IJSRTM
https://www.ijsrtm.com
Vol.2 Issue 4 December 2022: 11-15
Published online 11 Dec 2022
E-ISSN: 2583-7141

International Journal of Scientific Research in Technology & Management

A Review on various CAPTCHA in the field of Web Security

Rupesh Sahu
Dept. of Computer Science & Engineering
SAM College of Engineering & Technology, Bhopal, Madhya Pradesh, India
rupeshsahu1992@gmail.com

Neelesh Jain
Dept. of Computer Science & Engineering
SAM College of Engineering & Technology, Bhopal, Madhya Pradesh, India
neeleshcmc@gmail.com

Devendra Rewarikar
Dept. of Computer Science & Engineering
SAM College of Engineering & Technology, Bhopal, Madhya Pradesh, India
dev_rewadikar@rediffmail.com

***Abstract*— As a security test, CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) allows for the measurement of human and automated intervention. It is a form of test whereby the behaviour of the subject or the resolution of the issue allows for the detection of planned intervention. You may choose from a number of CAPTCHA challenges, including distorted strings, photo identification, audio, math, and gaming CAPTCHA. Comparatively speaking to other CAPTCHAs, game-based problems are engaging and extremely safe. Depending on the game, the player must utilize a drag-and-drop method or a click-based approach to solve an AI problem. The purpose of the study is to examine several CAPTCHA implementations, compare their flaws, and discuss security-related issues. Many CAPTCHAs employ click-based techniques, requiring the user to recognize the images based on their look and click appropriately. However, image processing methods like object classifiers may be used to bypass this type of CAPTCHA. Although it requires action or the solution of an intellectual issue, dragging an object to the desired location is an efficient method. Relay attacks may compromise the system if an item is automatically dragged to the target location.**

Keywords—Web Security, Picture Recognition, Mathematics CATPCHA, Image Processing, Relay Attack.

I. INTRODUCTION

In essence, the CAPTCHA was developed in the middle of the 2000s as a method of determining if a person was human or a robot—a sort of Turing Test. The exam wasn't entirely computerised; instead, humans had to try to decipher some twisted writing that was incomprehensible to computers and hope we got it right. It finished the task. Additionally, Google recognised an opportunity for something else because so many web clients regularly completed these tests. After CAPTCHA was acquired in 2009, it changed to reCAPTCHA, and we were assigned the task of translating antiquated writing, whether or not we understood it. Sadly, the free record-keeping system would not last. According to a recent Google research, AI robots could decipher numbers in photos with 90% accuracy and CAPTCHAs with 99.8% accuracy. There needs to be another way to separate. Although this situation may appear simple, there is a highly complex cycle at work. In the background, Google conducts its own Turing Test in order to analyse how clients behave throughout all of their site connections. Designers are constantly looking for ways to make confirmation procedures easier for us while also making it much simpler for us to complete them. Move "The Honeypot" approach forward. The Honeypot concept simplifies things for customers while providing a successful method for eliminating those pesky spambots. Additionally, it has been discovered that humans will solve any issue if it benefits them. So picture a situation where we added a few invisible fields that spambots would have to fill out [1]. You can be relieved that those spambots are willingly surrendering themselves by making the check cycle unnoticeable so that humans aren't bothered by it in any way, especially when combined with Google's notable evaluation. Modern spam filters often result in more complex course of events. It is worth investing in because there are a few outstanding online tutorials that detail how to set it up. Making sure your customers can use autocomplete without being mistaken for a robot is the most important thing to watch out for [1]. Risk analysis may be evaluated in a number of situations by tackling challenging AI-based tasks, but these challenges must be simpler for humans to answer than for robots, and they must do it quickly. People who are blind or visually challenged struggle with CAPTCHAs. Screen readers and other commonly used assistive devices cannot decipher CAPTCHAs since they are designed to be incomprehensible by computers. This challenge can prevent access since some websites incorporate CAPTCHAs into the

initial registration process or even every login. In certain regions, site owners that use CAPTCHAs that discriminate against specific persons with disabilities risk becoming the subject of legal action.

II. Related Work

A. Related Works

The NOMAD non-intrusive moving-target defence system was proposed by Shardul Vikram et al. [2]. By generating random HTML components while having no effect on conventional clients, NOMAD prevents web bots from automating the access to web assets. In particular, NOMAD randomly distributes the name/id boundary upsides of HTML components in every HTTP structure page to prevent web bots from noticeably differentiating HTML components for further mechanisation. According to the evaluation, NOMAD can prevent this significant quantity of web bots with a relatively low expense. NOMAD may often be implemented at the server-side by modifying the web applications' source code. In order to avoid complicating the server-side logic of web applications, NOMAD might also be used as middleware between the server and the client. NOMAD may be used as a middleware, which makes it free and universally applicable to different web applications (without directly altering the source code) and client-side technologies (such as different programmes and modules). Accordingly, the middleware configuration will be simple for both servers and end users to understand. A CAPTCHA based on a finger guessing game that Cao Lei et al. [3] presented requires machines make a second logic judgement as the foundation for the identification, improving the complexity for machines to pass. Given the wide appeal of the finger-guessing game, the CAPTCHA clearly lessens the challenge of human identification. It represents a development in the field of image verification code technology. However, playing the finger-guessing game is not a sophisticated method of exactly securing the server. Due to different actions that push the screen for identification and diminish the CAPTCHA's effectiveness, the finger guessing game might occasionally become more perplexing and upset users.

Fig. 1. All Finger Gestures [3]

Ibrahim et al.'s [4] strategy was to require the user to rotate the cube while identifying the corresponding colours that were indicated with question marks. Once the user has recognised the character indicated on the 3D cube by rotating it, the system permits the user to access the object; otherwise, a new issue will be presented, the colour model will be altered, and a new task will be suggested. For a successful Turing test, the user must match the colours of the text box and the 3D cube as well as recognise the proper letter and write it there.

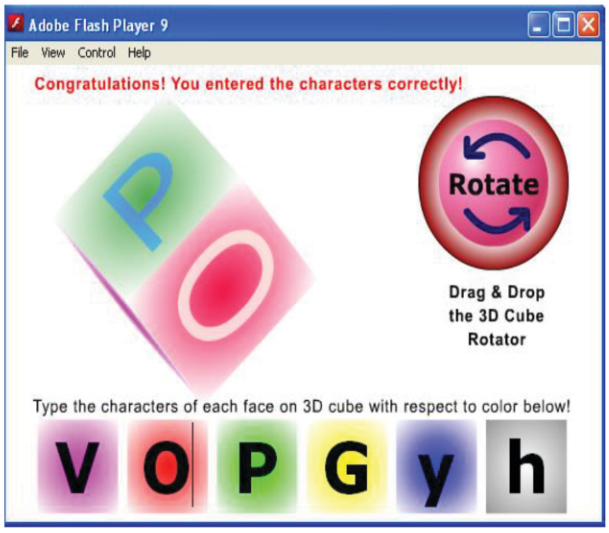

Fig. 2. 3D Cubic CAPTCHA [4]

A system based on vision that requires the user to identify the item based on distance was proposed by Aadhirai et al. [5]. The suggested system provides a representation of the real world, on which various types of things rely. User is required to identify a certain object that is farthest away from a given object in a system-generated challenge. Because of the fuzzy look, it may be challenging for persons with impaired vision to distinguish it from regular people. If observation is feasible, only humans, not robots, are capable of doing it. It is a very secure CAPTCHA with a challenging artificial challenge that bots cannot solve. The CAPTCHA that Nitisha Payal et al. [6] devised is based on hybrid pictures. A straight jigsaw puzzle-style Captcha called AJigJax uses drag-and-drop technology. The proposed work offers two levels of Captcha: CL1: AJigJax, for sites with minimal security requirements or no validation, and CL2: AJigJax, for sites with basic data that require confirmation to be completed and are often visited. We can categorically state that AJigJax Captcha is effectively handled, entertaining, less tiresome, and simple to comprehend based on the exhibition assessment of Captcha. As AJigJax is more straightforward than writing text to pass the test, it is safer. CL2: Since AJigJax now incorporates the concept of a graphical secret key, it needs to be handled by authorised clients. The audio CAPTCHA that is based on RastaPLP Features using SVM was proposed by Ahmet Faruk Akkmak et al. [7]. About 42% of the test digits can be distinguished correctly using the Naive Bayes approach. This technique also failed because each class component in the train set isn't modified since there are a lot of components in the commotion class (eleventh class) and relatively few components in the other classes (0 to 9). The test set's 100 sound documents were all partially perceived using the Naive Bayes technique. The commotion class has a usually low achievement speed of 71% since the number of components isn't altered, despite the fact that the classes from 0 to 9 may be somewhat perceived even in the train

set. Due to this, not all test sound documents are understood accurately, but whether a portion is incorrectly distributed to the clamour class or not, it means that the test component is misclassified. An evaluation mechanism for Flash-based CAPTCHA was proposed by Monther Aldwairi et al. [8]. According to the summary results, this CAPTCHA was the most advantageous to use because it was the easiest to complete and had the fewest disappointments. It was also thought to be the easiest to learn, the prettiest to complete, and the easiest to recall after being away from it for a long period. Additionally, compared to the current CAPTCHAs, Flash-based CAPTCHA requires fewer resources, making it easier to use. Since OCR attacks target text-based CAPTCHAs, the streak-based CAPTCHA is immune to them. Additionally, because this CAPTCHA requires mental processing power to solve, it is also immune to computerised attacks. Additionally, customers of all ages, educational levels, Internet proficiency levels, and, unexpectedly, those with vision impairments, had the chance to address it without any issues.

a. Flash-Based CAPTCHA

b. correctly solved CAPTCHA

c. unsuccessful attempt

Fig. 3. Drag and Drop Based Games [8]

A CAPTCHA that is grounded on game theory was proposed by Zhen Li et al. [9]. In this study, using a Stackelberg game theoretic framework, we explicitly modelled the interdependence of the decision-making of the attacker and defender. The break even points for selecting a machine solution or human solver may be identified through best response and strategy analysis. Contrary to conventional opinion, which advocates making CAPTCHA more difficult, we developed two methods that combine simple CAPTCHA with time delay restrictions and bitcoin mining. The outcomes produce a CAPTCHA business model that improves welfare while discouraging attackers from utilising human solvers. A CAPTCHA was suggested by Philip Kirkbride et al. [10] for intrusion detection. The authors of this research investigated the smart use of game-like CAPTCHAs as a method for information gathering to be used in developing a behaviour biometric for identifying dishonest record use. Given the need to improve security without sacrificing the user experience, it is believed that a game-like CAPTCHA can provide a response in the age of biometric social information. The designers propose that in order to do further research on the suitability of game-like CAPTCHA for account confirmation, a model game-like CAPTCHA be created and implemented as a feature of an interruption identification frameworks (IDS). If such a game is created using front-end web technologies like JavaScript and HTML, it will often be straightforward to collect the data using an old library like rrweb.io. The information acquired will be sent to a server-side data set following each game play. Instead of using the CAPTCHA a few times in a row, several guinea pigs will be allowed to use it on different days to simulate real usage. After that, meetings will be used with an SVM calculation to determine whether it can accurately separate the initial player from others. The underlying 5–10 game plays will be used as the enlistment time frame. Creators may attempt to further improve the pace of ID by combining various client credits like IP, client specialist, time-region, and login-time after accepting accurate results from this one-class SVM computation. A game-based CAPTCHA that is automatically generated was suggested by Hong Yu et al. [11]. The game-based CAPTCHA uses text-based concept marks for its basic implementation. As a result, a bot equipped with PC vision capabilities can unquestionably understand the text in the game.

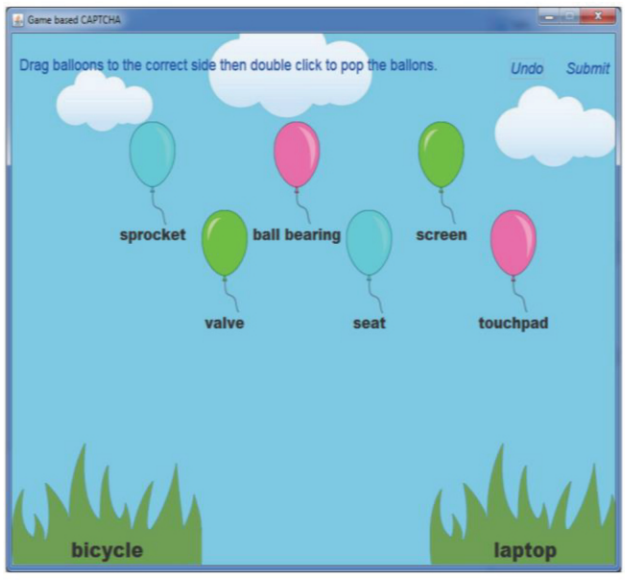

Fig. 4. A screenshot of a preliminary game-based CAPTCHA [11]

However, in order to bypass the CAPTCHA, the bot must also think critically about the relationships between the concepts, either by browsing the web or hacking into the information data set. The AGCG framework can be easily communicated with a private information data set that is safer for business usage, even though we remove the underlying information data set from ConceptNet, which is publically available. Because of the inadequacies of the information data set and the vast amount of possible conventional linkages, in an ideal world, private information data sets have relationships that do not entirely cover with public rational information data sets. Players may need a little more time to complete the suggested game-based CAPTCHA than they would need to use a computer to complete a standard visual CAPTCHA.

III. PROBLEM IDENTIFICATION

A technique based on image recognition called IRA (Image Recognition Annotation) was proposed by S. Ezhilarasi et al. [12]. Authors used morphology, transparency, and picture scaling in this system to distort the image. The photos now include some system-added noise, which complicates the processing of bots. But occasionally, adding noise to the image makes it difficult for humans as well. Humans should find CAPTCHA as simple as feasible, and it shouldn't take too long. It implies that CAPTCAH should be simple, quick, simple in terms of space requirements, and highly secure. Currently, CAPTCHA gaming is popular and demands that users pay attention by making it engaging. However, methods based on image processing, such as Google Lens, which uses tensorflow and yolo-based algorithms, are significantly more effective at identifying and classifying objects from photos and may circumvent the limitations of the image recognition-based CAPTCHA.

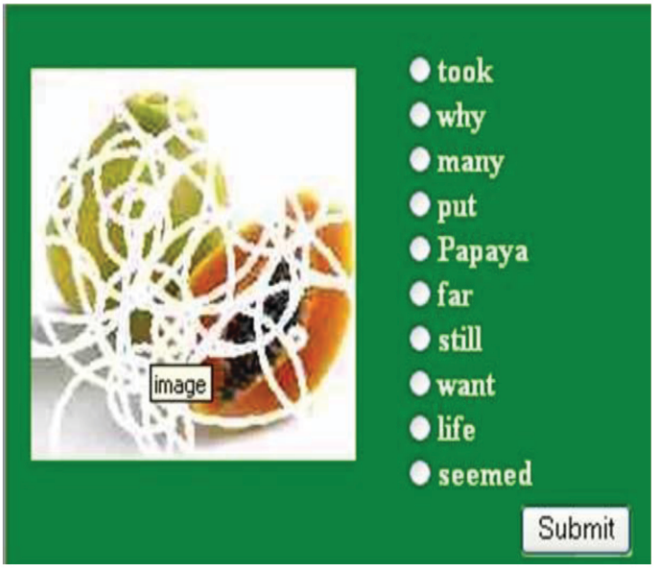

Fig. 5. IRA CAPTCHA for Distorted Picture [12]

Fig. 5 shows the IRA CAPTCHA where picture has been distorted and user is required to identify the picture and click on radio button accordingly. But sometime distortion level turns it more complicated for human too that may irritate users.

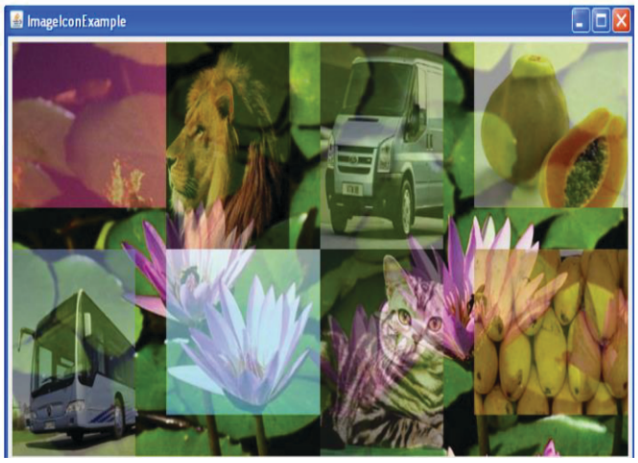

Fig. 6. IRA CAPTCHA for Overlapped Picture [12]

The IRA CAPTCHA is seen in Fig. 6, where users must recognise the picture and click appropriately since it has been overlaid with another image. It can make it difficult for consumers to find the right one.

IV. CONCLUSION & FUTURE SCOPE

The purpose of the article is to evaluate various CAPTCHA implementation systems. The majority of algorithms have been developed to recognise images in CAPTCHAs, whether they are in their original or warped form. Machine learning techniques may be used to identify normal images, although deformed images can also confuse humans. Some systems are based on flash games, however the difficulty of the games is often lower and often accessible to bots as well. Dragging anything to the desired location is not an intelligent strategy. A gaming CAPTCHA may now be improved and made more intelligent in order to more precisely safeguard the online premises. Games can be described as decisive games or as decision-based games. Games with a clear winner are frequently simple for humans but very hard for machines.

REFERENCES

[1] Adapt, CAPTCHA, 2018. [Online]. Available: https://www.adaptworldwide.com/insights/2018/the-evolution-of-captcha, [Accessed: 29- Jan- 2022]

[2] S. Vikram, Chao Yang and Guofei Gu, "NOMAD: Towards non-intrusive moving-target defense against web bots," 2013 IEEE Conference on Communications and Network Security (CNS), 2013, pp. 55-63, doi: 10.1109/CNS.2013.6682692.

[3] Cao Lei, "Image CAPTCHA technology research based on the mechanism of finger-guessing game," Third International Conference on Cyberspace Technology (CCT 2015), 2015, pp. 1-4, doi: 10.1049/cp.2015.0843.

[4] Ibrahim FurkanInce, YucelBatu Salman, Mustafa ErenYildirim and Tae-Cheon Yang, "Execution Time Prediction For 3D Interactive CAPTCHA By Keystroke Level Model" in Fourth International Conference on Computer Sciences and Convergence Information Technology of IEEE 2009.

[5] Aadhirai R, Sathish Kumar P J and Vishnupriya S, "Image CAPTCHA: Based on Human Understanding of Real World Distances" Proceedings of 4th International Conference on Intelligent Human Computer Interaction, IEEE 2012.

[6] N. Payal and R. K. Challa, "AJIGJAX: A hybrid image based model for Captcha/CaRP," 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON), 2016, pp. 38-43, doi: 10.1109/UPCON.2016.7894621.

[7] Cakmak, Ahmet & Balcilar, Muhammet. (2019). Audio Captcha Recognition Using RastaPLP Features by SVM.

[8] Aldwairi, Monther & Mohammed, Suaad & Padmanabhan, Megana. (2020). Efficient and Secure Flash-based Gaming CAPTCH.

[9] Z. Li and Q. Liao, "CAPTCHA: Machine or Human Solvers? A Game-Theoretical Analysis," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018, pp. 18-23, doi: 10.1109/CSCloud/EdgeCom.2018.00013.

[10] P. Kirkbride, M. A. Akber Dewan and F. Lin, "Game-Like Captchas for Intrusion Detection," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2020, pp. 312-315, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00061.

[11] Yu, Hong and Mark O. Riedl. “Automatic Generation of Game-based CAPTCHAs.” (2015).

[12] S. Ezhilarasi and P. U. Maheswari, "Image Recognition and Annotation based Decision Making of CAPTCHAs for Human Interpretation," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), 2020, pp. 1-6, doi: 10.1109/ICITIIT49094.2020.9071558.

[13] JingSong Cui, LiJing Wang, JingTing Mei, Da Zhang, Xia Wang, Yang Peng, WuZhou Zhang, “CAPTCHA Design Based on Moving Object Recognition Problem” in IEEE 2009.

[14] Jing-Song Cui, Jing-Ting Mei, Xia Wang, Da Zhang, Wu-Zhou Zhang , “A CAPTCHA Implementation Based on 3D Animation” in International Conference on Multimedia Information Networking and Security of IEEE 2009.

[15] Seyed Mohammad Reza1, Saadat Beheshti2 and Panos Liatsis3, “How Humans Can Help Computers to Solve an Artificial Problem survey”, international conference, IEEE 2015.