IJSRTM
https://www.ijsrtm.com
Vol.2 Issue 1 March 2022: 26-29
Published online 11 March 2022
E-ISSN: 2583-7141

International Journal of Scientific Research in Technology & Management

A Review on various CAPTCHA Techniques in the field of Turing Test

Arun Pratap Singh
Dept. of Computer Science & Engineering
Truba Institute of Engineering & Information Technology,
Bhopal, Madhya Pradesh, India
singhprataparun@gmail.com

Amit Saxena
Dept. of Computer Science & Engineering
Truba Institute of Engineering & Information Technology,
Bhopal, Madhya Pradesh, India
Amit.saxena78@gmail.com

Abstract— ***Human and automated intervention can be measured using the CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) security test. It is a test in which the intended intervention can be identified based on the subjects behavior or the way the problem is resolved. Numerous CAPTCHA challenges are available for you to select from such as distorted strings photo identification audio math and gaming CAPTCHA. In contrast to other CAPTCHAs game-based problems are both entertaining and incredibly secure. The player must use either a click-based or drag-and-drop method to solve an AI problem depending on the game. The study aims to analyze various CAPTCHA implementations contrast their shortcomings and talk about security-related concerns. The user must identify the images by their appearance and click the appropriate button in order to complete many CAPTCHAs which use click-based techniques. Nevertheless this kind of CAPTCHA can be gotten around using image processing techniques like object classifiers. Dragging an object to the desired location is an effective method but it necessitates action or the resolution of an intellectual problem. If an item is automatically dragged to the target location relay attacks could compromise the system.***

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

I. INTRODUCTION

In essence the CAPTCHA was created in the mid-2000s as a kind of Turing Test to determine whether a person was human or a robot. Rather than being fully computerized the exam required humans to attempt to decipher some twisted writing that computers couldn't understand and hope we got it right. The task was completed. Additionally because so many web clients consistently passed these tests Google saw a chance for something else. It changed to reCAPTCHA after CAPTCHA was purchased in 2009 and we were given the one. the undertaking of translating ancient literature regardless of our comprehension of it. Unfortunately the free system of record-keeping would not endure. A recent study by Google found that AI robots could interpret numbers in pictures with 90% accuracy and CAPTCHAs with 99.8% accuracy. Another method of separation is required. Despite the situations apparent simplicity a very intricate cycle is at play. Google uses its own Turing Test in the background to examine how users behave across all of their site connections. In addition to making confirmation processes much easier for us to finish designers are always searching for ways to make them easier for us. The Honeypot idea makes things easier for consumers while offering a practical way to get rid of those annoying spam bots. It has also been found that people will solve any problem as long as it serves their interests. Imagine then that we added a few invisible fields that spam bots would need to fill out [1]. You can feel relieved that those spam bots are voluntarily giving up by making the check cycle invisible so that people aren't bothered by it anyway especially when paired with Google's noteworthy assessment. These days spam filters frequently produce more intricate outcomes. Because there are some excellent online tutorials that explain how to set it up it is worthwhile to invest in. The most crucial thing to keep an eye out for is that your users can use auto complete without thinking it's a robot [1]. Risk analysis can be assessed in a variety of scenarios by addressing difficult AI-based tasks but these tasks need to be easier for humans to complete than for robots and they need to be completed fast. CAPTCHAs are difficult for blind and visually impaired people to complete. Because CAPTCHAs are made to be unintelligible by computers they cannot be decoded by screen readers or other widely used assistive technology. Access may be blocked by this difficulty because some websites use CAPTCHAs. first registration procedure or even each login. Site owners who employ CAPTCHAs that discriminate against particular people with disabilities run the risk of facing legal action in some areas.

II. Related Works

The non-intrusive moving-target defense system or NOMAD was put forth by Shardul Vikram and associates. [2] is made to stop web bots from automatically accessing web resources by creating random HTML elements on the fly. With this method automated bot activity is disrupted without affecting regular users. The name and ID attributes of HTML components within HTTP forms are specifically randomized by NOMAD making it challenging for bots to recognize and control them for automation. The evaluations findings show that NOMAD can effectively and reasonably cheaply block a sizable number of web bots. It can be implemented server-side by altering the source code of a web application. However NOMAD can also act as middleware between the client and the server to streamline server-side logic. Being a middleware solution NOMAD makes it possible to use it with a wide range of web applications and client-side technologies without requiring direct source code changes. Additionally servers and end users will find it easy to implement due to its simple middleware configuration. Additionally Cao Lei et al. [3] presented a finger-guessing game-based CAPTCHA that improves security by making machines perform an extra logical decision in order to be verified. This method makes it harder for bots to identify players while taking advantage of their familiarity with the game. Although the technique improves image verification technology it does not offer a server security solution that is 100% reliable. Screen gestures and touch actions are examples of user interactions that can occasionally lessen the effectiveness of the CAPTCHA leaving users more perplexed and irritated.

Fig.1.All Finger Gestures [3]

A technique created by Ibrahim and colleagues [4] asks users to rotate a 3D cube while recognizing the colors that correspond to it. A question mark is placed in specific areas of the cube to help users identify the character that is being shown. The system gives the user access to the object by enabling manipulation after it has been accurately identified. The color model changes presenting a new challenge and an alternate task if the user is unable to recognize the correct character. In order to pass the Turing test the user needs to correctly match the colors locate the matching text box and 3D cube and enter the right data in the appropriate space.

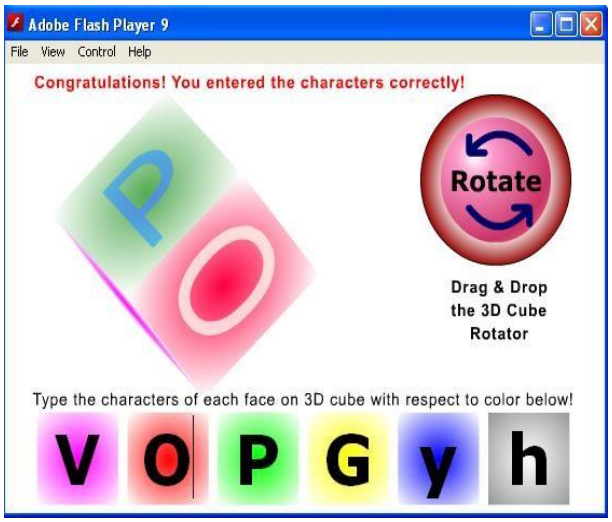

Fig.2.3D Cubic CAPTCHA [4]

Aadhirai et al. [5] proposed a vision-based CAPTCHA system where users identify the object farthest from a reference point, leveraging human perception to prevent bot access. Due to its fuzzy appearance, it is challenging for individuals with impaired vision but remains a highly secure CAPTCHA. Nitisha Payal et al. [6] introduced AJigJax, a hybrid image-based CAPTCHA that employs a drag-and-drop jigsaw puzzle mechanism, offering two security levels: CL1 for minimal security needs and CL2 for sites requiring authentication. AJigJax is engaging, easy to use, and safer than traditional text-based CAPTCHAs, incorporating a graphical secret key in CL2 for enhanced security. Ahmet Faruk Akkmak et al. [7] developed an audio CAPTCHA using RastaPLP features and SVM, but the Naïve Bayes approach faced classification issues due to imbalanced training data, leading to misclassification, particularly in the noise class. Monther Aldwairi et al. [8] evaluated Flash-based CAPTCHAs, finding them to be the most user-friendly, requiring fewer resources, and resistant to OCR attacks. Since solving them requires cognitive effort, they are difficult for bots to bypass, making them an efficient and inclusive solution for users of all backgrounds, including those with visual impairments.

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

Zhen Li et al. [9] proposed a CAPTCHA based on game theory, using a Stackelberg game framework to model the interaction between attackers and defenders. By analyzing strategy responses, they identified break-even points for choosing machine solutions or human solvers. Instead of making CAPTCHAs harder, they introduced methods combining simple CAPTCHAs with time delay restrictions and Bitcoin mining, creating a business model that enhances security while discouraging attackers from using human solvers. Philip Kirkbride et al. [10] suggested a game-like CAPTCHA for intrusion detection, exploring its use in behavioral biometrics to identify fraudulent account access. They proposed developing a game-based CAPTCHA using JavaScript and HTML, leveraging libraries like rrweb.io to collect behavioral data and store it in a server-side database. Multiple users interacting with the CAPTCHA over different days would simulate real-world usage, with an SVM algorithm analyzing gameplay sessions to distinguish between original and fraudulent users. The initial 5–10 plays would serve as an enrollment phase, and additional identifiers such as IP address, user agent, time zone, and login time could further improve identification accuracy. Hong Yu et al. [11] introduced an automatically generated game-based CAPTCHA that relies on text-based concept markers, but since bots with computer vision capabilities can easily interpret the text, its security may be limited.

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

A bot must not only identify concepts but also examine their connections in order to get past the CAPTCHA. This can be done by searching the internet or breaking into a data source. Despite being originally built on ConceptNet the AGCG framework can easily integrate with private datasets increasing its security for use in business applications. In order to minimize the risk of exploitation private datasets should ideally have distinct relationships that do not entirely overlap with knowledge that is available to the public. Players may take a little longer to finish the suggested game-based CAPTCHA than it would take to solve a typical visual CAPTCHA on a computer because of dataset limitations and the enormous number of potential conventional linkages.

III. PROBLEM IDENTIFICATION

S. Ezhilarasi et al. [12] IRA (Image Recognition Annotation) a CAPTCHA method based on image recognition was proposed. Morphology transparency and picture scaling are used by this system to warp images and system-generated noise is added to make bot processing more difficult. A lot of noise though can also make it difficult for people to understand. The perfect CAPTCHA should be easy to use quick space-efficient and extremely secure without being unduly complicated for users. Because they keep users attention and engage them game-based CAPTCHAs are currently becoming more and more popular. But sophisticated image processing methods like Google Lens which makes use of TensorFlow and YOLO-based algorithms have improved their efficiency in identifying and classifying objects potentially getting around the drawbacks of CAPTCHAs that rely on image recognition.

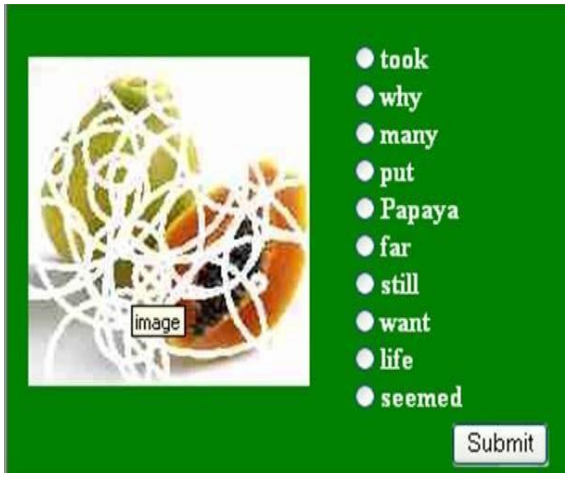

Fig.5. IRACAPTCHA for Distorted Picture [12]

Figure 5 displays the IRA CAPTCHA in which the user must recognize the distorted image and click the appropriate radio button. The distortion level however can occasionally make things more difficult for humans as well which could annoy users.

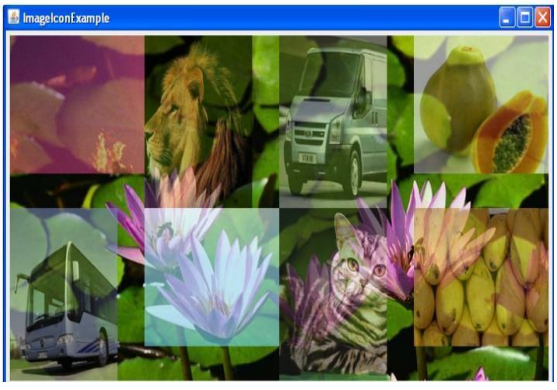

Fig.6.IRACAPTCHA for Overlapped Picture[12]

Fig. 6 displays the IRA CAPTCHA. Since the image has been superimposed with another image users must identify it and click the appropriate button. Customers may find it challenging to select the best one.

IV. Conclusion & Future Scope

Assessing different CAPTCHA implementation systems is the articles goal. Most algorithms are designed to recognize images in CAPTCHAs whether they are distorted or in their original format. While distorted images can also be confusing to humans' normal images can be recognized using machine learning techniques. Although some systems are based on flash games the games difficulty is frequently lower and they are also frequently accessible to bots. It is not a clever strategy to drag anything to the desired location. In order to better protect the online environment a gaming CAPTCHA can now be enhanced and made smarter. Games can be categorized as either decision-based or decisive. Humans often find games with a clear winner easy but machines find them extremely challenging.

References

[1] Adapt, CAPTCHA, 2018. [Online]. Available:https://www.adaptworldwide.com/insights/2018/the-evolution-of-captcha, [Accessed: 29- Jan- 2021]

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

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

[4] Ibrahim FurkanInce, YucelBatu Salman, Mustafa ErenYildirim andTae-Cheon Yang, "Execution Time Prediction For 3D InteractiveCAPTCHA By Keystroke Level Model" in Fourth InternationalConference on Computer Sciences and Convergence InformationTechnology of IEEE 2009.

[5] Aadhirai R, Sathish Kumar P J and Vishnupriya S, "ImageCAPTCHA: Based on Human Understanding of Real WorldDistances" Proceedings of 4th International Conference on IntelligentHuman Computer Interaction, IEEE 2012.

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

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

[8] Aldwairi, Monther & Mohammed, Suaad & Padmanabhan, Megana.(2020). Efficient and Secure Flash-based Gaming CAPTCH. Z.LiandQ.Liao,"CAPTCHA:MachineorHumanSolvers?AGame-Theoretical Analysis," 2018 5th IEEE International Conference onCyber Security and Cloud Computing (CSCloud)/2018 4th IEEEInternational Conference on Edge Computing and Scalable Cloud(EdgeCom), 2018, pp. 18-23, doi:10.1109/CSCloud/EdgeCom.2018.00013.

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

[10] Yu, Hong and Mark O. Riedl. "Automatic Generation ofGame-basedCAPTCHAs."(2015).

[11] S. Ezhilarasi and P. U. Maheswari, "Image Recognition andAnnotation based Decision Making of CAPTCHAs for HumanInterpretation,"2020InternationalConferenceonInnovativeTrendsinInformation Technology (ICITIIT), 2020, pp. 1-6, doi:10.1109/ICITIIT49094.2020.9071558.

[12] JingSong Cui, LiJing Wang, JingTing Mei, Da Zhang, Xia Wang,Yang Peng, WuZhou Zhang, "CAPTCHA Design Based on MovingObject Recognition Problem" in IEEE 2009.

[13] Jing-SongCui,Jing-TingMei,XiaWang,DaZhang,Wu-ZhouZhang

[14] , "A CAPTCHA Implementation Based on 3D Animation" inInternational Conference on Multimedia Information Networking andSecurity of IEEE 2009.

[15] SeyedMohammadReza1,SaadatBeheshti2andPanosLiatsis3,"HowHumansCan Help Computers to Solvean Artificial Problem survey",international conference, IEEE 2015.