addition, the proposed method has more shoulder-surfing resistance than that of the pattern method.

**Table I.** Rates of leakage of each digit and number

<table>
<thead>
<tr>
<th>Method</th>
<th>One position</th>
<th>2 positions</th>
<th>3 positions</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern method [5]</td>
<td>26.7%</td>
<td>10.0%</td>
<td>1.7%</td>
<td>—</td>
</tr>
<tr>
<td>Proposed method (exp. A)</td>
<td>11.7%</td>
<td>8.3%</td>
<td>0.0%</td>
<td>5.0%</td>
</tr>
<tr>
<td>Proposed method (exp. B)</td>
<td>15.0%</td>
<td>8.3%</td>
<td>6.7%</td>
<td>—</td>
</tr>
</tbody>
</table>
4 Conclusion

We proposed and implemented a personal authentication method that users can employ on shared PCs in public places. We evaluated its usability, increasing ease of use due to familiarization, and shoulder-surfing resistance. The success rate of the proposed method was 87%, and survey results indicated that it is easy to use. In addition, the average authentication success time after 6 days of use over 2 weeks was about 10 sec. Finally, we found that the proposed method has shoulder-surfing resistance because some authentication information was protected even under conditions favorable for leaks. Future work will be to evaluate the recording resistance and apply the authentication method to track pads.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Numbers JP17H01736, JP17K00139.