ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Survey on secured online authentication and defence technique against 3rd party human attacks using CAPTCHA

G. Sai Kirthiga* and **Vaithyasubramanian. S**
Department of Mathematics, Sathyabama University, Chennai
***Corresponding Author: E-mail:saikirthiga_g@yahoo.com**

ABSTRACT

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a test easier for humans but hard for computers to crack. But many programs have been developed to brute force attack any secured website. In this review paper, an algorithm created to achieve an online verification in a secure way has been analysed. As a result, a secured social noteworthiness to get to free web services is set which prompt the expansion in the handiness of very much guaranteed CAPTCHA. Many websites using CAPTCHAs are open to 3rd party human attacks. So as to show this a new human-based CAPTCHA attack using Instant messenger technology is developed. Further an interactive CAPTCHA has been designed as a defence technique against such vulnerabilities. The performance and usability of the proposed scheme has also been studied.

KEYWORDS: CAPTCHA, online verification, secure, defence technique, Instant messenger

1. INTRODUCTION

In 1997 Alta Vista developed a human-user validation by means of randomly generated images with letters or characters. The term CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) was given by Luis von Ahn, Manuel Blum, Nicholas J.Hopper and John Langford in 2000. CAPTCHAs were framed so as to distinguish humans from computers Luis von Ahn et al., (2004). CAPTCHAs play a major role to defend several web-based facilities for instance e-mail accounts.

Programs are created in view of stealing services and to execute fake transactions. Spammers can even create bots that possibly will either increase the rating of a product on a wrong notion or otherwise. CAPTCHAs provide an added layer of security for those websites which avoid e-mail, instant messaging and text message spam. Thus it is found often with account login systems. Though CAPTCHA has been providing security, usability features also play a major role Rezvan Pakdel, 2013. An Intelligence algorithm has also been developed in order to showcase the vulnerabilities that are present in them Thamotharan B et al., (2012). The existing CAPTCHAs can be categorised as (1) Text-Based (2) Image-Based (3) Video and Audio based. Visually challenged users are also benefitted by the audio CAPTCHAs developed later Jennifer Tam et al., (2008). Image-based CAPTCHAs have been developed based on several features to strengthen the CAPTCHA Sajida Kalsoom et al., (2012).

The notion of CAPTCHAs as an automated Turing test that influenced tough Artificial Intelligence problems was formalised by Luis von Ahn. EZ-Gimpy and the Gimpy CAPTCHAs have been broken using refined object recognition algorithms at a success rate of 92% and 33% respectively by Mori and Malik. A success rate from 4.89% to 66.2% has been achieved when Chellapilla and Simmard with the help of machine learning techniques attacked a number of visual CAPTCHAs.

The algorithm created for a secure authentication using CAPTCHA has been discussed in detail. In order to verify the strength, CAPTCHA has been solved. The outcomes have also been mentioned. The CAPTCHA designed in order to defend 3rd party human solver attack using Instant Messenger technology has also been discussed in this paper. A better attack detection performance has also been achieved.

Secured online: Authentication using CAPTCHA: In this paper Chandavaleand, 2010, a secured authentication is provided by checking the strength of CAPTCHA which is done by solving it. There are 3 steps involved in solving a CAPTCHA. They are pre-processing (noise removal), segmentation of raw image and character recognition (using pattern matching technique). The main purpose of noise removal is to discard the unnecessary bit pattern that insignificant to the final output. CAPTCHA image consists of several colours. Since it is difficult to work on each colour it is transformed into grey scale which means it is sufficient to deal with 256 intensity values. In the proposed algorithm, the grey scale value for each RGB value is obtained using

$$\text{Gray Scale Value} = (0.56 * G + 0.33 * R + 0.11 * B \quad (1)$$

Where R, G, B are the red, green, blue colour components of the pixel in the image.

Pixel values can be obtained using grab Pixel () function. The RGB value in the input image is replaced by grey scale value for each pixel and the algorithm stops. By thresholding a grey scale or colour image binary images are produced since it requires the separation of object in the image from the background. Segmentation is done where the letters are detached from the word and each segmented character is rarefied and scaled to an identical size of 60*40 Chandavaleand, 2010. In the character recognition process, two matrices namely, I matrix in which the values 0 and 1 are assigned to white and black pixels respectively and M matrix where the zeroes are replaced by -1 are both calculated. The matching probability for each character is then found using these matrices. Hence the output is based on selecting the character with maximum matching probability. In order to measure how good the recognition

system spots an input configuration as a correct match for one of its many learnt configurations the Recognition Quotient is calculated using Recognition Quotient (Q) = (Candidate score) / (Ideal weight model score) Where Candidate scores

$$\chi(k) = \sum_{i=1}^{x} \sum_{j=1}^{y} W_k(i,j) I(i,j) \quad (2)$$

And Ideal weight model score given by

$$\mu(k) = \mu(k) + W_k(i,j) \quad (3)$$

The similarity of input pattern to the pattern already existing is more for greater values of Q. The application was tested by collecting 180 CAPTCHA samples out of which 88% showed 100% accuracy and also the characters were identified appropriately.

Captcha designed to defend against 3rd party human attacks: A more efficient human-based CAPTCHA attack is developed using Instant Messenger infrastructure. A new defence system called Interactive CAPTCHA (iCAPTCHA) is created to face the serious threat Huy D Truong et al., (2011). It requires a user to resolve the CAPTCHA through a chain of user interactions. As this involves a back and forth traffic between the client and server it increases the time change between a genuine user and a human solver it supports in detecting the attack. A more efficient 3rd party human CAPTCHA attack system is developed to illustrate the human solver attack threat by making use of Instant Messenger network and server infrastructure referred to as Instant Messenger CAPTCHA Attack or IMCA. In order to detect a 3rd party human attack, timeout values are used for solving CAPTCHAs. But the use of Instant Messenger technology by IMCA permits the delivery of CAPTCHA images to 3rd party human solvers at very high speed that CAPTCHA timeout values fail to detect them. This results in developing a reliable defence technique iCAPTCHA. The iCAPTCHA input sequence begins when the user clicks on the CAPTCHA generated. Below the image several buttons appear with obfuscated characters, the corresponding button should be clicked to the first character in the image. After each click, a different set of characters is displayed and the sequence goes on until one click has been performed for each character. The indices of the correct responses and the user clicks are stored as the session information. The CAPTCHA has been decoded correctly if it matches. The time needed to provide a CAPTCHA image to a human solver is relatively small to the timeout value which is not sufficient resolution to identify whether the response is from a genuine user or a human solver. Hence iCAPTCHA measures the time taken for the response from a user based on each character. Thus a higher resolution is provided to govern human attacks since the relative time between each input and the time taken to provide the CAPTCHA to a human solver is minute. Users are allowed to take their own time to decipher the image primarily before arriving into the multi-step task. This results in clearing the interactive steps rapidly.

Table.1.Time Comparison

Total Time taken by a Genuine User	Total Time Taken by an Attacker
$R_u = t_1 + t_2 + U$ Where R_u = the total reply time for a single character in the legitimate user situation t_1 = the network time to download and view the CAPTCHA and complicated characters t_2 = the network time to surrender HTML post to the web server U = the time for user to crack and click on the corresponding character	$R_a = t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + U$ Where R_a = the total reply time for a single character in the 3rd party human attacker user situation t_1 = the network time to download and fix the CAPTCHA and complicated characters t_2 = the network time to upload or ftp CAPTCHA image and complicated characters to attacker's web server t_3 = the delay to download and view the CAPTCHA and complicated characters t_4 = the network time to submit HTML post to the web server t_5 = the polling time for response t_6 = network time to submit HTML post to the web server U = the time for a human user to interpret and click on the corresponding character

From the above Time Comparison Per – character reply time Table 1 it is evident that 4 additional time delays are caused by a 3rd party human solver attack while solving a single CAPTCHA character in the iCAPTCHA application. This supports iCAPTCHA to identify and stop 3rd party human attacks. The iCAPTCHA attack recognition algorithms are hence developed.

2. CONCLUSION

From the proposed algorithm Chandavaleand AA et al., (2010) we can conclude that a more effective and secured CAPTCHA can be created and hence a secured online authentication is available. The detection performance result for the proposed iCAPTCHA Huy D Truong et al., (2011) reveals its effectiveness as defence technique and

in addition about its usability, half of the users prefer to use mouse to respond to CAPTCHA challenges. Thus it is a feasible replacement for the text-based CAPTCHA.

REFERENCES

Chandavaleand AA, Sapkal AM, Algorithm for Secured Online Authentication Using CAPTCHA, IEEE 3rd International Conference on Emerging Trends in Engineering and Technology, 2010, 292-297.

Huy D Truong, Christopher F Turner, Cliff C Zou, iCAPTCHA: The Next Generation of CAPTCHA Designed to Defend Against 3rd Party Human Attacks, IEEE International Conference on Communications, 2011, 1-6.

Jennifer Tam, Sean Hyde, Jiri Simsa, Luis Von Ahn, Breaking Audio CAPTCHAs, Advances in Neural Information Processing Systems (NIPS), 2008, 1-8.

Luis Von Ahn, Manuel Blum and John Langford, Telling Humans and Computers Apart Automatically, Communications of the ACM, 47(2), 2004, 57-60.

Rezvan Pakdel, Seyedkaveh Ranjbar, Mohammed Hashemi, A User-Friendly CAPTCHA Scheme Based on Usability Features, Information Technology Journal, 12(1), 2013, 61-70.

Sajida Kalsoom, Sheikh Ziauddin, Abdul Rehman Abbasi, An Image-Based CAPTCHA Scheme Exploiting Human Appearance Characteristics, KSII Transactions on Internet and Information Systems, 6(2), 2012, 734-750.

Thamotharan B, Vaithiyanathan V, Aparna R, A De-CAPTCHA to Show the Vulnerabilities in CAPTCHA, Journal of Applied Sciences Research, 8(5), 2012, 2506-250.