Review Paper on Different CAPTCHA Techniques

[1]Anvesh Sinha, [2]Dr. Sandhya Tarar
[1,2]Gautam Buddha University, Greater Noida, UP, India

Abstract
CAPTCHA is a program or a system that protects against automated scripts (or bots). It generates tests that humans can pass but computer programs cannot. CAPTCHA systems are widely used nowadays for protecting and providing security to internet based services for humans from abuse by bots. Different types of CAPTCHA technologies are discussed in this paper and a detailed analysis on their reliability is performed. Subsequently, a new CAPTCHA technique is proposed which is based on facial expression detection.

Keywords
CAPTCHA, security, bots, facial expression detection

I. Introduction

The term CAPTCHA stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart" [1]. It was invented in 2000 by Luis Von Ahn, Manuel Blum, John Langord and Nicholas Hopper of Carnegie Mellon University. It is a Human Interaction Proofs (HIP) system which aims to differentiate a human and a computer program automatically. It can also be comprehended as a reverse Turing test in which the CAPTCHA plays the role of the judge and the user (that is, a human or machine) acts like a participant. If the given problem is solved by the user successfully, then the user is recognized as a human or else it is labelled as a machine. Most of the internet based applications have implemented CAPTCHA as a defensive system for practical security against bots. These artificially intelligent computer programs acts like human hoaxer to break the CAPTCHA and perform malicious activities. Comment spamming in blogs, misusing free e-mail services, worms and spams in e-mail, and dictionary attacks in password systems are some of the fraudulent activities which are prevented by the use of CAPTCHA system. Every CAPTCHA system has to concur too few basic pre-requirements. On one hand, it should be fast and simple for human users to unlock it but on the other hand it should be difficult to break for a software program. This means the systems front end complexity should be kept as low as possible without compromising its security aspects.

There are a number of CAPTCHA technologies which are being used in present day scenario like text-based, image-based, audio-based and video-based CAPTCHAs. In text-based CAPTCHAs, as shown in fig. 1, the system displays a sequence of characters after randomly arranging them and with some added noise to the user. The user is said to have passed the test if the input characters matches with the actual characters asked by the system. It is the most widely used CAPTCHA. Some alterations are made to the text-based CAPTCHA to get other types like the Gimpy, Ez-Gimpy and Baffle-Text CAPTCHA. Both Gimpy and Ez-Gimpy method uses word from a dictionary to which some distortions are infused. In Baffle-Text method, words that do not belong to an English dictionary are used. In image-based CAPTCHAs, as shown in fig. 2, the computer randomly generate images in which the user has to select the images havingsome similarities. A type of question-basedCAPTCHA also exists as shown in fig. 3. The audio-based CAPTCHA was initially created for visually disabled users. In this the user is required to listen and then enter the spoken word. Nowadays, mostly all of the CAPTCHA systems come along with the option of audio-based CAPTCHA.

Fig. 1: reCAPTCHA Example [2]

Fig. 2: Image-based CAPTCHA [3]

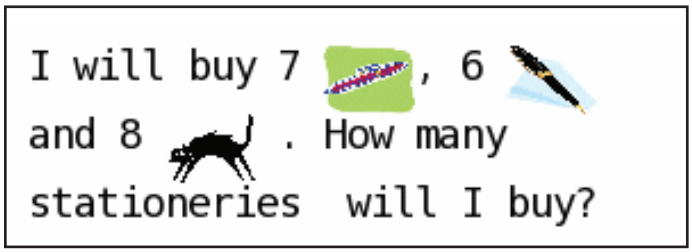

Fig. 3: Question based CAPTCHA

II. Review of CAPTCHA Techniques

In this section,work carried on the CAPTCHA techniques, which are being used presently, are discussed.

Jeff Yan, et al., in their paper [4] have presented a character segmentation techniqueto attack a number of text CAPTCHAs, including those designed and deployed by Yahoo, Microsoft and Google. Specifically they have targeted the Microsoft CAPTCHA which had been deployed since 2002 at a number of their own internet services including Windows Live, MSN and Hotmail. The existing CAPTCHA system was thought to be segmentation-resistant. However, their simple attack which involved 7 consecutive steps, namely – binarization, fixing broken characters, vertical segmentation, color filling segmentation, thick arc removal, locating connected characters and segment connected characters achieved a segmentation success rate of 92% against the scheme, that is out of 100 challenges 92 where segmented correctly. They implemented the attack in Java on an ordinary desktop computer (with a 1.86 GHz Intel Core 2 CPU and 2 GB RAM). The average speed to completely segment a challenge was recorded to be slightly more than 80 milliseconds. They estimated that the given Microsoft CAPTCHA could be broken instantly by a malevolent bot with an estimated (segmentation and then recognition) success rate of 60% or more. However, the goal at the time of designingfor the Microsoft CAPTCHA was that automated attacks should not achieve a success rate of more than 1 in 10000 attempts (that is, 0.001%). For the first time, the vulnerability of a segmentation resistant text-based CAPTCHA was exposed to different and simple attacks.

Gabriel Moy, et al., in their work [5] discussed two distortion estimation techniques that solved EZ-Gimpy and 4-letter Gimpy-r CAPTCHAs through object recognition with a high degree of success. They performed different attacks on the given visual CAPTCHAs. For EZ-Gimpy they developed a correlation algorithm which uses "core" and "minipatch" framework and their variations to determine distortions and subsequently find which distorted template image best correlated to the challenge image. Doing so they achieved a success rate of 99%. In the case of Gimpy-r a success rate of 78% was achieved by deploying a direct distortion estimation algorithm that was able to correctly identify the four lettered Gimpy-r CAPTCHA.

Another related work was carried out by Mori and Malik in their paper [6] wherein by using sophisticated object recognition algorithms they were able to break the EZ-Gimpy and Gimpy CAPTCHAs with a success rate of 92% and 33% respectively.
Jennifer Tam, et al., in their work [7] have tested the security of audio based CAPTCHAs. They have considered three specific audio CAPTCHAs, namely – Google, Digg and reCAPTCHA and have successfully "broken" them with a success rate of 71%. They have used algorithms like AdaBoost, SVM and k-NN to implement automated digit and letter recognition. The audio segment of a CAPTCHA was extracted iteratively. This segment was then inputted to one of the letter and digit recognizers for which a corresponding label was generated as an output. This process was continued till there are no unlabeled segments left. Finally the prediction for the solution to the CAPTCHA was then compared to the real solution.

El Ahmad, et al., in their work [8] have done a thorough study of visual CAPTCHAs which are available at captchaservice.org. It is a website that provides services for CAPTCHA generation publically which had sophisticated distortions and were meant to be resistant to OCR attacks. Instead of using complex machine learning algorithms or computer vision techniques, they implemented simple pattern recognition algorithms along with serious design faults found in every scheme to break the CAPTCHAs with close to 100% success rate. Their proposed algorithms are Vertical Segmentation (VS) and Snake Segmentation (SS). The results of their attacks are shown in Table 1. They further extended their research to other CAPTCHA schemes present at that time and found that they too were susceptible to their novel attack because of the similar design errors. They have implemented their attacks in Java using Pentium 2.8 GHz CPU and with 512 MB RAM. The average time for 100 sample tests were studied and then compared with the worst time (or slowest time). It took 20 to 50 milliseconds to break a challenge in the understudy CAPTCHA schemes.

Carlos Javier Hernandez-Castro , et al., in their work [9] have performed a case study for an already deployed CAPTCHA,which aims to protect free internet service,by attacking it using black box technique. The CAPTCHA, referred to as "Math CAPTCHA" or "QRBGS CAPTCHA", is tested for five types of problem (differentiation, polynomial questions and arithmetic calculations). The system asks the user for providing a solutionto a mathematical problem in order to prove that a human is behind the system. They have studied a number of problems both for its design and its execution, and how those mistakes can be used to solve the CAPTCHA completely using a low-cost attack. The attack does not require an artificial intelligence system or automatic character recognition, which is usually the intended path. It is instead a side-channel attack, which is based on the flaws of previously mentioned CAPTCHAs. They have related the flaws to common flaws found in other CAPTCHA proposals and concluded with certaintechniques for enhancing the given CAPTCHA that could be taken as general guidelines.

Ved Prakash Singh, et al., in their work [10] have described all type of CAPTCHA and have also mentioned their drawbacks of different types of CAPTCHA. The applications of the specified CAPTCHA are also studied in detail. According to their paper, CAPTCHA is basically used as a protection from the malicious programs like bot. For the purpose of web security people are using different types of CAPTCHA. Text based, Image based, Audio based, Video based and Puzzle based CAPTCHA are the specific techniques whose applications and drawbacks are reviewed. They have proposed, that in near future, main focus will be to develop a CAPTCHA that would provide the ease of access to the user and highest level of security by preventing the Bot attacks.

III. Analysis

The analysis of the studied work is done in this section and is tabulated in Table 1 and Table 2. In Table 1, the % success rate represents that out of 100 attacks done on a CAPTCHA the value associated with it is the number of times the CAPTCHA is "broken" successfully. For example, in the case of Text-based CAPTCHA we get a success of 92 times out of 100 while trying to attack it and pass through it using a computer program. In Table 2, the problems faced by userswhile using different CAPTCHA techniques arediscussed [11].

Table 1: Success Rate of Attacks on CAPTCHAs

S. No.	Type of CAPTCHA	Success rate of attacks (in %)
1.	Text based (Microsoft CAPTCHA)	92
2.	EZ - Gimpy	99
3.	Four lettered Gimpy-r	78
4.	Audio-based CAPTCHA	71

Table 2: Problems faced by users using CAPTCHAs

S. No.	Type of CAPTCHA	Problems
1.	Text-based CAPTCHA	Due to different font size, color, orientation and blurring of the texts user faces difficulties to identify them correctly. Also with the new advancements in OCR techniques they can be easily guessed by bots.
2.	Image-based CAPTCHA	Users having low vision or color blindness can face issues to identify them properly.
3.	Audio-based CAPTCHA	The availability of these are only in English, hence the user is required to have an understanding of the language. Also characters having similar sound can raise some problems.
4.	Math-based CAPTCHA	Requires problem solving skills and more time to solve to pass through the CAPTCHA.

IV. Conclusion

CAPTCHA is a widely popular system which is used to protect websites against malicious computer programs. A number of CAPTCHA technologies exist in literature. In this paper, a clear overview on the performance and implementation of the existing techniques is presented. Their reliability is thoroughly checked. Different type of attacks which are used to break the CAPTCHA systems and their success rate are also discussed in the review section. We believe that due to the high success of attacks, the need for a more robust CAPTCHA system is there. Hence we propose a new CAPTCHA which will use the implementation of facial expression detection. This system requires a more real-time human interaction which will help to fulfill the purpose of differentiating a human and a computer program. The proposed system will ask the user to provide the required facial expression. If it matches with the data, associated with that expression, CAPTCHA will be unlocked. The system exploits the fact that the input for the CAPTCHA system will be a human face with a particular facial expression.

References

[1] L. Ahn, M. Blum, J. Langford,"Telling Humans and Computers ApatAutomatically", Communications of the ACM, 47(2), pp. 57–60, 2004.

[2] 'Fig. 1' from www.captcha.net

[3] 'Fig. 2' and 'Fig. 3' from Google images

[4] Jeff Yan, Ahmad Salah El Ahmad,"A low-cost attack on a Microsoft captcha", Proceeding of the 15th ACM Conference on Computer and communications security, CCS '08, pp. 543-554, October, 2008

[5] Moy G., Jones N., Harkless C., Potter R.,"Distortion estimation techniques in solving visual CAPTCHAs", IEEE CVPR, pp. II-23-II-28, Vol. 2l, 2004

[6] Greg Mori, Jitendra Malik,"Recognizing objects in adversarial clutter: Breaking a visual captcha", IEEE Computer Vision and pattern recognition, pp. 134-141, 2003

[7] J. Tam, J. Simsa, S. Hyde, L. VohnAhn,"Breaking Audio CAPTCHAs", Advances in Neural Information Processing Systems, 2008.

[8] Ahmad Salah El Ahmad, Jeff Yan,"Breaking Visual CAPTCHAs with Naïve Patter Recognition Algorithms", IEEE Computer Security Applications Conference, pp. 279-291, Dec 2007.

[9] C.J. Hernandez-Castro, A. Ribagorda,"Pitfalls in CAPTCHA design and implementation: The MATH CAPTCHA, a case study", Computers & Security, 29(1), pp. 141-157, 2010.

[10] Ved Prakash Singh, Preet Pal,"Survey of Different Types of CAPTCHA", International Journal of Computer Science and Information Technologies, Vol. 5, pp. 2242-2245, 2014.

[11] ElieBursztein, Steven Bethard, John C. Mitchell, Dan Jurafsky, Celine Fabry,"How good are humans solving captchas? A large scale evaluation", In Security and Privacy, 2010.

Anvesh Sinha is presently a final year student (2016 batch) of Integrated Dual Degree B.Tech and M.Tech from Gautam Buddha University, Greater Noida in Computer Engineering, with a specialization in Software Engineering.

Dr. Sandhya Tarar received her B.Tech in Computer Science and Engineering from U.P.T. University, in 2005, M.Tech in Computer Science from Aligarh Muslim University and Ph.D. in Biometrics from Gautam Buddha University, in 2014. Her research interest is in Pattern Recognition. She has a teaching experience of more than 10 years and have a number of research paper publications in both national and international journals. Presently, she is a Research Associate in Gautam Buddha University, Greater Noida.