

November 2015

Labeled-Image CAPTCHA: concept of a secured and universally useful CAPTCHA

Mokter Hossain

University of Alabama, mokter@gmail.com


Ken Nguyen

Clayton State University, kennguyen@clayton.edu

Muhammad Asadur Rahman

Clayton State University, mrahman@clayton.edu

Follow this and additional works at: <https://knowledgecenter.ubt-uni.net/ijbte>

 Part of the [Computer Sciences Commons](#), and the [Digital Communications and Networking Commons](#)

Recommended Citation

Hossain, Mokter; Nguyen, Ken; and Rahman, Muhammad Asadur (2015) "Labeled-Image CAPTCHA: concept of a secured and universally useful CAPTCHA," *International Journal of Business and Technology*: Vol. 4 : Iss. 1 , Article 2.

DOI: 10.33107/ijbte.2015.4.1.02

Available at: <https://knowledgecenter.ubt-uni.net/ijbte/vol4/iss1/2>

This Article is brought to you for free and open access by the Publication and Journals at UBT Knowledge Center. It has been accepted for inclusion in International Journal of Business and Technology by an authorized editor of UBT Knowledge Center. For more information, please contact knowledge.center@ubt-uni.net.

Labeled-Image CAPTCHA: concept of a secured and universally useful CAPTCHA

Mokter Hossain, Ken Nguyen, Muhammad Asadur Rahman

Abstract. Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) is a widely used online security tool that ensures that a computer program is not posing as a human user. While smart programs with advanced image processing capability have already cracked picture based captcha systems there is a need for making the test harder. This paper presents a design prototype of a simplified type of labeled-image captcha where a picture of a common animal or household item is marked with a number of different labels and the users will be asked to provide the correct label for specific parts of the picture. Due to human's familiarity with body shapes and part names of such common pictures, they will easily identify a specific organ/parts of the picture. Such labeled-image captcha tests are expected to be very easy for human users regardless of their culture, age, gender, educational background and other discriminations but tough for the bots and automated computer programs.

Keywords: Captcha, Turing test, labeled-image captcha, computer security.

M. Hossain¹, K. Nguyen², M. Rahman²

¹ University of Alabama, Tuscaloosa, AL 35487, U.S.A

² Clayton State University, Morrow, GA 30260, U.S.A.

1. Introduction

CAPTCHA stands for *Completely Automated Public Turing Test to Tell Computers and Human Apart*, is a computer program that human can pass but the current computer programs cannot [1]. It is mainly used to protect web-based services against automated computer programs. Fundamentally, CAPTCHA is a cryptographic protocol whose principal mechanism is based on an Artificial Intelligence (AI) problem called Turing test. Through a CAPTCHA test, users of a web service are required to type in some distorted characters to authenticate that they are indeed a human. Such an automated test is designed with a problem that a human user can solve easily but hardly possible for current computer programs [2], [3].

A typical CAPTCHA is a group of words or images containing some distorted characters or other images that appears somewhere, usually at the bottom of Web forms. Unlike the original Turing Test in which a human person is employed as a judge, most modern-day CAPTCHAs are generated and the judged by computers. The paradox of CAPTCHA is that a computer program that can generate and grade tests that it itself cannot pass [2].

Create a New User Account

Please remember the email address and password that you use below to create your profile. Please note that the Password is **CaSe SenSiTiVe**.

***Email Address:**

***Password:**
Password must be at least 8 characters long

***Confirm Password:**

But **ngy500**

Enter the two words in the box separated by a space

Fig. 1. A Typical use of a CAPTCHA in a website.

A typical use of a CAPTCHA test is shown in Figure 1 where some alphanumeric characters are presented in distorted format. Once such a CAPTCHA is used in a Web-based service, a user of such web service is asked to type in the alphanumeric characters in their exact order. If the user is successful in doing so, s/he is considered as a human being and given access to the next steps of the web service.

There are a number of ways to implement CAPTCHAs in websites. However, the following three types of CAPTCHAs are widely found in most websites [4]:

1. Text-based CAPTCHAs: This type of CAPTCHAs are based on a chunk of text images presented in corrupted and distorted way to make them recognizable to human eyes but unusual for pattern recognition programs.

2. Image-based CAPTCHAs: This type of CAPTCHAs are based on some kind of distorted or faded images that require users to perform an image recognition task.
3. Audio-based CAPTCHAs: This type of CAPTCHAs are based on some audio or sound items that require the users to resolve a speech recognition task.

At this age of free access to the social networking sites, bots and spams are becoming increasingly annoying and unexpected threats to the Web-based application services and their users. Bots, shortened form of robots, also called “intelligent agents” are automated or semi-automated program tools that can accomplish some repetitive and routine tasks such as used for data mining or assisting operations [13]. Bots can secretly move to another computer, especially through network or Internet and then exploit that computer to launch some harmful activities or control attacks [14]. If compromised, bots can simultaneously share resources across many criminal or unwanted operators. They sometimes mislead human beings or legitimate users by trapping them to false actions or requests. Thus, the use of CAPTCHAs is considered as an important aspect of modern computer and Internet security systems. A complete list of CAPTCHA applications is maintained at <http://www.captcha.net>. A human user should be able to answer the CAPTCHA in one to two tries.

This study is an initiative to study about how to make better CAPTCHAs that will still serve as robust login security tool; however, will be easy to access and universally useful to all kind of web users. Rest of the paper focuses on some fundamental and required information needed for this purpose.

2. Limitations and Criticisms of CAPTCHAs

Some common criticisms of human identification procedure used in CAPTCHAs is cumbersome and time consuming which causes frustration and loss of productivity. In text-based CAPTCHAs, characters of the words are presented with multiple pictorial effects, and made an image with distorted word so that the optical character recognition (OCR) machines or algorithms cannot detect the characters. Although, this type of CAPTCHAs are most successful in establishing their goals, they have gained dissatisfactory by many users, especially by visually impaired users [8].

Creation of text-based CAPTCHAs with multiple pictorial effects is costly and time consuming. A more popular alternative is in the form of asking some questions such as “What is the sum of ten and 25?”, “What is 15 - five?”, “What is the even digit in one thousand forty three?”, “Chest, brain, chin, hair, and thumb: which is something each person has more than one of?”. The idea using text and number together was to make simple CAPTCHAs that are accessible by users with visually impaired [8]. There is a finite number of patterns used in this format making it is possible to design automatic solver for this type of CAPTCHAs. Audio CAPTCHA is another alternative, however, it also has limitations such as more time for users to solve the CAPTCHA and lower user’s success rate. Recent research shows that 71% of audio CAPTCHA can be solve by computer programs, while human success rate is about 70% [3]. Thus, audio CAPTCHA may not be as secured as once thought. A comprehensive review of

accessibility of different types of CAPTCHAs, especially for visually impaired and elderly users, are seen in [8].

3. Security Issues with CAPTCHAs

3.1 Possible Security Holes in CAPTCHAs

A computer program that breaks the CAPTCHA security check can imitate as human and gain access to services of the system provided by the website. For instance, it can automatically register with an email server with a spam account, vote in online polls, or purchase tickets of a popular event to resale later, etc. Thus, there is a trend among spammers to look for the security holes in CAPTCHAs, break CAPTCHA problems, and use them in performing many illegal activities that they could not do otherwise. A weak CAPTCHA, regardless of its presentation format, is the one that can be recognized by a computer program. Therefore, developing mechanisms to break CAPTCHA security such as solving CAPTCHA challenges [9] helps identify and correct CAPTCHA weaknesses. Current advancement in artificial intelligence enable computer programs to crack up to 90% of the CAPTCHAs used in Google, Yahoo, and PayPal websites [10].

3.2 How CAPTCHAs are Broken

There are several approaches of breaking the identification process used in CAPTCHAs such as: employing cheap human labors to decipher the distorted characters; exploiting program bugs used in implementing CAPTCHA – this may allow attackers to bypass the CAPTCHA; using an existing OCR software to detect the distorted characters; and so on. A common method to break CAPTCHA security that use dictionary words is blind guessing a dictionary attack [5]. This blind guessing technique yield a successful rate over 80% breaking Gimpy and EZ-Gimpy CAPTCHA security.

Another common method of breaking CAPTCHAs is using an image processing method. There are three major steps in this method: pre-processing, segmentation, and character recognition [1]. First, the color of distorted image of a CAPTCHA challenge is converted into a limited color (e.g. gray scale) or binary formatted (black and white) image. Noises are removed and the image is segmented into segments that may represent a character. Finally, in the character recognition phase the segmented characters are deciphered using pattern-matching techniques [1]. Figure 2 shows typical architecture of a CAPTCHA breaker system.

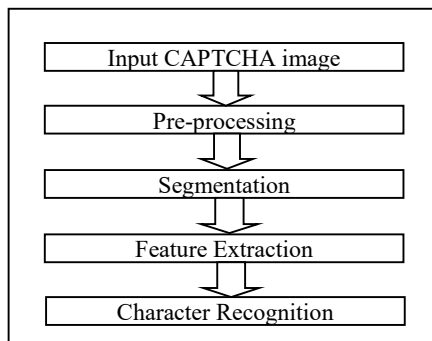


Fig. 2. A typical CAPTCHA breaking architecture

A common practice that spammers and mass-ticket purchasers use is outsourcing CAPTCHA problems solving to low-wage human workers in underdeveloped countries [7]. The results, including both the CAPTCHA problems along with their solutions, are saved in a database for use in dictionary type attacks.

4. Developing a Labeled-Image CAPTCHA

4.1 Needs for Creating New and Stronger CAPTCHAs

Character-embedded CAPTCHA is easy to generate and is prone to be broken. Von Ahn's group proposed the audio CAPTCHA to take advantage of human's ability to understand broken audio by using context clues [3]. The audio CAPTCHA has a dual use: one for security purpose and the other for transcribing old-time radio programs or historical speeches that are difficult for the current automatic speech recognition systems. Other interesting CAPTCHA researches such as grouping the animal types based on given pictures [11] or rearranging randomly presented cartoon figures based on the meaning and/or utterances of different cartoon panels [6].

Since CAPTCHA is a popular web-service security measure to deter unwanted automated access, a more secure, easily recognizable by human and simple to create CAPTCHA is always a challenging problem.

4.2 How to Create a New CAPTCHA?

CAPTCHAs are often programmatically created by combining distorted texts with irregular background patterns to create an image [5]. The generated CAPTCHAs are more vulnerable when the available stock images and background pattern are limited. Thus, most businesses rely on specialized entities such as <http://captchas.net> for CAPTCHA services.

Figure 3 shows a simple Gimpy CAPTCHA – redesigned from the demo program scripts generated from <http://captchas.net> written in Python. In order to integrate the distorted images of the CAPTCHA tests both the user's webserver and the CAPTCHA server (<http://captchas.net>, for instance) need and share a common secret key. When the

website requests for a CAPTCHA, it sends a random string to the CAPTCHA server. The CAPTCHA server then calculates a password and returns the image in an encrypted format and the solution of the image to the user website



Fig 3. A simple Gimpy CAPTCHA coded with Python

4.3 Concept of the Labeled-Image CAPTCHA

In this section, we propose an alternative version of image-based CAPTCHA that we named as Labeled-Image CAPTCHA. In this type of Captcha a picture of an animal or an item will be presented with a unique labels in each major organs of its body or structure and the user will be asked one or more questions to identify a certain or some specific parts of the presented picture. For instance, the whole body of a cat could be labeled as head, left ear, right ear, left front leg, right front leg, left rear leg, right rear leg, body, tail, etc. Each of these parts could be labeled with different number or character in random order, for instance, 1 for the left ear, 3 for the right ear, 4 for the tail, 5 for the left front leg, 7 for the right front leg, 7 for the left rear leg, 6 for the right rear leg of the cat.

Figure 4 shows sample use of a labeled-image CAPTCHA where the user will be asked, for instance: Which number is the closest label to the right front leg of the cat? As it is easy for human users to easily detect such a common organ of a cat and enter the number 7 regardless of their age, race, language and other distinctions they can easily solve such a Captcha problem.



Fig. 4. Possible use of a Labeled-Image CAPTCHA. The figure on the left is the enlarged label-CAPTCHA on the web-form on the left.

Design method of the form using a labeled-image CAPTCHA will be pretty similar to the design of a simple image CAPTCHA, as shown in Figure 4. However, each of the

labeled-images need to be labeled carefully and the corresponding question to the labeled-image be written in a different field with the database. Thus, the web registration form needs to have an image box for displaying the labeled-image, a text label for displaying the associated CAPTCHA question and a text box for inserting the CAPTCHA solution. With 26 characters in the English alphabet, 10 digit in the decimal system, and at least 10 distinct parts on most of common objects and animal. This system would give 10^{36} different case-insensitive CAPTCHA patterns and 10^{62} patterns for case-sensitive CAPTCHAs. An average person would have about 300,000 items at home [13] and is familiar with thousands of animals, structures, and places. Thus, a database containing unique pictures of these subjects would allow us to generate a very large set of unique CAPTCHAs that are trivial to human. Humans are very good at recognizing patterns and we can easily recognize the same of subject from different placement angle. Thus, the size of the picture database can be increased in several folds easily without hindering human capability to recognize them by changing the angle, perspective, and projection of the subject in the picture. The final number of distinct CAPTCHA patterns would be astronomic. Thus, making it much harder for computers to crank through every possible combinations to find a match.

4.4 Possible Implication of the Labeled-Image CAPTCHA

Humans normally have enough knowledge and sense to be familiar with the different organs of a cat or other animals no matter how large or different color of the animal is, but not the machines have. Such kind of knowledge this type of CAPTCHA are intuitive for human but machines. A labeled-image seems to understood and interpreted uniquely by the users regardless of their culture, age, gender, educational background and other discriminations. Due to abundant availability of pictures and images of various animals, household items and many other common pictures it will be easy to develop a large scale database for the labeled-image CAPTCHA. Recently Google announces a new type of reCAPTCHA is able to identify a human user based on its mouse and cursor movement pattern on the websites [12]. With the slogan “No more word puzzles: Google can tell you're human with one click” Google claims that this technology will be more powerful and faster as a user will be asked just to do a single click on a checkbox of the website using thus type of CAPTCHA. However, on mobile devices, the new reCAPTCHA works a slight differently as there is no mouse or cursor movement prior to tapping a button or place on a touch screen or mobile device [12]. So, instead of clicking on a checkbox, users will be asked to select all or a number of images that correspond to a specific clue in the CAPTCHA problem. Although, more details have not been known yet, the proposed labeled-image CAPTCHA could be applicable for implementing Google’s new reCAPTCHA for mobile devices. This seems to be a useful implication for the proposed labeled-image CAPTCHA.

Conclusion

CAPTCHA is a useful tool to deter unwanted machine automation, however, the traditional process of CAPTCHAs generation make it easy for machine to overcome the

intended security measure. In this study, we proposed a new CAPTCHA prototype based on labelled-image, where a picture of a common animal or household item will be marked with different labels. The users will be asked to provide the correct label of specific part of the picture to unlock the service. Since humans are familiar with the objects in the picture and the context of the question, they can easily decipher the problem. Empirical study and additional research on these aspects could be the scope for further study in this area. It is expected that further research on labeled-image CAPTCHA will introduce more secured and useful impact on the digital society.

References

1. A. Chandavale, and A. M. Sapkal. "Algorithm for secured online authentication using CAPTCHA," pp. 292-297, 2010, IEEE
2. L. Von Ahn, M. Blum, and J. Langford. "Telling humans and computers apart automatically," vol. 47, no. 2, pp. 56-60, 2004, ACM.
3. J. Tam, J. Simsa, S. Hyde, and L. V. Ahn. "Breaking audio captchas," pp. 1625-1632, 2008
4. J. Yan, and A. S. El Ahmad. "Usability of CAPTCHAs or usability issues in CAPTCHA design," pp. 44-52, 2008, ACM
5. Pope, and K. Kaur. "Is it human or computer? Defending e-commerce with captchas," vol. 7, no. 2, pp. 43-49, 2005, IEEE
6. T. Yamamoto, T. Suzuki, and M. Nishigaki. "A proposal of four-panel cartoon CAPTCHA: The Concept," pp. 575-578, 2010, IEEE
7. M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage. "Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context." vol. 10, pp. 4.1, 2010
8. S. Shirali-Shahreza, and M. H. Shirali-Shahreza. "Accessibility of CAPTCHA methods," pp. 109-110, 2011, ACM
9. J. Yan, and A. S. El Ahmad. "Breaking visual captchas with naive pattern recognition algorithms," pp. 279-291, 2007, IEEE
10. N. Summers. "Vicarious claims its AI software can crack up to 90% of CAPTCHAs offered by Google, Yahoo and PayPal," vol. 2014, no. October 25, pp. 3, 2013
11. B D. D'Souza, J. Matchuny, and R. Yampolskiy. "Zoo CAPTCHA: Telling Computers and Humans Apart via Animal Image Classification," 2014, Academy of Science and Engineering (ASE), USA, ASE 2014
12. Hill. "No more word puzzles: Google can tell you're human with one click." Available: <https://plus.google.com/+DaveHill47/posts/8uG4LcxYQdi>," vol. 2014, no. 12/05, 2014
13. M. MacVean, "LATimes: For many people, gathering possessions is just the stuff of life." Available: <http://articles.latimes.com/2014/mar/21/health/la-he-keeping-stuff-20140322>.