Online Script Recognition Using Captcha Over Internet

[1]Sweta, [2]Shivanand S. Rumma

[1,2] Dept. of P.G. Studies and Research in Computer Science,
[1,2] Gulbarga University, Kalaburagi, India

Abstract : A CAPTCHA which is based on identifying an image's upright orientation is a 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 large repository of images, such as those from a web search result, a suite of automated orientation detectors to prune those images that can be automatically set upright easily. It then applies a social feedback mechanism to verify that the remaining images have a human-recognizable upright orientation. The main advantages of CAPTCHA technique over the traditional text recognition techniques are that it is language-independent, does not require text-entry , and employs another domain for CAPTCHA generation beyond character obfuscation. This CAPTCHA lends itself to rapid implementation and has an almost limitless supply of images. The aim of the topic is to provide the security over the internet for spoofing type of threats using captcha application. Traditional CAPTCHAs require the user to identify a series of letters that may be warped or obscured by distracting backgrounds and other noise in the image. Various amounts of warping and distractions can be used. Recently, many character recognition CAPTCHAs have been deciphered using automated computer vision techniques. These methods have been custom designed to remove noise and to segment the images to make the characters amenable for optical character recognition. The existing system uses the traditional way of submitting the information to the server where validation is not taken place to justify whether the one who is sending the information is human or some kind of virus is involved. This is a serious issue for the web site administrator because one does not want to get the data uploaded from the virus.

IndexTerms **- Audio Captcha, Graphics Captcha, Spam, Turing test.**

I. INTRODUCTION

CAPTCHAs are used to prevent automated software from performing actions which degrade the quality of service of a given system, whether due to abuse or resource expenditure. It can be deployed to protect systems vulnerable to e-mail spam, such as the web mail services. CAPTCHAs are used to stop automated posting to blogs, forums and wikis, whether as a result of commercial promotion, or harassment and vandalism. CAPTCHAs also serve an important function in rate limiting. Automated usage of a service might be desirable until such usage is done to excess and to the detriment of human users. In such cases, administrators can use CAPTCHA to enforce automated usage policies based on given thresholds. The article rating systems used by many news web sites are another example of an online facility vulnerable to manipulation by automated software. The security for an application can be provide using the CAPTCHA as the virus does not have the intelligent power to see the displayed text in captcha and enter it. The image challenge is inaccessible to visually impaired users. This problem is usually addressed by providing an alternative audio CAPTCHA for these users. However, many audio CAPTCHAs can be difficult to hear even to those with good hearing due to background noise and distorted pronunciation. This distortion is necessary in order to prevent the audio being understood by automated agents. Providing both image and audio CAPTCHAs is difficult to implementer can simplify the process.

II. TYPES

A CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart is a type of challenge response test used in computing to determine whether or not the user is human. This turing test requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Since the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes called as a reverse Turing test. CAPTCHAs by definition are fully automated, requiring little human maintenance or intervention to administer, which results benefits in cost and reliability. It is majorly used for security reasons, and also serves as a benchmark task for artificial intelligence technologies. The main purpose of a CAPTCHA is to block form submissions from spam bots automated scripts that harvest email addresses from publicly available web forms and to ensure that the users are indeed human. A most common kind of CAPTCHA used on major websites requires the users to enter the string of characters that appear in a distorted form on the screen. It is used because of the fact that it is difficult for the computers to extract the text from such a distorted image, whereas it is relatively easy for a human to understand the text hidden behind the distortion. So, the correct response to a CAPTCHA challenge is assumed to come from a human and the user is permitted into the website. The free e-mail service might find itself bombarded by account requests from an automated program. That automated program could be part of a larger attempt to send out spam mail to millions of people. So the CAPTCHA test helps identify which users are real human beings and which ones are computer programs. CAPTCHA technology has its foundation in an experiment called the Turing Test. The Turing test is a test of a machine's ability to exhibit intelligent behaviour equivalent to, or indistinguishable from, that of a human. CAPTCHAs are by definition fully automated, requiring little human maintenance or intervention to administer and has benefits in cost and reliability. The text-based CAPTCHAS are designed such that they require the simultaneous use of three separate abilities, invariant recognition, segmentation, and parsing as shown in Fig.1 to correctly complete the task with any consistency.

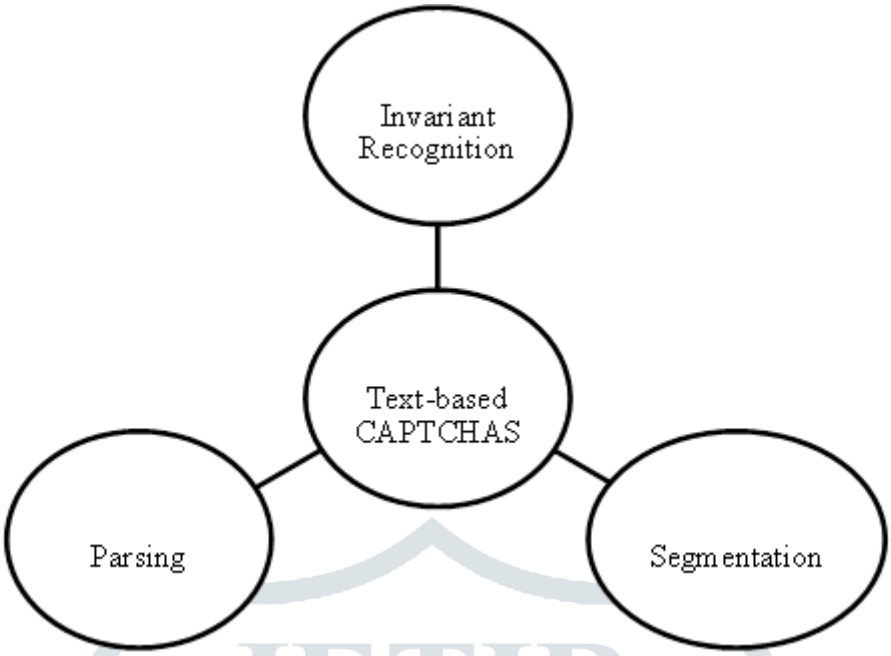

Fig.1 Abilities of Text based Captchas

Invariant recognition refers to the ability to recognize the large amount of variation in the shapes of letters. There are nearly an infinite number of versions for each character that a human brain can successfully identify. The same is not true for a computer, and teaching it to recognize all those differing formations is an extremely challenging task. Segmentation, or the ability to separate one letter from another, is also made difficult in CAPTCHAs, as characters are crowded together with no white space in between. Context is also critical. The CAPTCHA must be understood holistically to correctly identify each character. Unlike computers, humans excel at this type of task. While segmentation and recognition are two separate processes necessary for understanding an image for a computer, they are part of the same process for a person. CAPTCHAs are designed to be unreadable by machines, common assistive technology tools such as screen readers cannot interpret them. Since many sites may use CAPTCHAs as part of the initial registration process, or even every login, this challenge can completely block access. While used mostly for security reasons, CAPTCHAs also serve as a benchmark task for artificial intelligence technologies. The advantages of using hard AI problems as a means for security are twofold. Either the problem goes unsolved and there remains a reliable method for distinguishing humans from computers, or the problem is solved and a difficult AI problem is resolved along with it. In the case of image and text based CAPTCHAs, if an AI were capable of accurately completing the task without exploiting flaws in a particular CAPTCHA design, then it would have solved the problem of developing an AI that is capable of complex object recognition in scenes. As many CAPTCHAs have the option of audio CAPTCHAs for the visually impaired people, an audio file of the CAPTCHA can be downloaded that reads out the CAPTCHA which can be decoded using a speech to text synthesis software with greater accuracy and the obtained result can be used to serve as the input to the CAPTCHA asked.

CAPTCHAs are classified based on what is distorted and presented as a challenge to the user. They are:

Text CAPTCHAs: Text-based captchas are extensively used to distinguish humans from automated computer programs. Most websites and applications still use it as a security and authentication mechanism. Text captchas are keeping evolving and have become more robust, the newly introduced security features make many of the previous scheme-specific attacks no longer applicable. TEXT Captchas: in this Captchas they ask simple questions from us like if today is Sunday then what was yesterday. This are very easy for humans to solve but not for bots. They also display the words by distorting it.

Other text CAPTCHAs involves text distortion and the user is asked to identify the text hidden. The various implementations are:

Gimpy: Gimpy is a very reliable text CAPTCHA built by CMU in collaboration with Yahoo for their Messenger service. Gimpy is based on the human ability to read extremely distorted text and the inability of computer programs to do the same. Gimpy works by choosing ten words randomly from a dictionary, and displaying them in a distorted and overlapped manner. Gimpy then asks the users to enter a subset of the words in the image. The human user is capable of identifying the words correctly, whereas a computer program cannot.

Ez – Gimpy: This is a simplified version of the Gimpy CAPTCHA, adopted by Yahoo in their signup page. Ez – Gimpy randomly picks a single word from a dictionary and applies distortion to the text. The user is then asked to identify the text correctly.

Baffle Text: This is a variation of the Gimpy. This doesn't contain dictionary words, but it picks up random alphabets to create a nonsense but pronounceable text. Distortions are then added to this text and the user is challenged to guess the right word. This technique overcomes the drawback of Gimpy CAPTCHA because, Gimpy uses dictionary words and hence, clever bots could be designed to check the dictionary for the matching word by brute-force.

MSN Captcha: Microsoft uses a different CAPTCHA for services provided under MSN umbrella. These are popularly called MSN Passport CAPTCHAs. They use eight characters and digits. Foreground is dark blue, and background is grey. Warping is used to distort the characters, to produce a ripple effect, which makes computer recognition very difficult.
Graphic CAPTCHAs: Graphic CAPTCHAs are challenges that involve pictures or objects that have some sort of similarity that the users have to guess. They are visual puzzles, similar to Mensa tests. Computer generates the puzzles and grades the answers, but is itself unable to solve it. Graphics Captchas: in this Captchas they display the images like horse, flower and ask from us what they resemble or we need to find such similar objects from many.
Bongo: Bongo. Another example of a CAPTCHA is the program we call BONGO. It asks the user to solve a visual pattern recognition problem. It displays two series of blocks, the left and the right. The blocks in the left series differ from those in the right, and the user must find the characteristic that sets them apart.
Audio CAPTCHAs:
This is based on sound. The program picks a word or a sequence of numbers at random, renders the word or the numbers into a sound clip and distorts the sound clip; it then presents the distorted sound clip to the user and asks users to enter its contents. This CAPTCHA is based on the difference in ability between humans and computers in recognizing spoken language. The idea is that a human is able to efficiently disregard the distortion and interpret the characters being read out while software would struggle with the distortion being applied, and need to be effective at speech to text translation in order to be successful. This is a crude way to filter humans and it is not so popular because the user has to understand the language and the accent in which the sound clip is recorded. Audio Captchas: in this Captchas then they play the word in form of sound. This sound is distorted with other things, now we have to hear the sound and then enter the correct word in the box.

III. CONCLUSION

CAPTCHAS is software that distinguishes human and machine. Research in CAPTCHAS implies advancement in AI making computers understand how human thinks. Different methods of CAPTCHAS are being studied but new ideas like ReCAPTCHA using human time on internet is use full. Internet use has been increased from last 20 years. Therefore we need to provide security over the internet. For that we may use Captchas. There are many types of Captchas are used like: Text captcha, Graphics Captchas, Audio Captchas, Bongo, msn and baffle text. All this kind can be used in the private blogs to prevent from spams. Used by web site that has registrations. They are also used in emails services. They are also used by some search engines.

REFERENCES

[1] “A Survey on Different CAPTCHA Techniques”, Kumary R Soumya, Rose Mary Abraham, Swathi K V , International Journal of Advances in Computer Science and Technology, Volume 3, No.2, February 2014.
[2] Jayavasanthi Mabel.J et.al,”prevention from online attacks: captcha, a defense strategy”,published by International Journal of Computer Science and Management Research,2013, pp.1905-1910.
[3] Suhas Agarwal ,”CAPTCHAs with a purpose”,presented by Srushti Dhope.
[4] Huy D. Truong, Christopher F. Turner, Cliff C. Zou, iCAPTCHA: The Next Generation of CAPTCHA Designed to Defend Against 3rd Party Human Attacks, published by IEEE Communications Society, 2011.
[5] Vimina E R, Alba Urmese Areekal,Telling Computers and Humans Apart Automatically Using Activity Recognition, published by IEEE International Conference on Systems, Man, and Cybernetics,2009,pp. 4906-4909
[6] Richard Chow, Philippe Golle et .al, Making CAPTCHAs Clickable, published by Palo Alto Research Center,2011.
[7] Juraj Rolko et.al,” 3D CAPTCHA:Captcha based on spatial perspective and human imagination”, published by rolko,2010,pp 1-15.
[8] C. Winter-Hjelm, M. H. Kleming, R. H. Bakken, “An interactive 3D CAPTCHA with semantic information”, published at NAIS,2009,pp.157-160.
[9] Jeffrey P. Bigham and Anna C. Cavender, Evaluating Existing Audio CAPTCHAs and an Interface Optimized for Non-Visual Use, published by CHI Boston, Massachusetts,2009.
[10] Mohammad Shirali-Shahreza, Sajad ShiraliShahreza, Question-Based CAPTCHA, published by International Conference on Computational Intelligence and MultimediaApplications,2007,pp.54- 58.
[11] H. Baird and K. Popat, “Human Interactive Proofs and Document Image Analysis”, In Proceedings of the 5th IAPR International Workshop on Document Analysis Systems (DAS'02), Princeton, NJ, USA, 2002, Vol. 2423 of Lecture Notes in Computer Science (LNCS), pp. 531-537, Springer.
[12] S. Shirali-Shahreza, M. Shirali-Shahreza and M. T. Manzuri-Shalmani,”Easy and Secure Login by CAPTCHA,” International Review on Computers and Software (IRECOS)”, Vol. 2, No. 4, July 2007, pp. 393-400.
[13] L. von Ahn, M. Blum, and J. Langford, “Telling Humans and Computers Apart Automatically”, Communications of the ACM, Vol. 47, No. 2, February 2004, pp. 57-60.
[14] T.Y Chan. “Using a Text-to-Speech Synthesizer to Generate a Reverse Turing Test”, In Proceedings of the 15th IEEE International Conference on Tools with Artificial Intelligence, Sacramento, CA, USA,2003, pp. 226-232.
[15] M. Chew and J. D. Tygar, “Collaborative Filtering CAPTCHAs”, In Proceedings of the 2nd International Workshop on Human Interactive Proofs (HIP'05), Bethlehem, PA, USA, 2005, pp. 66-81, Springer.