Gamified CAPTCHA

Gamified CAPTCHA

Junya Kani* Masakatsu Nishigaki**

*Graduate School of Informatics, Shizuoka University, Japan
gs12012@s.inf.shizuoka.ac.jp
** Graduate School of Science and Technology, Shizuoka University, Japan
nisigaki@inf.shizuoka.ac.jp

Abstract. The Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) has been widely used as a technique that will allow a machine to distinguish between input from a human and that of another machine. The security of current CAPTCHA methods is not sufficient to protect against advanced modern malware. This paper focuses on applying gamification, the use of game elements in non-game human interaction systems, in order to improve the security and usability of CAPTCHA systems. We propose to use movie-based quizzes to achieve a Gamified CAPTCHA system that employs the human capability to recognize the strangeness of a short movie story.

Keywords: CAPTCHA, Entertainment, strangeness, quiz

1 Introduction

With the expansion of Web services, denial of service (DoS) attacks by malicious automated programs (e.g., bots) are becoming a serious problem as masses of Web service accounts are being illicitly obtained, bulk spam e-mails are being sent, and mass spam blog posts are being created. Thus, the Turing test is becoming a necessary technique to discriminate humans from malicious automated programs and the CAPTCHA [1] system developed by Carnegie Mellon University has been widely used. The simplest CAPTCHA presents distorted or noise added text (Fig.1) to users who visit Web sites and want to use their services. We refer to this simple CAPTCHA as text recognition based-CAPTCHA. If they can read the given text, they are certified as human. If they cannot read the text, they are certified to be malicious automated programs (bots).

However, many researchers have recently pointed out that automated programs with optical character reader (OCR) and/or machine learning can answer those conventional text recognition based-CAPTCHA [2]. Indeed, these sophisticated malwares have been spreading and they have cracked the text recognition based-CAPTCHA [3 ,4].

It can be made more difficult for automated programs to pass tests (i.e. read texts) by increasing the distortion or noise. However, it also becomes more difficult

adfa, p. 1, 2011.

for humans to read such texts. We therefore need to adopt even more advanced human cognitive processing capabilities to enhance CAPTCHA to overcome this problem.

Image recognition-based CAPTCHA such as Asirra [6] (Fig.2) is known as one of the effective solutions for enhancing CAPTCHA, because image recognition is a much more difficult problem for a machine than character recognition [5]. Labeled images are used in image recognition based-CAPTCHA to confirm that a user can recognize the meaning of the image. In Asirra, several photos of animals (i.e. images of cats and dogs with diverse backdrops, angles, poses, and lighting) are presented to a user, and the user is then asked to select a specific animal in a test. For example, suppose that the user is asked to select a "cat"; if he or she can select all photos labeled as cat in the test, then he or she is certified to be human. If not, he or she is certified to be an automated program.

However, a technique that has effectively been used to breach image recognition-based CAPTCHA has been reported and shocked researchers [7, 8]. Advancements made to cracking capabilities (CAPTCHA cracking algorithms and CPU processing speeds) will continue indefinitely. No matter how advanced malicious automated programs are, a CAPTCHA that will not pass automated programs is required. Hence, we have to find another human cognitive processing capability to tackle this challenge.

While we desire to enhance CAPTCHA safety, we of course must be conscious of the trade-off between safety and usability. Even supposing we have a CAPTCHA system that has high resistance to malware, but if it is difficult to read for humans, then the CAPTCHA cannot be used. Furthermore, proving that one is human can be an annoyance for users. Therefore, CAPTCHA systems should also be designed to be user-friendly.

To endeavor overcoming this challenge, we had previously focused on the human capability to "understand humor", by proposing the "four-panel cartoon CAPTCHA" [9]. This four-panel cartoon CAPTCHA is presented with the four rearranged randomly panels, and users that are able to sort in the correct order are then identified as human. Even if the panels of a four-panel cartoon are rearranged randomly, a human can understand the meaning of the pictures and utterances in each panel, and thereby sort the order in which the panels must be rearranged in order to create a funny story. For a malware, however, even if image processing and natural language processing abilities developed to the level where the computer could recognize the meaning of the pictures and utterances, it would be still difficult for the computer to arrange the four panels in the correct order unless it also was able to understand humor. Furthermore, because reading cartoons is fun and entertaining for humans, a four-panel cartoon CAPTCHA will most likely be seen as an agreeable and enjoyable Turing Test that does not adversely affect the convenience for users.

We believe that entertainment is one of good driving-forces for enhancement of usability of security technologies, and this motivates us to explore how to improve the entertainment value. This paper is now focusing on the human capability of solving "quiz". When a human challenges a difficult quiz, he or she feels engaged and eager to solve the problem. People may often want to do it again when they fail to

get the correct answer. We try to use such human characteristics to develop even safer and more enjoyable CAPTCHA system. This is essentially the application of gamification, or the use of game elements in non-game scenarios, to engage users when solving CAPTCHA challenges. This is why we entitled it “Gamified CAPTCHA”. It should be noted that the four-panel cartoon CAPTCHA makes use of the fun activity in a “passive” manner; the user reads cartoon and will just be satisfied. On the other hand, the Gamifird CAPTCHA makes use of the fun activity in an “active” manner; the user tries quiz and will want one more try.

This paper will discuss Gamified CAPTCHA with quiz solving. In particular, we play a movie, in which the scenes were altered, for the user. The human will be able to pick out the altered scenes by recognizing the strangeness in the movie. Furthermore, even if the user cannot pick out the altered scenes, the user will want to do it again. By contrast, it will be difficult for malware to solve Gamified CAPTCHA unless the malware can recognize the strangeness of a story with altered scenes. In this paper, we implement Gamified CAPTCHA for swapped scenes, deleted scene, and reversed scene, and we evaluate the effectiveness of this proposal through experimentation. Fig.3 shows a concept image.

Fig.1: CAPTCHA used by Google

Fig.2: Asirra

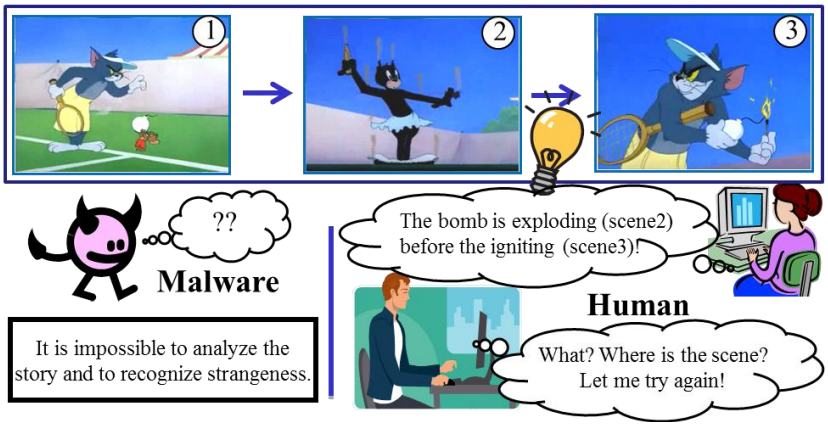

Fig.3: Concept Image (Referenced by “Tennis Chumps”, Tom and Jerry DVD VOL.7, Warnerbros.)

2 Gamified CAPTCHA

2.1 Quiz Use To Leverage Entertainment Value

For enhancement of CAPTCHA, we need to think of both safety and usability. For enhancement of safety, there is a need to use more advanced human cognitive processing capability. For usability of CAPTCHA, there is a need to make CAPTCHA fun. Therefore, the four panel cartoon CAPTCHA with capability to understand humor can be effective. This paper tries to even leverage the "entertainment value" of CAPTCHA by using "quiz", in order to engage the user and make the activity more enjoyable. We in this paper refer to it as "Gamified CAPTCHA".

In particular, we will play a movie, where the scenes in it are altered (i.e., swapped, deleted or reversed), to a user. It is expected that a human can correctly understand the story of the movie and recognize the strangeness of the altered scenes, even when he or she watches the altered version of the movie. For malware, on the other hand, even if technologies such as image processing capabilities are developed, it would continue to be difficult for the malware to correctly pick out the swapped scenes, deleted scene or reversed scene, unless the malware recognizes strangeness of story with altered scene.

The four-panel cartoon CAPTCHA has its merit that users can solve the CAPTCHA while having fun because reading a cartoon is fun and entertaining for humans. Therefore, in this work the Gamified CAPTCHA uses a funny movie for the quiz. As an example, we used the animated movies "Tom and Jerry". The movie was played without sound in order to avoid making a jumping sound which may clue the malware into the skipping scene.

Existing CAPTCHA systems are often a burden for users. Failure to answer the CAPTCHA test correctly is directly linked to a decrease in usability, resulting in frustration of the user. For the Gamified CAPTCHA, on the other hand, even if the user cannot correctly answer, it would be expected that the user would feel encouraged to repeat the test due to the 'fun' nature of the quiz. People often say "Please let me one more try!" when they challenge quiz, and these words are more likely to be uttered when they fail to get the correct answer. Therefore, we would expect that the user would not mind doing the Gamified CAPTCHA again.

2.2 Authentication procedure

Authentication procedure of the Gamified CAPTCHA is as follows. It is here assumed that the Gamified CAPTCHA system has a movie database, in which enough number of short (and funny) movies are archived.

Step1. The system randomly selects one of the movies from the movie database.
Step2. The system divides the movie into scenes.
Step3. The system randomly selects scene(s) in the movie to which the alteration process is applied.
Step4. The system randomly selects the scene swapping, deletion, or reversion.
Step5. The system performs the scene alteration.

(i) If swapping is chosen: The system randomly selects two scenes (Scene A, Scene B), and then swaps these scenes. See fig.4 for an example. The order of the swapped scenes will no longer make sense to the human, which will bring a feeling of strangeness to the viewers.

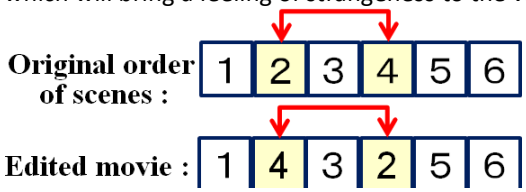

Fig.4: Swapping CAPTCHA

(ii) If deletion is chosen: The system randomly selects one scene, and then deletes the scene. See fig.5 for an example. The movie will skip playing the scene, which will bring a feeling of strangeness to the viewers.

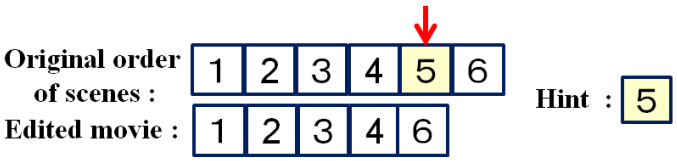

Fig.5: Deletion CAPTCHA

(iii) If reversion is chosen: The system randomly selects one scene, and then reverses the scene. That is, the scene will be played with reverse playback, which will bring a feeling of strangeness to the viewers. See figure 6 for an example.

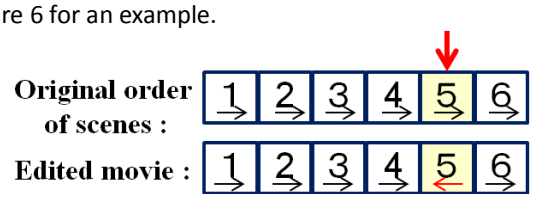

Fig.6: Reversion CAPTCHA

Step6. The system plays the altered movie to the user.

Step7. The user clicks on the screen as soon as the user feels strangeness in watching the movie.

Step8. If the user clicked the altered scene correctly, the system certifies the user as human. To be more precise, (i) for swapping, the user who made a click during either one of the two swapped scenes is certified as human, (ii) for deletion, the user who made a click during the subsequent scene of the deleted scene is certified as human, or (iii) for reversion, the user who made a click during the

reversed scene is certified as human. Otherwise, the user is certified as malware.

Step9. (This is an optional step for the deletion CAPTCHA.) If the user has trouble finding the deleted scene, the system can optionally show the deleted scene to the user. By using the deleted scene as a hint, it would become easier for the user to recognize the location of the deleted scene.

3 Verification experiment

We conducted basic experiments to evaluate the authentication rate and the entertainment value of the proposed method. Due to time constraints, the experiment was not yet performed on the reversion CAPTCHA.

3.1 Experiment method

The subjects included ten volunteers, subjects A-J, who all are college students of Faculty of Informatics and Faculty of Engineering. These subjects received the initial introductory training concerning the proposed CAPTCHA. Then they were shown the movies that are altered by the swapping process or the deletion process. Subjects were instructed to click the mouse when they recognized any strangeness.

As mentioned in Section 3.1, the movies should be fun to watch and easy to understand the story without voice. To meet these conditions, we adopted the “Tom and Jerry” cartoon movies in this experiment. We prepared four “Tom and Jerry” movies, each of approximately 30 seconds in length. Two of them are used for the swapping CAPTCHA and the remaining are used for the deletion CAPTCHA. Here, the length of the scenes that had been swapped was about five seconds (the total time of two scenes), and the length of the scenes that had been deleted was one to two seconds.

The number of times watching the movie is unlimited. That is, we allowed the subjects to replay the movie as many times as desired. However, the number of submitted answers allowable is limited (up to three times). In the case of the deletion, the subjects were optionally allowed to see an image of one frame of the deleted scene as a hint. After seeing a hint, the quiz then becomes easier to solve and the fun of solving it is then decreased. Therefore, the hint image was shown only when the subject asked to see it.

In the case of the swapping, if the subject could click during either of the scenes that were swapped, the answer was correct. In the case of the deletion, if the subjects could click before or after the scene that was deleted (within approximately one second), the answer was correct. The “clicking before the deleted scene” is available to account for the case where the user has watched the movie once and has replayed it. In that case, the user may anticipate the scene and try to click just before the scene.

As a comparison experiment, we also tested a text recognition-based CAPTCHA. Intrinsically, we should create a variety of tests with respect to different

texts/movies. Also, we should randomize the order of tests to take into account the effect of the experimental sequence. However, as this was a basic experiment, all of the subjects took the same tests in the following order: two question of text recognition-based CAPTCHA, two questions of the swapping CAPTCHA, and finally two questions of the deletion CAPTCHA.

After completing all CAPTCHA tests, we had the subjects responded to the following questionnaire.

- Did you enjoy solving the CAPTCHA? (Enjoyed) : Yes (5) – No (1)
- Is it user-friendly? (User-friendly) : Yes (5) – No (1)
- Is it easy solving the CAPTCHA? (Easy) : Yes (5) – No (1)
- Are you happy when you are correct? (Happy) : Yes (5) – No (1)
- Did you want to do it again? (One-more-time) : Yes (5) – No (1)
- Overall points: Good (5) – Bad (1)

3.2 Experiment result

The experimental results are shown in Tables 1-4. Table 1 summarizes the average rate of correct answers for the swapping CAPTCHA and the deletion CAPTCHA. Tables 2-4 show the points from the questionnaire responses regarding the text recognition-based CAPTCHA, the swapping CAPTCHA, and the deletion CAPTCHA, respectively.

Table 1. Authentication rate for Gamified CAPTCHA

CAPTCHA	Percentage
Swapping CAPTCHA(1 question)	90%
Swapping CAPTCHA(2 question)	100%
Deletion CAPTCHA(1 question)	100%
Deletion CAPTCHA(2 question)	100%

Table 2. Text recognition based-CAPTCHA result of questionnaire

Ques. \ Subject	A	B	C	D	E	F	G	H	I	J	Ave.
Enjoyed	1	1	1	1	1	1	2	5	3	3	1.9
User-friendly	1	1	3	4	5	3	3	2	2	3	2.7
Easy	3	2	1	5	5	4	4	2	2	3	3.1
Happy	1	1	3	1	1	1	3	2	3	2	1.8
One-more-time	1	1	1	1	1	1	2	1	2	1	1.2
Overall	1	1	2	5	1	4	3	1	2	2	2.2

Table 3. Swapping CAPTCHA result of questionnaire

Ques. \ Subject	A	B	C	D	E	F	G	H	I	J	Ave.
Enjoyed	5	5	4	4	5	4	3	5	4	4	4.3
User-friendly	2	1	5	1	4	1	3	5	3	2	2.7
Easy	2	5	4	3	4	2	3	3	3	2	3.1
Happy	5	4	4	4	5	4	5	5	4	4	4.4
One-more-time	5	5	4	4	5	2	5	5	4	4	4.3
Overall	3	4	4	2	5	3	4	4	4	3	3.6

Table 4. Deletion CAPTCHA result of questionnaire

Ques. \ Subject	A	B	C	D	E	F	G	H	I	J	Ave.
Enjoyed	4	5	5	5	5	2	4	5	5	4	4.4
User-friendly	2	1	5	1	1	1	4	4	2	4	2.5
Easy	1	3	3	1	1	1	2	4	1	3	2
Happy	5	4	4	3	5	5	5	5	5	4	4.5
One-more-time	5	5	4	4	5	2	5	5	4	5	4.4
Overall	3	5	4	1	5	2	5	5	4	4	3.8

Let us begin with taking a look at Tables 2-4. For the questions of “Enjoyed“, “Happy”, and “One-more-time”, theses averages were four or more points for the Gamified CAPTCHA (Tables 3 and 4), while these were two or fewer points for the text recognition–based CAPTCHA (Table 2). For the question of “User-friendly”, the average is about three points for Gamified CAPTCHA (Tables 3 and 4) as well as the text recognition-based CAPTCHA (Table 2). Therefore, we can confirm that the Gamified CAPTCHA has higher entertainment value compared to the text recognition-based CAPTCHA. However, it must be noted that we have not yet studied how much the entertainment value would be leveraged by using quizzes, instead of four-panel cartoons. We should carry out further investigations to compare the Gamified CAPTCHA with the four-panel cartoon CAPTCHA.

As for the question of “Easy” in Tables 2-4, we found the difficulty for the swapping CAPTCHA and the text recognition-based CAPTCHA to be the same, while the deletion CAPTCHA was more difficult. However, in the experiment for the deletion CAPTCHA, many of the subjects were able to answer correctly without a hint image. Presenting the hint image will reduce the difficulty of the deletion CAPTCHA. From these results, we can see that the Gamified CAPTCHA presents a moderate level of difficulty for a human. This observation is also supported by Table 1. As per the “Average rate for all subjects” in Table 1, it was shown that the authentication rate is sufficiently good for the swapping CAPTCHA (about 90%) and the deletion CAPTCHA (100%). This result would confirm the recognizableness of the Gamified CAPTCHA.

4 Discussion

4.1 Operation

A large volume of movie data would be required to put a Gamified CAPTCHA system into actual operation on the Internet. From the point of view of the movie fees, it is considered to be an effective way to take advantage of movie sites such as “You Tube”. However, the movies posted on such movie sites are a mixture of good and bad. Not all movies necessarily have a story that is easy to understand for everyone. The clarity of the story is considered to be directly linked to the rate of correct answers of the Gamified CAPTCHA. Therefore, the question of how to collect the movies that are easy to understand in large quantities and at low cost is an important issue. In the case of using copyrighted movies, the question would become even more complex. That is because we must obtain not only merely licensing, but also the approval for that the movie can be altered.

4.2 Time-consumeness

In the current stage, the Gamified CAPTCHA uses a movie of about 30 seconds in length. Therefore, the Gamified CAPTCHA test is considered to be very time-consuming, compared to the text recognition-based CAPTCHA. Even though the entertainment value leveraged by quizzes may increase the convenience and actual usability, 30 seconds is still long enough. Therefore the reduction of the time required for answer is another important issue in the Gamified CAPTCHA.

4.3 Security

It is expected to be difficult for malwares to recognize the strangeness in the altered movie and defeat the Gamified CAPTCHA. Therefore, we now focus on brute force attack. In the next stage of this study, we will of course have to cope with not only brute force attack but also a variety kind of attacks.

In the case of the swapping CAPTCHA, if a malware can make a click at the place when the scenes were swapped, the malware is authenticated as a human. Supposed that the movie is about 30 seconds in length and the swapped scenes are about 5 seconds in total, and then this means that even malware could respond with a correct answer at a rate of one out of every six tries. In the case of the deletion CAPTCHA, if a malware can make a click at the place before or after the scenes were deleted, the malware is authenticated as a human. Supposed that the movie is about 30 seconds in length and the tolerance time is 2 seconds, and then this means that even malware could respond with a correct answer at a rate of one out of every fifteen tries. before or after the extracted scene by about one second, In the case of the reversion CAPTCHA, if a malware can make a click at the place when the scenes the scene were played with reverse playback, the malware is authenticated as a human. Supposed that the movie is about 30 seconds in length and the reversed

scenes are about 2.5 seconds in total, and then this means that even malware could respond with a correct answer at a rate of one out of every twelve tries. Ensuring safety against brute force attack is one of the very important issues of the Gamified CAPTCHA.

5 Conclusion and future work

In this study, we focused on "quiz" to enhance the usability and security in the CAPTCHA system, and proposed the Gamified CAPTCHA. The fun nature of the quiz will leverage the entertainment value of the CAPTCHA tests, and therefore, the users will feel encouraged to repeat it. At present, there continues to be room for improvement in terms of both security and usability. We are planning to upgrade the Gamified CAPTCHA based on the knowledge obtained through the experimental results.

Reference

1. The Official CAPTCHA Site, http://www.captcha.net .
2. PWNtcha-Captcha Decoder, http://caca.zoy.org/wiki/PWNtcha .
3. J.Yan, A.S.E.Ahmad, Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms, 2007 Computer Security Applications Conference, pp.279-291,2007.
4. J.Elson, J.Douceur, J.Howela, J.Saul, Asirra: a CAPTCHA that exploit interest-aligned manual image categorization. 2007 ACM CSS, pp.366-374, 2007.
5. K.Chellapilla, K.Larson, P.Simard, M.Czerwinski, Computers beat humans at single character recognition in reading-based Human Interaction Proofs(HIPs), 2nd Conference on Email and Anti-Spam (CEAS), 2005.
6. MSR Asirra Project, http://research.microsoft.com/asirra/ .
7. P.Golle, Machine Learning Attacks Against the ASIRRA CAPTCHA, 2008 ACM CSS, pp.535-542, 2008.
8. S.J.Vaughan-Nichols, How CAPTCHA got trashed, Computerworld, 2008.7.15, http://www.computerworld.com.au/article/253015/how_captcha_got_trashed/
9. T.Yamamoto, T.Suzuki, M.Nishigaki, A Proposal of Four-panel cartoon CAPTCHA, Proceedings of IEEE International Conference on Advanced Information Networking and Applications 2011, pp.159-166, 2011.