Implementation of CAPTCHA suitable for mobile devices

Kentaro Aburada\textsuperscript{(a)}, Shotaro Usuzaki\textsuperscript{1}, Hisaaki Yamaba\textsuperscript{1}, Tetsuro Katayama\textsuperscript{1}, Masayuki Mukunoki\textsuperscript{1}, Mirang Park\textsuperscript{2}, and Naonobu Okazaki\textsuperscript{1}
\textsuperscript{1} University of Miyazaki, Japan
\textsuperscript{2} Kanagawa Institute of Technology, Japan
\textsuperscript{(a)} aburada@cs.miyazaki-u.ac.jp

Abstract: CAPTCHA is a technology designed to prevent automated programs (known as bots) from acquiring access to on-line accounts to send spam mail, manipulate vote numbers in on-line polls, or take other malicious actions. In addition, access to Web services has been incorporated into mobile devices, such as smartphones. However, because most CAPTCHAs are not designed for mobile devices, user-friendly CAPTCHA for mobile devices is required. Thus, we implemented CAPTCHA on mobile devices and evaluated its resistance to bots. Our CAPTCHA showed robustness against bots, with good usability.

Keywords: CAPTCHA, mobile web access, bot detection, automated attack

Classification: Multimedia Systems for Communications

References

[1] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, ”CAPTCHA: Telling humans and computers apart automatically,” Advances in Cryptology, Eurocrypt’03, vol. 2656 of Lect. Notes Comput. Sci., pp. 294-311, 2003.

[2] M. Mohamed, N. Sachdeva, M. Georgescu, S. Gao, N. Saxena, C. Zhang, P. Kumaraguru P. C. van Oorschot and W.-B. Chen, ”A three-way investigation of a game-CAPTCHA: automated attacks, relay attacks and usability,” Proceedings of the 9th ACM symposium on Information, computer and communications security. ACM, pp. 195-206, 2014. DOI:10.1145/2590296.2590298

[3] Google reCAPTCHA, https://www.google.com/recaptcha/intro/android.html, accessed June. 25, 2019.

[4] Ryohei Tatsuda, Kentaro Aburada, Hisaaki Yamaba, Tetsuro Katayama, Masayuki Mukunoki, Mirang Park and Naonobu Okazaki, ”An examination of the interactive video CAPTCHA method to resist relay attack,” IEICE Communications Express, vol. 7, no. 4, pp. 136-141, 2018. DOI:10.1587/comex.2017XBL0192

[5] Nan Jiang, Huseyin Dogan and Feng Tian, ”Designing Mobile Friendly CAPTCHAs: An Exploratory Study,” Proceedings of the 31st International BCS Human Computer Interaction Conference (HCI 2017), 2017. DOI:10.14236/ewic/HCI2017.92

[6] The System Usability Scale (SUS), https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html, accessed June.
1 Introduction

In recent years, there have been problems with abuse of Web services, such as acquiring a large amount of accounts using automatic programs called bots. To prevent such problems, CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) has been developed to distinguish humans from bots[1]. In addition, mobile devices, such as smartphones, have appeared, and they are often used to access Web services. Because most CAPTCHAs are not designed for mobile devices, they cause a decline in conversion rates, such as website registration. Therefore, it is necessary to design a user-friendly CAPTCHA for mobile devices.

In this paper, we implemented a new CAPTCHA for mobile devices and evaluated its resistance to bots. Our CAPTCHA is an interactive CAPTCHA that prepares several objects and moves them at random continuously. Humans are distinguished from bots because human users can track the target object for a definite period of time, even if there are some decoy objects. We verify whether our CAPTCHA has sufficient practicality from the viewpoint of the success rate, usability test and resistant to bots. In particular, we find the optimal number of decoy objects, the optimal threshold and examine the effectiveness of a new idea which sets the degree of change of transparency of each object.

2 CAPTCHA for mobile devices

2.1 Implementation of CAPTCHA based on the previous one

Although various CAPTCHAs have been proposed[2, 3], there is almost no CAPTCHA specialized for mobile devices. In order to realize such CAPTCHA, we extended our previous CAPTCHA to be more suitable for mobile devices[4]. In our previous CAPTCHA, a user tracks one target object among multiple decoy objects. It is hard for bots to find the target object because it has the same characteristics (color, shape, and size) with the decoys, and the decoys appear and disappear randomly. However, a human can find the target object easily by looking continuously.

Under the solving process of the original CAPTCHA, a user tracks the target object by keeping the arrow shaped cursor in the object. In the new CAPTCHA for mobile devices, a user tracks the target object by the finger through the touch panel. Since a previous exploratory study stated that “the CAPTCHA scheme must be designed in a way to only rely on native gesture interactions on mobile devices (e.g., tap and swipe)”[5], we design our mobile CAPTCHA to meet this guideline.
And also, we separated a touch screen into a display area and a touch zone to avoid a problem that a user loses track of a moving object when tracking it with a finger directly. If the user touches the touch zone with a finger, a tracking circle is displayed at the same coordinates in the display area. The “user” is judged to be a human or bot depending on whether the user can track the target object by keeping it in the circle shaped cursor. Fig. 1 (left) shows this CAPTCHA that is called “the first version” in this paper.

2.2 Improvement of CAPTCHA
We improved the first version of our CAPTCHA to counter some attack method; e.g., template matching might identify the target object from successive frames. Since decoy objects in the original CAPTCHA appear and disappear only and don’t move, human users can track the target object from decoy objects. But it is also a hint to find out the target for bots. To prevent this, we adopted a new idea to make decoy objects move randomly in the same way as the target one. And also, we introduced the method that the target object is not designated in advance and a user selects one object as the target one because human users either cannot distinguish the target objects from decoys. Fig. 1 (right) shows this CAPTCHA (the improved version) that uses the procedure described and listed below.

1. CAPTCHA displays multiple moving objects.
2. The user selects any one object and tracks its movement for more than 1 sec; CAPTCHA recognizes this object as the tracking object.
3. CAPTCHA measures the time span for which the user could trace the target object.
4. If tracking success time is longer than the threshold, the user is judged as a human; if not, the user is judged as a bot.
Fig. 2. Success rates for mobile CAPTCHAs.

We also added other features to the improved version; we reduced the number of decoy object to improve usability and introduced the method that changes the transparency of the objects randomly for keeping resistance to bot attacks, such as template matching.

3 Experiment

3.1 Experimental environment
We determined whether a human user could successfully use the mobile CAPTCHA and measured the operation time. In addition, we examined the usability of our methods. We used an iPhone 8 as the mobile device in all cases. The human subjects were 17 students from the University of Miyazaki.

3.2 Results and discussion
The success rate is defined as the percentage of the total of tracking success time that exceeds the threshold of 7 to 9 sec. We executed five challenges each for four CAPTCHA patterns with the first version and the improved version with 5, 10, and 15 moving objects. Fig. 2 shows the results of success rates for each CAPTCHA. The success rate of the first version was higher than that of the improved version, regardless of the threshold. Also, the first version and the improved version with 5 and 10 objects had similar success rates and therefore had sufficient practicality.

3.3 Usability test
We administered a questionnaire using a system usability scale (SUS)[6], which is often used to evaluate usability. The questionnaire consisted of 10 questions; the odd items were positive questions, and the even items were negative questions. An average SUS score of more than 68 was considered to indicate that minimum usability has been achieved. The SUS score for the first version was 84, and the improved version score was 76.5, which means good usability for both versions. A user commented about the improved
version, “it is easy to lose sight of the target object when circles of the same transparency overlap,” so this should be addressed in future work.

3.4 Resistance to bots

We verified that our CAPTCHAs are resistant to automated attacks by bots. The bot tracked the specified object using a mean-shift algorithm, which is an efficient approach for tracking objects whose appearance is defined by histograms[7]. We performed 80 attacks for each method and measured the tracking success time. The breakthrough rate is the percentage of the number of times the tracking success time exceeds the threshold. When this rate is low, CAPTCHA has demonstrated higher resistance to automated attack. Fig. 3 shows the results of breakthrough rate for each CAPTCHA. The breakthrough rate of the first version was 85% and 76% when the threshold was 7 and 8 sec, respectively. However, one of the improved versions had a breakthrough rate of less than 4% when the threshold was 8 sec. From these results, it is considered that the improved version has high resistance to automated attacks. This is because the automated attack could not trace the specified object with less than a certain level of transparency.

Fig. 3. Results of breakthrough rate for the first version (top) and improved version (bottom).
4 Conclusion
In this paper, we proposed a CAPTCHA suitable for mobile devices and discussed its practicality. The experimental results showed that our CAPTCHA has not only a high success rate for humans but also good usability. Also, we found a high resistance to automated attack by bots. In the future, it is necessary to test subjects of various ages in addition to young subjects.

Acknowledgments
This work was supported by JSPS KAKENHI Grant Numbers JP17H01736, JP17K00139, JP18K11268.