PVRotate: An Improved Vibration-Based User Authentication Method

Yutaka Hirakawa, Fumiya Hirose, and Isao Sasano

***Abstract*—In this study, we discuss password-based authentication methods that use the vibration function on smartphones. Password-based methods are relatively simple and are occasionally used as a backup when other methods fail. The main research goal in this area is to prevent shoulder surfing or video-recording attacks, which can be achieved by using vibrations to transmit secret information to users. Authentication succeeds when the user correctly incorporates the received secret information into the process. However, conventional vibration-based methods are slow, and reducing the time required would improve usability. We discuss ways of achieving this, leading us to propose a new, relatively fast authentication method that is nonetheless resistant to multiple-video-recording attacks.**

***Index Terms*—Password authentication method, multiple-video-recording attack, vibration.**

I. Introduction

Internet-based services such as banking, finance, and shopping are now commonly used worldwide. These systems all require user authentication, and many types of authentication methods have been proposed. Here, we focus on password-based authentication because it is relatively simple method and is occasionally used as a backup when other methods fail. The most popular of these methods, known as personal identification number-entry (PIN-entry), involves four-digit numerical passwords and has been adopted for ATM machines worldwide.

The main problem with password authentication is password leakage. Here, we had two main research objectives: avoiding shoulder surfing, where criminals look over the user's shoulder during authentication to steal their password, and preventing video-recording attacks, where the authentication process is video-recorded, possibly more than once. These attacks involve analyzing video-recorded authentication operations to narrow down the possible password candidates. The most challenging aspect of this work was developing a defense against multiple-recording attacks, in which the user's authentication process is recorded multiple times for analysis.

For security reasons, many authentication processes use challenge-and-response techniques where, during each authentication, the system transmits information (a challenge) to the user and the following authentication operation (response) varies depending on the information received. These steps must be performed secretly to avoid leakage. To transmit information securely, haptic or auditory information has been used in recent years.

This article focuses on a password authentication method based on the vibration function that all smartphones have. Previously, such vibration-based methods have generally been slow, but we propose an improved method that is relatively fast while still resisting multiple-recording attacks.

Manuscript received March 1, 2019; revised May 12, 2019.

Yutaka Hirakawa is with Department of Computer Science and Engineering, Shibaura Institute of Technology, Tokyo, Japan (e-mail: hirakawa@shibaura-it.ac.jp).

Fumiya Hirose is with NEC Networks & System Integration Corporation, Tokyo, Japan (e-mail: ma16084@shibaura-it.ac.jp).

Isao Sasano is with Department of Computer Science and Engineering, Shibaura Institute of Technology, Tokyo, Japan (e-mail: sasano@shibaura-it.ac.jp).

II. Related Work

Many studies have attempted to avoid private information leaking through direct observation, via so-called shoulder surfing [1], [2]. These involve criminals looking over the user's shoulder while they are entering their password in order to steal it. However, although these methods are effective against shoulder surfing, they offer no defense against attacks where the user's authentication process is video-recorded and analyzed.

Defending against video-recording attacks is relatively straightforward, but when the same user's authentication process is recorded several times, attackers can easily narrow down the list of password candidates. A few reports [3]-[5] have already discussed this problem. One approach is based on a mobile authentication method [3] that requires long passwords (more than 12 numeric digits) to prevent attacks where the user's authentication process is recorded twice. A later study [5] improved on this approach to achieve the same performance with shorter passwords, while another proposed authentication method [4] uses random selection and ambiguity to defend against video-recording attacks. However, none of these methods can deal with attacks where the user's authentication process is recorded more than twice.

In recent years, researchers have focused on such attacks, where the user's authentication process is recorded multiple times (more than twice). Two main approaches have been developed. The first uses vibrations [6]-[9], under the assumption that no-one but the user can recognize them, while the other uses sound [10], [11], requiring the user to wear earphones to prevent leakage. These sound-based approaches involve using a spoken message to transmit secret information from the system to the user, which is then used to implement a challenge-and-response technique. However, both of these approaches are rather slow, so a more rapid and easy-to-use authentication method is required.

Another issue with sound-based approaches is their

doi: 10.18178/ijfcc.2019.8.2.539

dependence on language for the message. For example, [11] proposed three different authentication methods, all using English labels and letter pronunciations, while [10] used Japanese guidance messages. The fact that the messages are language-dependent could cause difficulties for individuals unfamiliar with the language. To deal with this issue, a borderless sound interface has been proposed [12].

III. Conventional Vibration-Based Methods

A. Circle Chameleon Cursor(CCC) [8]

This section gives an overview of the Circle Chameleon Cursor (CCC) method, whose interface is shown in Fig. 1. The four boxes at the top indicate that two digits have already been selected, and the third digit is currently being entered. The center circle shows the numeric panel used for password entry. Pressing the left and right "rotate" buttons rotate the panel clockwise and counter-clockwise, respectively, while the "delete input" button is used to delete wrong input and the user presses the "enter" button when the password digit is placed on the correct place indicated by vibrations.

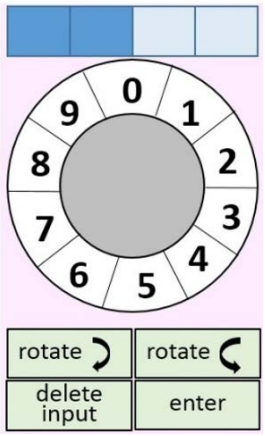

Fig. 1. CCC interface.

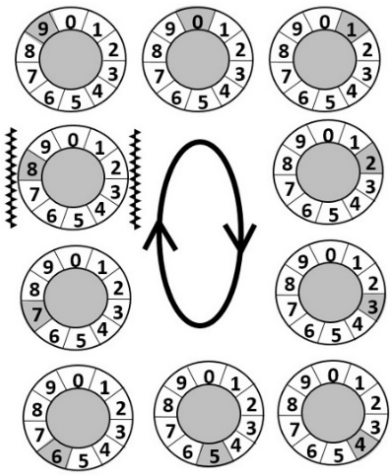

Fig. 2. Indicator movement.

The CCC system indicates each correct place where the password should be placed using vibrations. In the CCC, a four-digit password is used, and secret information for each digit is transmitted securely to the user via vibrations to prevent password leakage. In Fig. 2, the currently-indicated places are shaded. Before entering each password digit, the indicator rotates by one full turn clockwise, and the user's smartphone vibrates when it is over a certain place (the place being at digit 8 in this example). The user must then rotate the panel until the password digit is in that position (by three steps counter-clockwise in this example, if they intend to enter the password digit 1) and press the "enter" button.

This approach is resistant to video-recording attacks, even if the authentication process is recorded multiple times. However, it takes an average of 34 seconds to enter a four-digit numeric password, which is unacceptably long.

B. VibraInput [9]

Next, we discuss another conventional authentication method, called VibraInput [9]. This uses four different vibration patterns, labeled as A, B, C, and D in Fig. 3. Entering each password digit involves making two different selections. Fig. 3 shows the process for entering the password digit 1, which involves the user rotating the outer circle by touch. First, the smartphone makes the first vibration pattern, say A. The user responds by rotating the outer circle until A is next to 1. Then, the smartphone makes the second vibration pattern, say D. Again, the user responds by rotating the outer circle until D is next to 1. This process is repeated four times to enter a four-digit PIN.

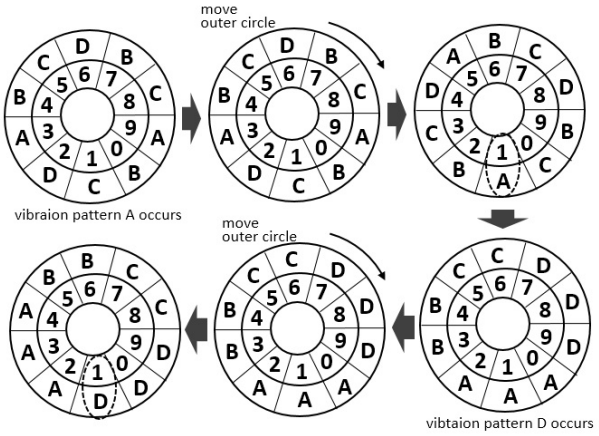

Fig. 3. Password entry via VibraInput.

With four different vibration patterns, VibraInput enables passwords to be input more rapidly: after evaluating two different interfaces, its designers found an average input time of 23.8 seconds, with authentication being successful 96% of the time [9]. VibraInput can resist video-recording attacks, but not completely, because the password candidates can be narrowed down by analyzing multiple recordings. As shown in Fig. 3, the user can rotate the outer circle to place D next to 1 in three different ways (two, three, or four steps clockwise), but users tend to select the easiest option (here, two steps clockwise). So, when they see the user move the circle clockwise in this case, the attacker can determine that the secret digit is very likely to be 1, 4, 6, or 8. They can then recalculate these probabilities by analyzing subsequent recordings, gradually improving their accuracy. A similar method of exploiting human behavior patterns to narrow down the number of password candidates is discussed in [10].

IV. Preliminary Experiment

VibraInput [9] tries to improve authentication by using multiple vibration patterns, which does speed up the process but weakens its defense against video-recording attacks. We therefore discuss another way to improve this approach in this section.

Here, we attempt to improve the CCC method [8]. The most time-consuming step is the initial rotation of the indicator around all ten numerals. This time could be reduced by either moving the indicator more rapidly or using two indicators, each only covering five digits.

The authentication interface used in this experiment is shown in Fig. 4 and Fig. 5. Fig. 4 shows two indicators, in blue and red, where the red indicator starts at P0 and the blue one starts at P5. We use a long continuous vibration for the red indicator and two short vibrations for the blue one. Each indicator only rotates by half a turn, during which either one long vibration or two short vibrations will occur. When a long continuous vibration occurs in the situation shown in Fig. 4, the password digit should be rotated to P2; alternatively, when two short vibrations occur in the situation shown in Fig. 4, the password digit should be rotated to P7.

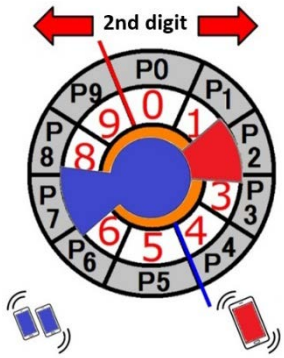

Fig. 4. Interface with two indicators.

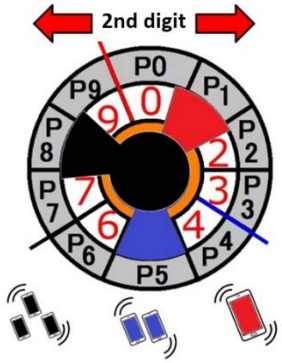

Fig. 5. Interface with three indicators.

We also considered using three indicators, adding a black indicator that uses three short vibrations, as shown in Fig. 5. These experiments also included trials with several different indicator rotation rates.

The experimental results are shown in Tables I and II. Here, Table II shows that the authentication speed increases with the indicator rotation rate, but the authentication success rate also decreases. A rotation rate of more than 4 sec/round was needed to yield accurate results with one or two indicators, but this means the process was still too slow. However, faster operation meant the success rate dropped below 90%, which is not acceptable in a real system.

TABLE I: Authentication Success Rate

		rotating speed (sec/round)				
		1	2	3	4	5
the number of indicators	1	31%	75%	88%	94%	94%
	2	75%	88%	88%	94%	94%
	3	25%	50%	75%	69%	94%

TABLE II: Operation Time

		rotating speed (sec/round)				
		1	2	3	4	5
the number of indicators	1	13.1sec	15.7sec	20.4sec	24.9sec	29.5sec
	2	14.4sec	17.0sec	20.8sec	26.9sec	31.5sec
	3	15.2sec	18.9sec	22.1sec	29.1sec	33.0sec

One issue with this method is that users must simultaneously recognize both the vibration pattern and indicator position, rapidly processing haptic and visual information correctly, which is very difficult for humans to do.

V. Proposed PVRotate Method

Building on the results of our preliminary experiments, we now describe the proposed Paired Vibration and Rotation (PVRotate) authentication method, which avoids the need to simultaneously recognize haptic and visual information.

Fig. 6. Interface of PVRotate (automatic vibration).

Fig. 7. Interface of PVRotate (manual vibration).

Fig. 6 shows PVRotate's interface. It uses four different vibration patterns: one long vibration, two short vibrations, three short vibrations, and no vibration. The outer circle is

divided into four blocks, each of which includes a number of white circles that indicates the corresponding vibration pattern. In this interface, no vibration is difficult to recognize for the users. Thus, no vibration is used only in combination with one long vibration, where only one long vibration occurs instead of two different types of vibrations.

The authentication process is as follows. Before each digit is input, the system automatically makes two different types of vibrations. The user recognizes these vibrations (haptic information), and uses them to identify where the password digit should be placed (visual information). They then rotate the inner number circle using one of the arrow buttons until the password digit is in the correct place and enter it by pressing the key-hole icon in the center of the circle.

As described above, the two vibrations are produced automatically. However, users may wish to customize when these vibrations start, so we compared this with another approach where the vibrations are not automatic but instead the user must press an icon, as shown in Fig. 7. Here, touching the red smartphone icon starts the first vibration, and touching the blue icon starts the second vibration. We also considered whether or not to allow the user to repeat the vibrations, resulting in the following four methods.

Method 1: Both vibrations occur automatically, and only happen once.

Method 2: Both vibrations occur automatically, and can be repeated at the user's request.

Method 3: Each vibration occurs when the icon is pressed, and only happens once.

Method 4: Each vibration occurs when the icon is pressed, and can be repeated at the user's request.

VI. Evaluation

This section demonstrates the evaluation results of the proposed four methods described in the previous section. Ten student volunteers evaluated these four methods, each in a random order. After a short practice session, each student carried out the authentication process four times for each method using four-digit passwords. Table III shows the results of this evaluation.

TABLE III: Evalustion Results

	success rate	operation time	min time	max time
meth1	93%	18.6sec	14.1sec	25.0sec
meth2	90%	20.6sec	14.1sec	38.5sec
meth3	95%	21.9sec	15.7sec	35.2sec
meth4	98%	23.6sec	14.9sec	36.4sec
average	94%	21.2sec	14.1sec	38.5sec

TABLE IV: Comparison

method	operation time	success rate
CCC [8]	34.3sec	91%
VibraInput [9] (average)	23.8sec	96%
PVRotate (average)	21.2sec	94%

Here, we can see that allowing the vibrations to be repeated increased the authentication time. It also increased the success rate for Method 4 but, for some reason, reduced the success rate of Method 2. Although we expected that manual (non-automatic) vibration would reduce the authentication time, the reverse was true. However, it did improve the success rate. We also found that the time taken tended to decrease as the volunteers repeated the same method, indicating that they may not have been trained on each method for long enough before beginning the evaluation.

Table IV compares our approach with the conventional methods (CCC [8] and VibraInput [9]), showing the average results presented by the original authors. Here, we see that while the proposed method is slightly faster than the other methods, its success rate is slightly lower than that of VibraInput. However, it is still comparable to VibraInput in terms of both authentication time and success rate, and is fully resistant to multiple-recording attacks. In contrast, VibraInput allows the password candidates to be narrowed down by analyzing multiple video recordings of the user.

VII. Conclusions

This study discusses a password authentication method using vibrations on smartphones. No conventional method satisfies both short operation time and concrete tolerance against multiple video-recording attacks. The proposed PVRotate requires a reasonably short time for authentication operation while maintaining concrete tolerance.

To our knowledge, the proposed method is novel, and it satisfies the following aspects: 1) it is a PIN-entry method; 2) merely four numerical digits of password need to be remembered; 3) no additional equipment is needed, but vibrations are used to transmit secret information to users for each digit of password input; 4) it is tolerant against multiple video attacks because a narrow down technique for password candidates is yet unknown; and 5) authentication operation is fast enough in comparison with other tolerant methods using vibrations.

Although the usability is improved, it is not enough. Further improvements are desired.

References

[1] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proc. CCS'04*, 2004, pp. 236-245.

[2] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proc. IEEE Advanced Information Networking and Applications Workshops*, 2007, pp. 467-472.

[3] S. Sakurai and T. Munaka, "Resistance evaluation of user authentication method using matrix against shoulder surfing," *IPSJ Transaction*, vol. 49, no. 9, pp. 3038-3051, 2008.

[4] Y. Hirakawa, "Random board: password authentication method with tolerane to video-recording attacks," *International Journal of Innovation Management and Technology*, vol. 4, no. 5, pp. 455-460, 2013.

[5] Y. Hirakawa, T. Itoh, and K. Ohzeki, "A new numerical password authentication method," *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 12, no. 4, pp. 7-15, 2013.

[6] K. Hinokuma, Y. Kita, H. Yamaba, S. Kubota, M. Park, and N. Okazaki, "A study of puzzle authentication method with video recording attack resistance," IPSJ Technical Report, vol. 2015-IOT-31, no. 4, pp. 1-6, 2015.

[7] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in *Proc. TEI '11*, 2011, pp. 197-200.
[8] M. Ishizuka and T. Takada, "Shoulder surfing resistant authentication system by using vibration," in *Proc. IPSJ Computer Security Symposium*, 2013, vol. 2013, no. 4.
[9] T. Kuribara, B. Shizuki, and J. Tanaka, "VibraInput: Two-step PIN entry system based on vibration and visual information," in *Proc. CHI 2014*, 2014, pp. 2473-2478.
[10] Y. Hirakawa, Y. Kogure, and K. Ohzeki, "A password authentication method tolerant to video-recording attacks analyzing multiple authentication operations," *International Journal of Computer Science and Electronic Engineering (IJCSEE)*, vol. 3, no. 5, pp. 356-360, 2015.
[11] M. Lee, H. Nam, and D. Kim, "Secure bimodal PIN-entry method using audio signals," *Computer and Security, Elsevier*, vol. 56, pp. 110-150, 2016.
[12] Y. Hirakawa, K. Kurihara, and K. Ohzeki, "Borderless interface for user authentication method tolerant against multiple video-recording attacks", in *Proc. of 2017 International Conference on Computer Systems, Electronics and Control*, 2017, pp. 1144-1148.

Yutaka Hirakawa was born in Hamamatsu, Shizuoka, Japan, in 1956. He received B.S., M.S., and Ph. D. degrees from Kobe University in 1976, 1980, and 1991, respectively. In 1980, he joined the Nippon Telegraph and Telephone Corporation. He is currently a professor at the Shibaura Institute of Technology. His current interests include user authentication methods, distributed algorithms, and content delivery methods. He is a member of the IEEE Computer Society, the Institute of Electronics, Information and Communication Engineers of Japan (IEICE), the Institute of Image Electronics Engineers of Japan (IIEEJ), and the Information Processing Society of Japan (IPSJ).

Fumiya Hirose born in Tsukuba, Ibaraki, Japan, in 1994. He received B.S. and M.S. degrees from the Shibaura Institute of Technology in 2016 and 2018, respectively. His current interests include user authentication methods and IT technology in general. He joined the NEC Networks & System Integration Corporation in 2018. He is a member of the Information Processing Society of Japan (IPSJ). He received the Best Paper Award for Young Researcher of IPSJ National Convention in 2018.

Isao Sasano was born in Okayama, Japan, in 1973. He received B.E., M.E., and Ph.D. degrees from the University of Tokyo in 1997, 1999, and 2002, respectively. He was a research fellow of the Japan Society for the Promotion of Science from 2001 to 2003, a visitor at the Oxford University Computing Laboratory from 2002 to 2003, a research associate at JAIST from 2003 to 2005, a research associate at Tohoku University from 2005 to 2007, an assistant professor at Tohoku University from 2007 to 2008, and an assistant professor at the Shibaura Institute of Technology from 2008 to 2012. He has been an associate professor at the Shibaura Institute of Technology since 2012. He is interested in programming languages in general and program development systems in particular. He is a member of the Association for Computing Machinery (ACM), Japan Society for Software Science and Technology (JSSST), and the Information Processing Society of Japan (IPSJ).