Enhanced Authentication Scheme using Image Captcha

Ms Yadla Haritha[1], Dr Kalavathi A[2]
Vasireddy Venkatadri Institute of Technology

Abstract— *Authentication is the act of validating the truth of an attribute of a user or a piece of data claimed true by an entity. Authentication is the method of confirming one's identity. It involves confirming the identity of a person by validating the user identity proofs or verifying the authenticity of a website using x.509 digital certificates. Authentication is related to multiple fields. In art, historic and anthropology, a general problem is to verify that the given artifact was produced by a definite person or in a definite place or period of history. In computer science, verifying a person's identity is often required to allow access to confidential data or systems. The basic authentication scheme is using alphanumerical usernames and passwords. To crack these passwords, many times attackers use intelligent programs. To avoid this, Captchas can be used as an add-on security measure to verify whether the interacting person is human or an automated bot. There are several methods proposed by various authors. In this research, authors propose an elegant method to design the captcha which prevents the interaction of intelligent bots in any information system..*

Index Terms— Security, Captcha, Authentication, Digital Certificate, Signature, Identity, Bot detection

1 Introduction

CAPTCHAs are extensively used to thwart any action that is mechanized to execute an action that is employed for a human. They are principally used to thwart intelligent bots who creates fraudulent accounts at the websites. A CAPTCHA is a function that can engender and evaluate whether the interacting person is human or an automated computer program. Humans can easily pass through these evaluation tests, where as an automated computer program cannot pass through it. Such applications can be used to distinguish humans from automated bots and are extensively used in network security.

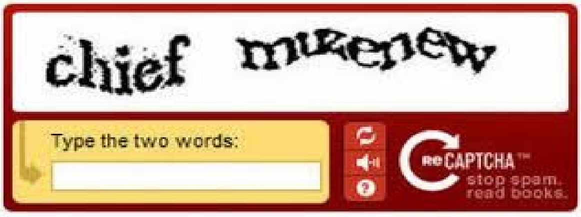


Fig 1. An example of Visual Catcha

Audio CAPTCHAs uses characters written on a complex surface like Visual CAPTCHAs and these characters are read out and is very helpful for a physically challenged person or sometimes visual captcha characters can't be recognized by a normal human being. BotDetect CAPTCHA is a model of audio Captcha is used to assure human verification and is also adaptable to the blind and visually impaired persons. It is developed with the guide lines of Access Board section 508, and uses XHTML 1.1 and WCAG, AAA compliant markup. Normally, BotDetect audio Captcha works with HTML5 <audio> elements for sound playback. It also identifies browsers which don't support Html5 Wav audio fully or partially, and falls back to using <embed> and <object> elements. It protects all kinds of browsers which play audip captcha and endure as accessible like they perform before Html5 audio. BotDetect audio Captcha mechanism uses 12 different audio styles, whereas each style uses a unique mixture of effects and noises. It makes audio Captcha greatly powerful to any automated audio analysis, exclusively when the audio style is picked arbitrarily. A simple Audio CAPTCHA model is shown in the following figure Fig.2

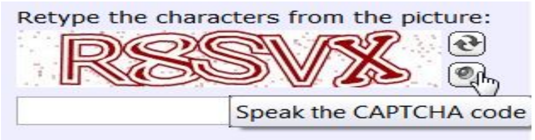


Fig 2. A model audio captcha which pronounces the captcha code

The next category of CAPTCHA is image CAPTCHA.

The naming CAPTCHA displays six images to the user. Each image is labelled with corresponding name. If the user enter the correct name of the image which is already tagged with the image, then the user can pass the verification round.

2 Review of Literature

CAPTCHAs are generated in the unbreakable possible way which avoids any algorithm to disrupt them, but still some significant work was done to break these CAPTCHAs . In 2003, Mori and Malik [3] developed a shape matching algorithm to disrupt EZ-Gimpy and Gimpy CAPTCHAs. They attained a success rate of 92% in EZ-Gimpy and 33% in case of Gimpy. In 2004, Moy et. al. [2] used distortion estimation procedure to break EZGimpy CAPTCHAs and also attained a great success rate. EZ- Gimpy CAPTCHAs have been focused in Chellapilla research. This work shows “segmentation” is a very difficult problem than “recognition” because machine learning algorithms can competently solve the recognition problem, but currently there was no effective algorithm to decipher the segmentation problem causing by these added clutters[5]. The image opening and labelling techniques are used to develop a segmentation algorithm [4]. EZ-Gimpy and Gimpy CAPTCHAs can be categorized into four types namely Simple Background (No Mesh), Black Mesh Background, White Mesh Background and Loosely Connected Characters. This method takes words from a dictionary with 850 words, so one can easily break this algorithm. A correlation algorithm was designed to identify the exact word from EZ-Gimpy CAPTCHA 99% of the time. A direct distortion estimation algorithm identifies the correctly the first four letters from a Gimpy-r CAPTCHA is 78% [5].

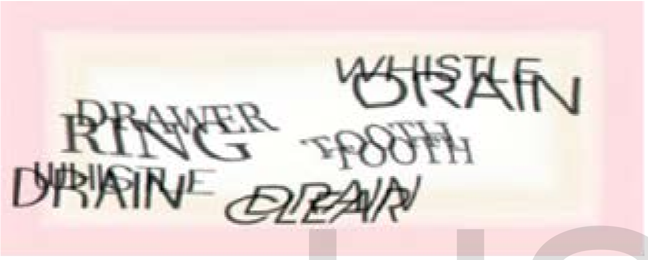


Fig 3: Gimpy Captcha

In Simple (No Mesh) EZ-Gimpy, the characters were written on a simple background whereas in Black characters are written on a black, White Mesh EZGimpy the characters are written on white mesh. Most of the web servers use CAPTCHAs as an add on security measure to distinguish human users from Bots. In a text CAPTCHA, characters are intentionally distorted and connected to thwart recognition by Bots. Text CAPTCHA security can be enhanced by scientifically adding noise, distortion, and arranging characters more strongly [7, 9] is a significant concern in designing Text CAPTCHAs [26]. Examples of text-based CAPTCHAs include the Gimpy method [8], Handwritten CAPTCHA [22], the Baffle text method [16], the PayPal method [22], the Hotmail Method [19], Dynamic Visual Patterns [18], and Pessimal Print method [17]. Successful text CAPTCHAs that were used by Microsoft, Google and Yahoo works with techniques that are resistant to segmentation [12, 13], and [14] attacks by using random acrs, connected random lines and crowding characters.

Game CAPTCHA method works with a database of cartoon mini-games which are very interesting and supportive for end users with some accessibility difficulties as well. These CAPTCHAs are not likely suitable for desktop terminals, but they are more suitable for mobile and touch-screen devices also [20] and is shown in Fig 4..

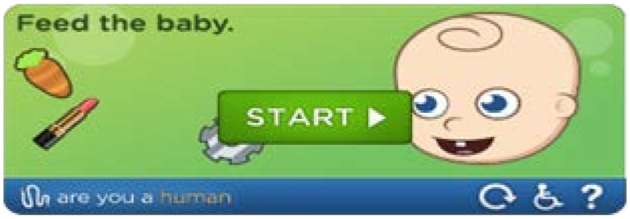
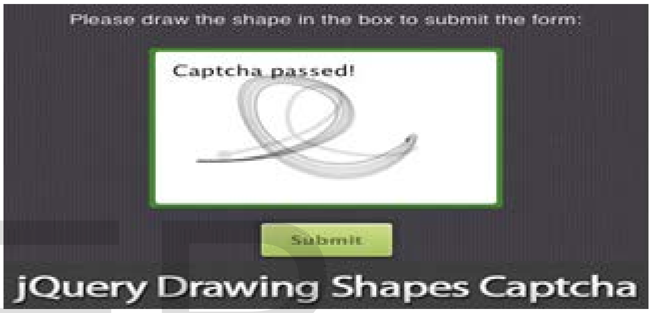


Fig 4. An example of Game Captcha

Image-based CAPTCHAs [21] require the end users to recpgnize labelled images or rotated images. In Image Recognition CAPTCHAs, the end users are provided with a finite set of images to name, distinguish or identify anomalies in them. In implicit CAPTCHAs [15], end users need not have to read or type anything and makes simple clicks on hot spots. Drawing captcha [26] generates various dots on a screen with noisy background. The following figure shows an example of drawing captcha


Please draw the shape in the box to submit the form:

Captcha passed!

Fig 5. Drawing Captcha

OCR works with automatic recognition of different characters in a document image which leads to clear, unambiguous recognition, analysis and understanding of the document content. OCR system segments the captcha text zone into text lines, text lines into words, and then words into characters.

These characters are then recognized by the user. The assignment of recognition can be generally separated into two types: machine printed data and the handwritten data. Preprocessing, Segmentation, Feature Extraction, Recognition and Post processing are major stages in OCR captchas[10, 11]. The success or failure rate of an OCR system depends on segmentation and feature extraction functions.

OCR-based CAPTCHAs are mostly text-based CAPTCHAs where the user is shown distorted images of letters and/or digits. The user is required to recognize them and type the answer in the given text field. But, these CAPTCHAs have an inbuilt drawback.

OCR-based CAPTCHAs are very problematic for mobile phones and devices like PDAs and palmtops, because the use of keyboard may be infeasible or difficult. CAPTCHAs are becoming more and more difficult for genuine users, and at the same time attackers are also improving better in breaking the existing CAPTCHAs [31].

3 Proposed Method

The improved method is designed in such a way to increase the resistance of image CAPTCHA method to hackers attack. The structure is as follows:

a) The method displays a series of 3D images on left and right side of the screen.

b) Images are displayed in a jumbled order with different models of same images.

c) Now the computer program asks the user to choose the 3D image with its corresponding image of the same type. These images need not be identical but contains images of similar type.

d) If the user matches all these images correctly, then the user is allowed to enter the names of these images in the given text box in the displayed sequential order.

e) If the entered name sequence is correct, then one can guess that user is human, and is not a bot.

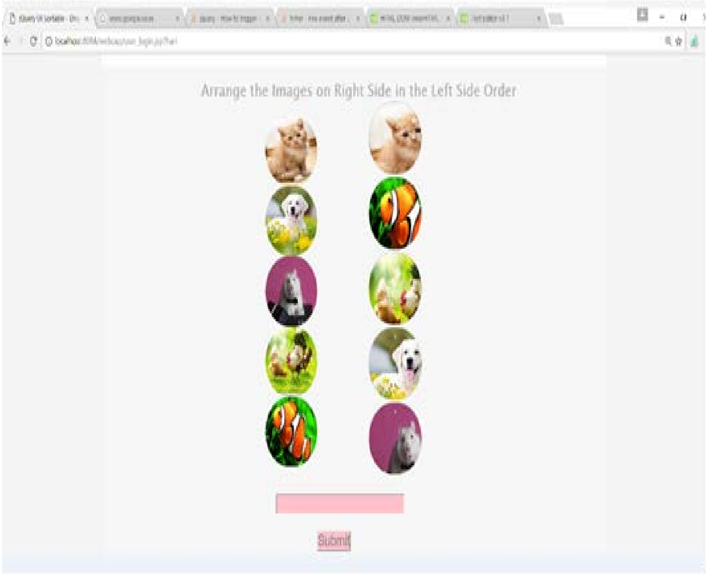
More over the text box remains disabled until the user matches all these images correctly, then only the text box is enabled and user can enter the correct sequence of names of the mapped images in text box. In this method computer requires four abilities to pass the test

i) User has to identify the shape of the given image
ii) User has to match all these images with the corresponding same type of images on the right hand side.
iii) Finally user has to find the names of these images and he has to type in the given text box by using a comma as a separator of these names.

To enter the name of the image in the text box by an intelligent bot, it is difficult for the computer to realize these tasks in correct order, only a human user can recognize and choose the concerned object. This method can be implemented by Java or any other programming language. The implementation is similar to original CAPTCHA method with some differences. The CAPTCHA program select 6 images (objects) randomly that must be different from the previous images.

4 Experimetal Results

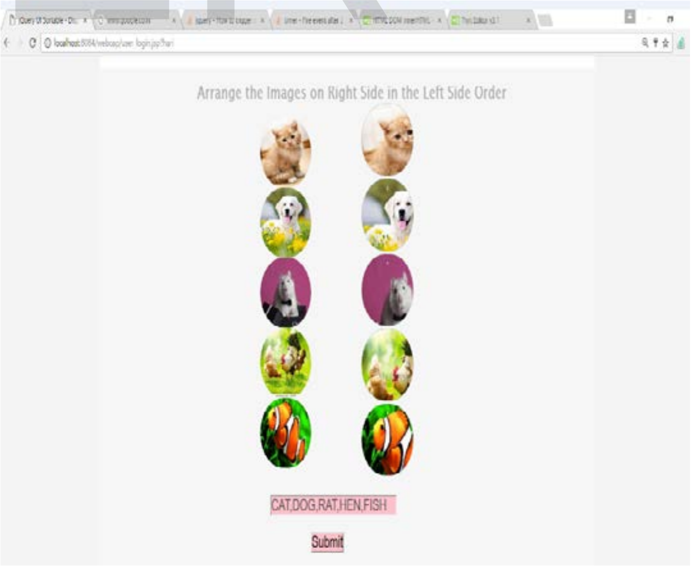
This method displays a series of 3D images on left and right side of the screen. Images are displayed in a jumbled order with different models of same images. Now the computer program asks the user to choose the 3D image with its corresponding image of the same type. These images need not be identical but contains images of similar type.



Arrange the Images on Right Side in the Left Side Order

Fig 6: Captcha Verification

If the user matches all these images correctly, then the user is allowed to enter the names of these images in the given text box in the displayed sequential order. If the entered name sequence is correct, then one can guess that user is human, and is not a bot.



Arrange the Images on Right Side in the Left Side Order

CAT,DOG,RAT,HEN,FISH

Fig 7: Captcha Analysis

5 Conclusion

In distributed networks, verifying a person's identity is often required to allow access to confidential data or systems. The basic authentication scheme is using alphanumerical usernames and passwords. To crack these passwords, many times attackers use intelligent programs. To avoid this, Captchas can be used as an add-on security measure to verify whether the interacting person is human or an automated bot. There are several methods proposed by various authors. In this research, authors propose an elegant method to design the captcha which prevents the interaction of intelligent bots in any information system. The proposed captcha provides more security than the other methods. To enter the name of the image in the text box by an intelligent bot, it is difficult for the computer to realize these tasks in correct order, only a human user can recognize and choose the concerned object. This method can be implemented by Java or any other programming language. The implementation is similar to original CAPTCHA method with some differences.

6 References

[1] B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in Proc. of the 9th CCS, V. Atluri, Ed. ACM Press, Nov. 2002, pp. 161–170.

[2] Gabriel Moy, Nathan Jones, Curt Harkless, and Randall Potter “Distortion Estimation Techniques in Solving Visual CAPTCHAs” proceedings of the Computer Vision and Pattern Recognition (CVPR’04) Conference ,IEEE Computer Society ,vol. 2 ,pp.23-28,2004.

[3] G Mori and J Malik. “Recognising objects in adversarial clutter: breaking a visual CAPTCHA”,IEEE Conference on Computer Vision & Pattern Recognition (CVPR), 2003 , IEEE Computer Society ,vol. 1 ,pp.I-134-I141, June 18-20 ,2003.

[4] L von Ahn, M Blum and J Langford. “Telling Humans and Computer Apart Automatically”, CACM(Communications of ACM), V47, No2, February 2004.

[5] Kumar Chellapilla Patrice Y. Simard “Using Machine Learning to Break Visual Human Interaction Proofs (HIPs) ” in L. K.Saul, Y. Weiss, and L. Bottou, editors, Advances in Neural Information Processing Systems 17, pp. 265–272. MIT Press, Cambridge, MA, 2005.

[6] Ahn, L. von, Blum, M., & Langford, J., (2003) “Telling humans and computers apart automatically”, Communications of the ACM, vol 46, August, pp 57-60.

[7] Ahn, L. von, Blum, M., Hopper, N. J., & Langford, J., (2003), “CAPTCHA: Using hard AI problems for security”, Proceedings of Eurocrypt 2003.

[8] Ahn, L. v., Blum M. & Langford, J., (2000) “The CAPTCHA Project (Completely Automatic Public Turing Test to tell Computers and Humans Apart)”, Project at Department of Computer Science, Carnegie-Mellon University, http://www.captcha.net.

[9] Baird, H. S. & Popat, K., (2002) “Human interactive proofs and document image analysis”, Proceedings of Document Analysis Systems 2002, pp 507–518.

[10] Bansal, V. & Sinha, R.M.K (2002) “Segmentation of Touching and Fused Devanagari Characters”, Pattern Recognition, vol. 35, pp. 875-893, April.

[11] Bansal, V. & Sinha, R.M.K, (2001) “A Devanagari OCR and A Brief Overview of OCR for Indian Script”, Proceedings of Symposium on Transaction support System (STRANS 2001), February 15-17, Kanpur, India.

[12] Baird, H.S. & Riopka, T., (2005) “ScatterType: a Reading CAPTCHA Resistant to Segmentation Attack”, Proceedings of IS&T/SPIE Document Recognition & Retrieval XII Conference, San Jose, California, USA, January 16-20.

[13] Ahmad, A.S.E., Yan, J. & Marshall, L., (2010) “The robustness of a new CAPTCHA”, Proceedings of EUROSEC 2010, Paris, France, ACM 978-1-4503-0059-9/10/0004.

[14] Baird, H.S., Moll, M.A. & Wang, S.Y., (2005) “A highly legible CAPTCHA that resists segmentation attacks”, Proceedings of Second International Workshop on Human Interactive Proofs (HIP 2005), ed. By H.S.Baird and D.P.Lopresti, Springer Verlag, LNCS 3517, Bethlehem, Pennsylvania, USA 2005.

[15] Baird, H.S. & Bentley, J.L., (2005) "Implicit CAPTCHAs", Proceedings of the SPIE/IS&T Conference on Document Recognition and Retrieval XII (DR&R2005), San Jose, pp. 191-196.

[16] Chew, M. & Baird, H. S., (2003) “BaffleText: a Human Interactive Proof.”, Proceedings of 10th SPIE/IS&T Document Recognition and Retrieval Conference (DRR2003), Santa Clara, California, USA, pp 305-316.

[17] Coates, A.L., Baird, H.S. & Fateman, R. (2001) “Pessimal Print: a Reverse Turing Test" Proceedings of IAPR 6th International Conference on Document Analysis and Recognition, pp 1154-1158, Seattle, Washington, USA, September 10-13.

[18] Liao, W.H. & Chang C., (2004) “Embedding information within dynamic visual patterns”, Proceedings of the IEEE International Conference on Multimedia and Expo, 2004. (ICME 04), Taipei, Taiwan, vol. 2, pp 895-898.

[19]Microsoft Hotmail, Website http://www.hotmail.com.

[20] http://areyouahuman.com/

[21] Merler, M. & Jacob, J., (2009) “Breaking an Image based CAPTCHA”, Technical Paper submitted to the Department of Computer Science, Columbia University, USA, Spring term, Available at w.cs.columbia.edu/~mmerler/project/FinalReport.pdf.

[22] Rusu, A. & Govindaraju, V., (2004) “Handwritten CAPTCHA: using the difference in the abilities of humans and machines in

reading handwritten words", Proceedings of the Ninth International Workshop on Frontiers in Handwriting Recognition (IWFHR-9), Tokyo, Japan, pp 226-231.

[23] PayPal (2006), PayPal registration. Website https://www.paypal.com.

[24] Shirali-Shahreza1, S. & Shirali-Shahrezal, M., (2010) "A Survey Of Human Interactive Proof Systems", International Journal of Innovative Computing, Information and Control, vol 6, num 3(A), March.

[25] Shirali-Shahreza, M. & Shirali-Shahreza, S., (2006) "Drawing CAPTCHA", Proceedings of the 28th International Conference Information Technology Interfaces (ITI 2006), Cavtat, Dubrovnik, Croatia, June 19-22, 2006, pp 475-480.

[26] Yan, J. & El Ahmad, A. S., (2008) "Usability of CAPTCHAs or usability issue in CAPTCHA design", Proceedings of 4th Symposium on Usable Privacy and Security (2008), pp 44-52.

[27]. Alan Turing. Computing machinery and intelligence. In Mind, pages 433–60, 1950.

[28]. L. von Ahn, M. Blum, N. Hopper, and J. Langford. Captcha: Using hard AI problems for security. In Eurocrypt, 2003.

[29]. Manuel Blum, Luis A. von Ahn, John Langford, and Nick Hopper. The CAPTCHA Project. http://www.captcha.net, November 2000.

[30]. Monica Chew and Henry Baird. Baffletext: A human interactive proof. In Document Recognition and Retrieval X, 2003.

[31] H.S. Baird and K. Popat, "Human Interactive Proofs and Document Image Analysis," in Proc. of the 5th IAPR International Workshop on Document Analysis Systems, Springer LNCS 2423, pp. 507-518, 2002.

[32] Kumar Chellapilla, Kevin Larson, Patrice Y. Simard, and Mary Czerwinski, "Building Segmentation Based Human-Friendly Human Interaction Proofs (HIPs)," in Proc. of HIP 2005, pp. 1-26, 2005.

[33] L. von Ahn, M. Blum and J. Langford, "Telling Humans and Computer Apart Automatically," in Communications of the ACM, vol.47, no. 2, pp. 57-60, 2004.

[34]. Greg Mori and Jitendra Malik. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. In Computer Vision and Pattern Recognition, 2003.