Security Enhancement in Captcha Recognition using Animated GIF Images

Manoj T. H.
Assistant Professor,
Dayananda Sagar Academy of Technology and Management
Bangalore, India

Basavaraj R.
PG Scholar,
Dayananda Sagar Academy of
Technology and Management
Bangalore, India

Jyoti
PG Scholar,
Dayananda Sagar Academy of
Technology and Management
Bangalore, India

ABSTRACT

CAPTCHAs is Turing test are used to distinguish whether a user is a human or a computer. Till today huge number of CAPTCHA schema have been suggest or put forth and applied on miscellaneous websites to secure online services (SOS) from automated decaptcha programs. So development of a good CAPTCHA scheme that is both secure by automated recognition and human usable is an important research problem. The proposed paper that addresses the above problem by new animated GIF images. This paper present the novel method of designing the CAPTCHA using animated GIF image and in addition to that it analyze time complexity and the security issues.

Keywords

CAPTCHA Recognition, Character Recognition, Security, Animated GIF image, Image Processing

1. INTRODUCTION

In order to enhance the security of the server and verify that the client request which is submitted by the users through online Operations rather than unwanted software, Luis von Ahn and his team coined the term CAPTCHA in 2003. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) are tests that protect websites against bots by generating and grading tests that humans can pass but current computer programs cannot. CAPTCHAs are a very necessary for the Internet and have been effective in deterring automated abuse of online services intended for humans. However, many CAPTCHAs have been found to be insecure against automated attacks [1]. An assortment of various CAPTCHA plans has risen throughout the years, huge numbers of which have been conveyed on various sites. Real organizations, for example, Google, Yahoo!, Microsoft, and informal communities like Facebook, Twitter and other business sites utilizes the utilization of CAPTCHAs to give some level of security against online mishandle.

A few research on CAPTCHA acknowledgment have shown that specific plan blemishes in various CAPTCHAs can be decoded with a high level of progress [2]. This has given rise to the important research problem of how to develop CAPTCHAs that are secure against such automated programs. The task of developing a good CAPTCHA scheme is a very challenging problem. This is because the resulting CAPTCHA must be secure against attacks, and the same time it should be easier to interpret by humans. The tradeoff between CAPTCHA security and usage by humans is a hard to balance. In addition, it has been argued that the difficulty in creating robust CAPTCHAs is further compounded by the fact that the current collective understanding of CAPTCHAs is rather limited [3]. The design of a robust CAPTCHA must in some way capitalize on the difference in ability between humans and current computer programs. This raises the question about whether is it possible to design a CAPTCHA that is easy for humans but difficult for computers [4].

This paper is an endeavor towards a deliberate examination of ease of use issues that ought to be considered and tended to in the plan of strong and usable of CAPTCHA's. While there types of CAPTCHAs; Text based - they normally depend on advanced contortion of content pictures rendering them unrecognizable to the best in class of example acknowledgment programs however conspicuous to human. CAPTCHAs, Audio based CAPTCHAs-they commonly oblige clients to comprehend a discourse acknowledgment errand and Image-based CAPTCHAs they regularly oblige clients to play out a picture acknowledgment undertaking. This paper concentrates on designing new way of Text based CAPTCHAs and its strength against the automated captcha recognition programs. Some of the text based CAPTCHAs are shown in the following figure1.

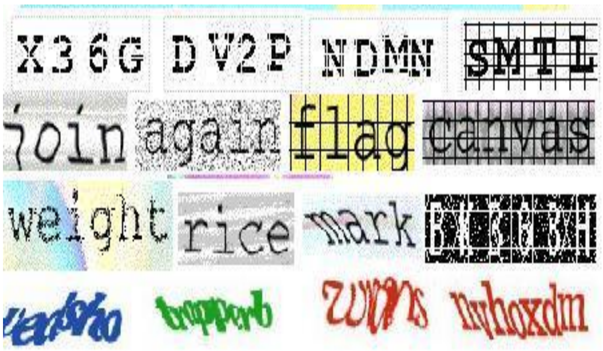

Fig1. Text based CAPTCHAs

2. LITERATURE SURVEY

Mori and Malik have proposed another CAPTCHA which depends on recognizing a picture's upright orientation [5]. This task requires analysis of the often complex contents of an image, a task which humans usually perform well and machines generally do not. Given a huge dataset of images, such as those from a web search result, Use a suite of automated orientation detectors to prune those images that can be automatically set upright easily. The main advantages of CAPTCHA technique over the traditional text recognition techniques are that it is language-independent, does not require text-entry (e.g. for a mobile device), and employs another domain for CAPTCHA generation beyond character obfuscation [6].

Jeff Yan, Ahmad Salah El Ahmad review some of the standard security technology, and has found widespread application in commercial websites. Usability and robustness are two main issues with CAPTCHA, and they often interconnect with each other. They discuss the usability issues that should be considered and addressed in the design of CAPTCHAs[7]. however some others have unpretentious ramifications for vigor or security. A straightforward yet novel structure for inspecting CAPTCHA ease of use is likewise proposed [8 9].

In order for a CAPTCHA scheme to have any practical value, humans must be able to correctly solve it with a high success rate, while the chances for a computer to solve it must be very small. While security considerations push designers to increase the difficulty of CAPTCHAs, usability issues force the designer to make the CAPTCHA only as hard as they need to be and still be effective at deterring abuse [10]. These clashing prerequisites have brought about a progressing weapons contest between CAPTCHA creators and the individuals who attempt to break them.

With advances in research areas like computer vision, pattern recognition and machine learning, and enhancements in Optical Character Recognition (OCR) software, exponentially increase in attacks have been developed to break CAPTCHAs. On the other hand, humans have to rely on their inherent abilities and are unlikely to get better at solving CAPTCHAs. Hence, in order to exploit the gap in ability between human and computers it is vital to examine work by others, which highlight the security flaws and usability issues of various CAPTCHAs. In terms of usability, text-based CAPTCHAs that are based on dictionary words are intuitive and easier for humans to solve. This is because humans find familiar text easier to read as opposed to unfamiliar text. At the same time, CAPTCHAs based on language models are easier to break via dictionary attacks.

Mori and Malik were successful in breaking a number of CAPTCHAs that were based on the English language. Rather than attempting to identify individual characters, they used a holistic approach of recognizing entire words at once. Similar attacks exploiting language models have also been performed on a number of other CAPTCHAs. To take advantage of text familiarity without using actual dictionary words, it is possible to use ‘language like’ strings instead. Phonetic text or Markov dictionary strings are pronounceable strings that are not words of any language. Humans perform better at correctly identifying pronounceable strings in contrast to purely random character strings. Nevertheless, the disadvantage of using this approach is that certain characters (e.g. vowels) will appear at higher frequencies compared to other characters in pronounceable strings [5].

In an attempt to show that machine learning techniques could be used to break CAPTCHAs, Chellapilla and Simard deliberately avoided exploiting language models and were still successful at breaking in a variety of CAPTCHAs [3]. Solving text-based CAPTCHAs consists of a segmentation challenge, the identification of character locations in the right order, followed by recognition challenges, recognizing individual character. Their work demonstrated that computers could outperform humans at the task of character recognition [11]. Hence, this led to the important principle that if a CAPTCHA could be segmented, it was essentially broken. As such, the state-of-the-art in robust text-based CAPTCHA design relies on the difference in ability between humans and computers when it comes to the task of segmentation.

In order to increase the difficulty of segmentation, techniques such as crowding or connecting characters together can be employed. In addition, the use of both local and global warping to distort characters can also make the task of segmentation harder. It should also be noted that CAPTCHAs with fixed length strings, with characters that possibly appear at fixed locations, are easier to segment [12, 13]. While color and/or textures can be used for aesthetic reasons, or for making it easier to distinguish text from background clutter, the inappropriate use of color and textures can have detrimental effects on both the security and usability of a CAPTCHA.

3. PROPOSED SYSTEM

Animated CAPTCHA is designed to overcome security flaws highlighted in other text-based CAPTCHA schemes. The core idea of novel proposed CAPTCHA using animated GIF image is: motion parallax. This capitalizes on the inherent human ability to perceive depth from the apparent difference in motion of objects located at different distances from a moving viewpoint.

The first step in the process of creating animated CAPTCHA technology is the selection of a suitable Image or text material for further processing. The Main advantage of proposed captcha is that, it is easily recognized human and hard to recognized by automated captcha recognition programs . People can recognize a real object despite the fact that it is only a simplified, abstract form of a realistic display of an existing object. By the selection of these types of images a database with plenty of source data for animated CAPTCHA system is created. Next text randomization techniques are employed which automatically change the position and character. Along with this a blank images with other objects {other than Text) are appended to GIF images. These texts are stored in database user giving the running comment the text are coming from the screen in random position.

3.1 Methodology

1) Create an Image text in 2D dimensional and randomize which consist of text & other Objects.
2) Create dynamically n blank images in between Text.
3) Integrate the n unknown blank images with image text and create a GIF image with 10 frames/Second.
4) The image will be displayed only for a fixed amount of time based on number of frames in the GIF image.
5) After a fixed time the image will be automatically refreshed and new image is loaded.

Above methodology is implemented and generated an animated CAPTCHA and their image sequences are shown in the following figure 2.

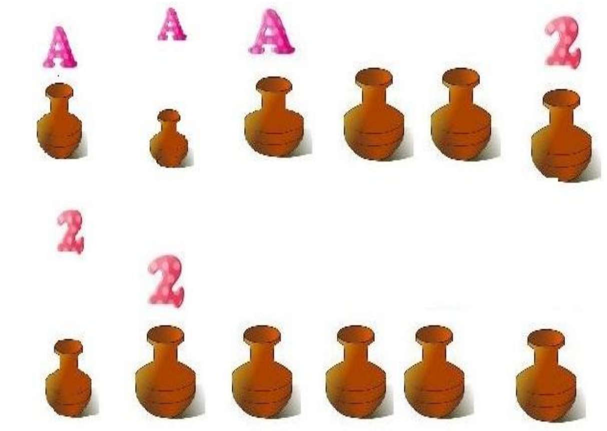

Fig. 2: Image sequences of animated CAPTCHA.

For the above simple background image like above, result and comparisons are in table 1.

Resultant for the above animated gif image using Chellapilla's algorithm is as follows:

AGAGAGGGaGdGaGGGGG

Generally in a classification task, high precision means that an algorithm returned substantially more relevant results than irrelevant, while high recall means that an algorithm returned most of the relevant results.

Precision = TP/ (TP+FP)

Recall = (relevant douments) ∩ (retrived documents)/ (retrived dcuments)

False Positive rate=FP/(FP+TN)

Where TP, FP and TN are True Positive, False Positive and true Negative respectively.

4. EXPERIMENTAL RESULTS

The proposed method is secure by the external automated CAPTCHA programs. It is very difficult to decode the frames in GIF images and recognizing the each frame will result with multiple characters of same text and false recognition of characters because presence of non-textual objects in the gif images. Even any algorithm recognize text correctly, which take more time than the fixed allotted time based on the number of frames used to create the gif images. The proposed methodology is test by various text–based CAPTCHA recognition algorithm and their result is tabulated below.

Table 1: Comparison of text based CAPTCHA algorithms for GIF Images.

Algorithm	Accuracy	No of Frames	Time
Chellapilla's algorithm	10%	40	16s
Projection-only algorithm	13%	40	13s
Projection and middle-axis point separation algorithm	14%	40	14s

From the above table 1, it clearly states that each and every algorithm recognize only below 15%. This shows that proposed methodology of animated CAPTCHA still has very great struggle to all algorithms.

5. CONCLUSION

This paper presents a novel animated CAPTCHA method. It is built on the underlying concept that humans can perceive depth through motion parallax, thus capitalizing on the difference in ability between humans and computers at the task of perceiving depth through motion. Foreground characters and other objects in CAPTCHA are placed at different depths in the 3D scene. If the CAPTCHA is only to protect the safety excessively but lose the practicality, its practical value and research significance will be lost, too. In order to improve its usefulness, a novel captcha using GIF image has developed to improve the security of Captcha in web application.

Decoding the GIF image CAPTCHA which is time consuming and tedious, because the recognition algorithm should separate and check all image, and extracting features and recognizing it. As the time stamp of animated gif images completes, the image will be refreshed and new image will be loaded. So it is very difficult to decode by any other captcha recognition program/alogirthm. This simple and effective animated gif captcha can be used in future rather than simple jpg/png/tiff images.

6. ACKNOWLEDGEMENT

Our sincere thanks to our guide, **Prof. Mr. Manoj .T .H,** Department of MCA, Dayananda Sagar Academy of Technology & Management, who helped to this research article. He has guided us to the maximum to carry out phases of the research work. Last but not the least, thanks to almighty, my beloved Parents for their constant encouragement without which this paper would have not been completed.

7. REFERENCES

[1] A. S. E. Ahmad, J. Yan, and L. Marshall. "The Robustness of a New CAPTCHA". In M. Costa and E. Kirda, editors, EUROSEC, pages 36–41. ACM, 2010.

[2] J. Elson, J. Douceur, J. Howell and J. Saul. Asirra: "A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization". The 14th ACM Conference on Computer and Communications Security (CCS), 2007.

[3] K Chellapilla, K Larson, P Simard and M Czerwinski," Building Segmentation Based Human-friendly Human Interaction Proofs, 2nd International Workshop on Human Interaction Proofs, Springer-Verlag, LNCS 3517,2005.

[4] E. Athanasopoulos and S. Antonatos. " Enhanced captchas: Using animation to tell humans and computers apart". In H. Leitold and E. P. Markatos, editors, Communications and Multimedia Security, volume 4237 of Lecture Notes in Computer Science, pages 97–108. Springer, 2006.

[5] G. Mori and J. Malik. "Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA". In *CVPR (1)*, pages 134–144, 2003.

[6] J. Yan and A. S. E. Ahmad. CAPTCHA Security: A Case Study. IEEE Security & Privacy, 7(4):22–28, 2009.

[7] I. Fischer and T. Herfet. “Visual captchas for document authentication”. In 8th IEEE International Workshop onMultimedia Signal Processing (MMSP 2006), pages 471–474, 2006.

[8] J. Yan and A. S. E. Ahmad. A Low-Cost Attack on a Microsoft CAPTCHA. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security, pages 543–554. ACM, 2008.

[9] J. Yan and A. S. E. Ahmad. Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms. In *ACSAC*, pages 279–291. IEEE Computer Society, 2007.

[10] J.-S. Cui, J.-T. Mei, X. Wang, D. Zhang, and W.-Z Zhang. A captcha implementation based on 3d animation. In Proceedings of the 2009 International Conference on Multimedia Information Networking and Security – Volume *02*, MINES ’09, pages 179–182, Washington, DC, USA, 2009. IEEE Computer Society.

[11] Monica Chew and J. D. Tygar. “Image recognition Captcha. Technical Report” UCB//CSD-04-1333, UC Berkeley, 2004.

[12] Jeff, Y., Ahmad Salah, E.A.: “Captcha security: A case study. IEEE Security & Privacy” 7(4), 22–28 (2009)

[13] A. Goodrum. “Image information retrieval: An overview of current research. Informing Science”, 3(2):63 66, February 2000.