

# Improvements in a Puzzle Authentication Method

Yutaka Hirakawa, Ayaka Shimoda, Isao Sasano, Kazuo Ohzeki

Shibaura Institute of Technology, Tokyo, Japan

Email: hirakawa@shibaura-it.ac.jp, al13054@shibaura-it.ac.jp, sasano@shibaura-it.ac.jp, ohzeki@shibaura-it.ac.jp

**How to cite this paper:** Hirakawa, Y., Shimoda, A., Sasano, I. and Ohzeki, K. (2018) Improvements in a Puzzle Authentication Method. *Journal of Computer and Communications*, 6, 12-20.

<https://doi.org/10.4236/jcc.2018.61002>

**Received:** September 28, 2017

**Accepted:** December 26, 2017

**Published:** December 29, 2017

---

## Abstract

This article discusses improvements in a puzzle authentication method that adopts the interface of the Puzzle and Dragons game [1] and is tolerant against video-recording attacks. A problem that the conventional puzzle authentication methods face is that they are time consuming and have low success rate in authentication. We evaluated improvements of the interface to verify the usability of the improved system. The results suggested that the usability in terms of operation time and authentication success rate attained a level that was comparable with other leading methods in the field.

## Keywords

Authentication Method, Vibration, Video-Recording Attack

---

## 1. Introduction

Currently, network services such as internet banking, internet finance, and network shopping are commonly used worldwide. The system requires user authentication to deliver these services. Additionally, with the explosive increase of smart phone users, authentication is used for smart phone locking to avoid the leaking of private information.

Many types of authentication methods have been proposed. However, this article focuses on password authentication since it is the basic method and is occasionally used as a remedy when other authentication methods fail. The most popular method is called the personal identification number-entry (PIN-entry) system, which has been adopted worldwide by ATM machines.

The main problem with password authentication is the leaking of passwords. To avoid shoulder surfing, which means peeping over someone's shoulder during their authentication operation to steal a password, is the first research objective. The recent research objective is to achieve tolerance against video-recording

attacks, wherein authentication operations are video-recorded and analyzed. There are two major approaches. The first one uses acoustic information to secretly transmit information from the system to the users. Other approaches comprised using vibration to transmit information to the users.

This study focused on a puzzle authentication method that adopts the puzzle interface used in the Puzzle Dragon Game [1]. This interface is tolerant against video-recording attacks. However, the conventional puzzle authentication methods are time consuming and have low authentication success rate.

This article discusses improvements on the method. Through the proposed improvements, we show that the usability significantly improves and reaches a level that is comparable with that of other leading methods in this field with regard to operation time and authentication success rate.

## 2. Related Work

Numerous password authentication methods exist. In the early stages, shoulder surfing is discussed [2] [3]. The methods in this stage provide safety when someone tries to observe a user's authentication operations. However, they are not safe when authentication operations are video-recorded and analyzed.

In the next stage, tolerance against video-recording attacks is discussed [4] [5] [6] under the assumption that authentication operations are video-recorded twice.

In these years, research objective moves to more difficult one. Tolerance is discussed under the assumption that authentication operations are video-recorded multiple times. There are two major approaches. One is to use acoustic information [7] [8] and the other is using haptic information [9] [10] [11] [12]. Haptic or acoustic information is used to secretly send a message to the user.

This article discusses authentication methods using vibrations. There is an advantage that it can be used by smart phone easily for these methods, but also long consuming time and low success rate are still problems and needed to improve.

## 3. Toward the Improvement

### 3.1. Authentication Method Using Vibration

The puzzle authentication method [9] is described in detail. At first, we mention a famous game called the "Puzzle and Dragon" [1], which was released in 2012. The game interface is shown in **Figure 1**. There are 30 colorful round icons, which are called drops, in the display. The aim of this game is to erase drops by joining three or more identical drops in a line. When a user touches a drop, it can be freely moved for four seconds. If the drop that is touched moves left, the drop to its left moves right. This operation can be performed continuously for a maximum of four seconds. This is a very popular game, and its interface is used in the puzzle authentication method [9].



**Figure 1.** Puzzle and dragon game.

In the puzzle authentication method, a user registers four passwords in advance, and each password is a number less than 17 and larger than 0. Let us assume  $\{3, 7, 11, 16\}$  to be passwords. When these passwords are placed at the correct locations simultaneously by the user, authentication is successful. In this article, the correct locations are called target locations. The interface of the puzzle authentication method is shown in **Figure 2**. If four corners, such as locations 1, 4, 13, and 16, are the assumed target locations, a user moves these drops and all of his passwords to the target locations. The authentication method allows combinatory ambiguity. Therefore, when each password is located at one of the four target locations, the authentication is successful.

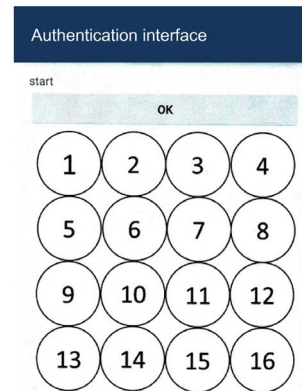
In this study, we assumed that two target locations are registered in advance. For authentication, four target locations are required for passwords with a length of four. The other two target locations are randomly designated by the system for each authentication.

The authentication operation is divided into two stages. In the first stage, the user touches all drops in a single stroke. In this stage, all drops are displayed in the order shown in **Figure 2**, and no drops are moved. The image of a single stroke touch is shown in **Figure 3**. Vibration occurs when a user's finger touches a certain drop. It is a sign of a target location. There are two locations where vibration occurs. These are the target locations that the system selects for authentication.

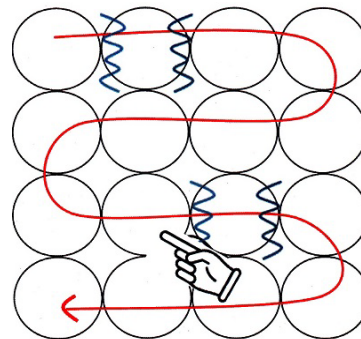
In the beginning of the second stage, drops are displayed in a random order. In this stage, the drop moves freely. The user moves each password to the target place by his single stroke touch. The operation image is shown in **Figure 4**.

### 3.2. Preliminary Experiment

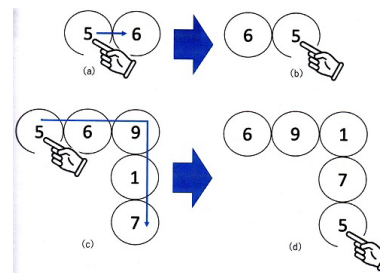
The recognition rate of the two target locations of the puzzle authentication method [9] is experimentally evaluated. Ten students participated in this experiment.



**Figure 2.** Authentication interface.



**Figure 3.** Single stroke and vibration.



**Figure 4.** Finger touch and drop move.

In this experiment, drops are fixed and does not move. Each participant touches all drops in one stroke as shown in **Figure 3**. When a participant touches a drop at the target place, which is selected by the system, vibration occurs. Two places are selected as target places in each operation. After the operation, each participant answers which are the vibrating drops. Each participant repeats this operation fifteen times, where target places are randomly selected in each operation.

The resulting recognition rate was 68%. The success rate of authentication was 63%. A lot of mistakes in recognizing the next location where vibration occurred were found in the experimental results. This means a mistake that user recognizes vibration occurs at the drop labeled number 3 when vibration occurs at the drop labeled number 2 in **Figure 2**.

### 3.3. Scenarios for Improvements

We considered the following to improve the recognition rate:

1) Designation using vibration and visual information:

When a user's finger touches a drop, the drop changes its color. Therefore, a user can recognize the touched drop easily. When a finger touches a drop at the target location not only does the drop change its color but vibration also occurs.

2) Designation using acoustic and visual information:

In this method, a simple tone is used instead of a vibration. When a user's finger touches a drop, the drop changes its color in every location. When a finger touches a drop at the target location, the drop changes its color and a tone is produced. We assumed that users will use headphones to avoid leaking acoustic information.

3) Designation using acoustic, visual, and haptic information:

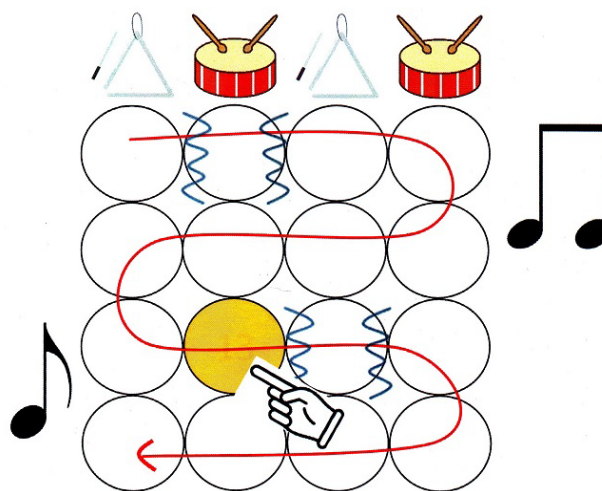
In this method, when a finger touches a drop at the target location, the drop changes its color and a vibration occurs along with a tone. Herein, the same tone is used for each of two different target places.

4) Designation using visual, haptic, and two kinds of acoustic information:

In this method, two types of tones are used. The image is shown in **Figure 5**. We assume that positions 2 and 11 are target locations. When a user touches a drop at location 2, a drum tone is sounded along with vibration. When a user touches a drop at location 11, a triangle tone is emitted with vibration.

5) Finger touch pattern is changed from single stroke:

In the case of a single touch stroke, a user follows must touch drops one after the other in a continuous order. In other words, user's finger moves along the arrow in **Figure 5**. This causes a recognition error; therefore, we adopt a finger touch pattern in a non-continuous order, as shown in **Figure 6**, where the number on the drop indicates the tap order. In this article, this is called alternate tap. This approach is used in target location designation. The alternate tap is adopted and evaluated with each one of the above four improvements.



**Figure 5.** Using two different tones.

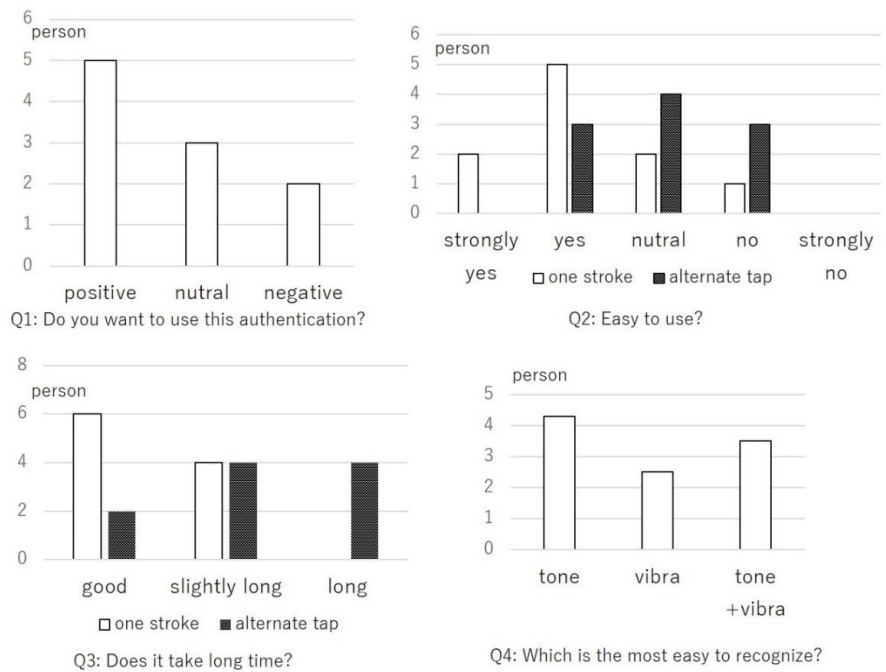


**Table 1.** Results of target place recognition experiments.

	alternate tap		single stroke	
	recognition rate	Time (sec)	recognition rate	Time (sec)
vibra	92%	10.3	68%	6.3
vibra+color	93%	10.9	89%	5.9
color+sound	95%	10.1	83%	6.1
vibra+color +sound	96%	10.2	92%	6.1
vibra+color +2xsound	98%	10.2	96%	6.2

**Table 2.** Authentication results.

	alternate tap		single stroke	
	recognition rate	Time (sec)	recognition rate	Time (sec)
vibra	91%	27.9	63%	22.3
vibra+color	91%	26.9	83%	20.1
color+sound	93%	27.1	81%	19.2
vibra+color +sound	93%	27.3	85%	20.0
vibra+color +2xsound	95%	27.0	93%	19.5



**Figure 7.** Usability evaluation.

## 5. Conclusion

In this article, we discuss the improvement of the puzzle authentication method. The mistakes that occurred in the authentication operation were clarified while investigating the conventional methods, and possible improvements were evaluated. In the improved method, the authentication success rate increased by 30% and the authentication time decreased by 3 seconds in comparison with the conventional method. The improved authentication method was compared to other leading PIN-entry methods. And it is shown that the usability of the improved method reaches the comparative level of these studies.

## 6. Further Work

This study focused on interface improvement. The experimental approach is not the most secure usage of the puzzle authentication method. In the experiment, two target locations were assumed to be registered in advance; however, if four target locations were designated by the system for each authentication without preliminary location registrations, tolerance against a random attack increased. Additionally, in the experiment, each password was allowed to be placed at one of the target locations, where ambiguity is allowed. If this was not allowed, tolerance against random attack increased further. Thus, further usability evaluations according to various security levels are required and will be included in future work.

## References

- [1] GungHo: Puzzle and Dragons.  
<http://www.gunghoonline.com/games/puzzle-dragons/>
- [2] Roth, V., Richter, K. and Freidinger, R. (2004) A PIN-Entry Method Resilient against Shoulder Surfing. *CCS'04*, 236-245.
- [3] Zhao, H. and Li, X. (2007) S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme. *IEEE Advanced Information Networking and Applications Workshops*, 467-472.  
<https://doi.org/10.1109/AINAW.2007.317>
- [4] Sakurai, S. and Munaka, T. (2008) Resistance Evaluation of User Authentication Method Using Matrix against Shoulder Surfing. *IPSJ Transaction*, **49**, 3038-3051.
- [5] Hirakawa, Y. (2013) Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks. *International Journal of Innovation Management and Technology*, **4**, 455-460. <https://doi.org/10.7763/IJIMT.2013.V4.441>
- [6] Hirakawa, Y., Itoh, T. and Ohzeki, K. (2013) A New Numerical Password Authentication Method. *International Journal of Information Technology and Computer Science (IJITCS)*, **12**, 7-15.
- [7] Lee, M.-K., Nam, H. and Kim, D.K. (2016) Secure Bimodal PIN-Entry Method Using Audio Signals. *Computer & Security*, Elsevier, **56**, 140-150.  
<https://doi.org/10.1016/j.cose.2015.06.006>
- [8] Hirakawa, Y., Kogure, Y. and Ohzeki, K. (2015) A Password Authentication Method Tolerant to Video-Recording Attacks Analyzing Multiple Authentication Operations. *International Journal of Computer Science and Electronic Engineering*

(*IJCSEE*), **3**, 356-360.

- [9] Hinokuma, K., Kita, Y., Yamaba, H., Kubota, S., Park, M. and Okazaki, N. (2015) A Study of Puzzle Authentication Method with Video Recording Attack Resistance. *IPSJ Technical Report*, **2015-IOT-31**, 1-6.
- [10] Bianchi, A., Oakley, I., Kostakos, V. and Kwon, D.S. (2011) The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices. *TEI'11*, 197-200. <https://doi.org/10.1145/1935701.1935740>
- [11] Kuribara, T., Shizuki, B. and Tanaka, J. (2014) VibraInput: Two-Step PIN Entry System Based on Vibration and Visual Information. *Proc. CHD2014*, 2473-2478. <https://doi.org/10.1145/2559206.2581187>
- [12] Ishizuka, M. and Takada, T. (2013) Shoulder Surfing Resistant Authentication System by Using Vibration. *IPSJ Computer Security Symposium*, **2013**, 708-715.