REUSABLE CAPTCHA SECURITY ENGINE

Yamsani Vaishnavi
Department of Information Technology
Vardhaman College of Enginnering
Hyderabad, India
yamsanivaishnavi03@gmail.com

Touria Tanazzum
Department of Information Technology
Vardhaman College of Enginnering
Hyderabad, India
tanazzumtauriya@gmail.com

Hari Bharadwaj
Department of Information Technology
Vardhaman College of Enginnering
Hyderabad, India
hariyadav170802@gmail.com

***Abstract*—**Computers can be safeguarded against harmful bots with the help of CAPTCHA. Modern text-based CAPTCHAs have been shown to be vulnerable with the advancement of deep learning techniques. Consequently, much effort has been made to construct image-based CAPTCHAs,and a new direction in this evolution known as image-based visual reasoning is emerging. The Visual Turing Test (VTT) CAPTCHA was recently introduced by Tencent. It appears that this was the first time a visual reasoning method was used.

Later, additional CAPTCHA service providers (such as Geetest, NetEase, Dingxiang, etc.) offered their own visual reasoning frameworks to combat bots. So, it makes sense to inquire fundamentally: Are visual reasoning CAPTCHAs as secure as their creators anticipate? In this research, we describe the first method for resolving visual reasoning CAPTCHAs. We used a holistic assault and a modular approach, and on the VTT CAPTCHA, they respectively had overall success rates of 67.3% and 88.0%. The findings demonstrate that visual reasoning CAPTCHAs are less secure than expected; this most recent attempt to apply challenging, unique AI challenges for CAPTCHAs has not yet been successful. We also provide some recommendations for developing visual CAPTCHAs with greater security based on the lessons we learnt from our assaults.

I. INTRODUCTION

Systems susceptible to email spam, such as the webmail services of Gmail, Hotmail, and Yahoo!, can be protected with CAPTCHA. Additionally, CAPTCHA has been successfully used to prevent automated posting to blogs and forums, whether as a result of advertising, harassment, or vandalism. As automated utilisation of a service may be desirable up until it is done excessively and to the detriment of human users, CAPTCHA also play a crucial role in rate restriction. An illustration of a system with flaws that could be quickly fixed by utilising CAPTCHA. Bots are prevented from using a variety of computing services via CAPTCHAs. To stop bots from publishing spam links as comments or messages on blogs and online message boards, CAPTCHAs are utilised. The CAPTCHA system uses a question and response format. By posing questions that users must respond to, it is intended to shield any Web form from spam bots trying to submit information automatically. Additionally, it can identify brute force attacks, and by adding the visitor's IP address to the.access file, it will prevent further misuse. By confirming the visitor's IP address, CAPTCHA prevents unintentionally blocking useful bots. Additionally, CAPTCHA can be used as a bot trap that automatically blocks traffic. The recommendations contain an implementation guide for bot traps. Visual reasoning tasks based on computer vision and natural language processing have emerged in recent years as a result of expectations that computers will soon be able to understand complex tasks as well as humans thanks to the development and widespread application of deep learning.

II.LITERATURE REVIEW

A way to tell apart a human from a computer by a test is known as a Turing Test. When a computer program is able to generate such tests and evaluate the result, it is known as a CAPTCHA (Completely Automated Public test to Tell Computers and Humans Apart). In the past, Websites have often been attacked by malicious programs that register for service on massive scale. This has driven researchers to the idea of CAPTCHA-based security, to ensure that such attacks are not possible without human intervention, which in turn makes them ineffective. CAPTCHA-based security protocols have also been proposed for related issues, e.g., countering Distributed Denial-of-Service (DDoS) attacks on Web servers. A CAPTCHA acts as a security mechanism by requiring a correct answer to a question which only a human can answer any better than a random guess. Humans have speed limitation and hence cannot replicate the impact of an automated program. Thus the basic requirement of a CAPTCHA is that computer programs must be slower than humans in responding correctly. To that purpose, the semantic gap between human understanding and the current level of machine intelligence can be exploited. Most current CAPTCHAs are text-based. Commercial text-based CAPTCHAs have been broken using object-recognition techniques, with accuracies of up to 99% on EZ-Gimpy. This reduces the reliability of security protocols based on text-based CAPTCHAs. There have been attempts to make these systems harder to break by systematically adding noise and distortion, but that often makes them hard for humans to decipher as well. Image-based CAPTCHAs have been proposed as alternatives to the text media. More robust and user-friendly systems can be developed. State-of-theart content-based image retrieval (CBIR) and annotation techniques have shown great promise at automatically finding semantically similar images or naming them, both of which allow means of attacking image-based Captcha’s.

III. PROPOSED MODEL

The suggested CAPTCHA security system will create the CAPTCHA using a new, enhanced algorithm that can be engaging while also making it harder than before for bots to solve while appearing to be simple. Since humans are slower than computers when responding, we will fully utilise this and employ it in the suggested method. Humans are slower than computers because of this. The CAPTCHA security system will have a defined border line thickness and colour and a coloured graphical user interface with a maximum of two font sizes.

A. Text-based CAPTCHA's

Text-based CAPTCHAs used the anti-recognition concept for increased security and used the character recognition task as the underlying hard AI problem. Two examples of standard text-based CAPTCHAs are Gimpy and EZ-Gimpy. These two initiatives, though, have already been effectively dismantled. The general method used for early CAPTCHA cracking was segmentation followed by recognition. Designers therefore focused on anti-segmentation algorithms in an effort to block the successful extraction of characters from images. Wang et al. showed that text-based CAPTCHAs based on huge character sets, such as Chinese, Korean, and Japanese, are likewise insecure, in addition to text-based CAPTCHAs created with English letters and digits. Researchers have started to emphasize effectiveness in CAPTCHA-cracking due to the high success rates attained so far. Unsupervised learning, representation learning, limited training sets, the generative adversarial network (GAN)-based approach, and other machine learning techniques have also been used in cracking efforts.

B. Image-based CAPTCHA's

The most often used alternative to text-based CAPTCHAs is image-based CAPTCHAs. The following are some examples of how image-based CAPTCHAs can provide more information than the straightforward text-based approach, with additional categories and diversity in image material based on various AI problems:

CAPTCHA based on object recognition.

Object recognition was used as the underlying AI problem in early image-based CAPTCHAs. Users are typically asked to select particular images from a variety of categories in this form of CAPTCHA. The quantity of object categories affects how resilient an image-based CAPTCHA of this type is. Right now, object recognition-only image CAPTCHAs are insufficient.

CAPTCHA based on behavior detection.

A brand-new variation of CAPTCHA that relies on behaviour detection is the slider CAPTCHA. To fill in a notch in a background image, the user is asked to drag a slider, or they can just slide it from one side to the other. Such a CAPTCHA essentially presents an object detection and behaviour simulation challenge to a machine.The security of slider CAPTCHAs still need more analysis because an increasing number of protection methods tend to detect abusive traffic based on user interactions with the website, not just the behaviour when sliding the bar.

CAPTCHA based on facial recognition.

The hard AI challenge at the heart of image-based CAPTCHA creation is frequently the facial recognition task. In FaceCAPTCHA, a number of human faces are included into the background, and for further security, black colour blocks are added to the faces. However, both ruses have been exposed and defeated.

VI. IMPLEMENTATION

In today's digital landscape, where automated bots pose a significant threat to online security and user privacy, the need for effective CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) systems has become paramount. CAPTCHAs serve as a crucial line of defense, preventing automated bots from accessing sensitive information, conducting malicious activities, or spamming online platforms. However, traditional CAPTCHA systems often present challenges that are difficult for users and may lead to frustration and poor user experiences.

We have developed a website where it contains all the information about CAPTCHA. We have different sections related to CAPTCHA .We also included two python files where we demonstrate the usage of CAPTCHA. We included two buttons which relate to the different python files. First one is the demonstration of text based CAPTCHA. And the second one in the demonstration of image based CAPTCHA.

V. RESULT

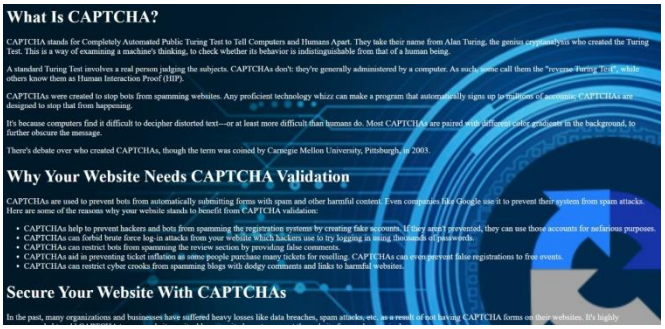

Fig. 1 Home page

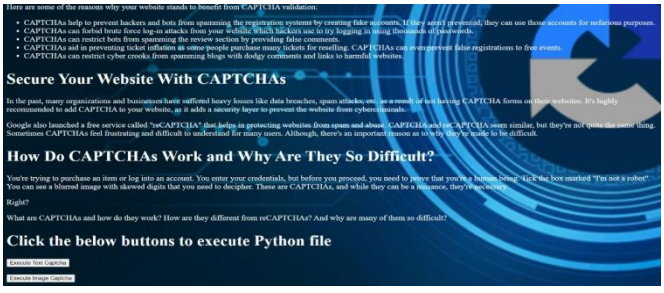

Fig. 2 Home page

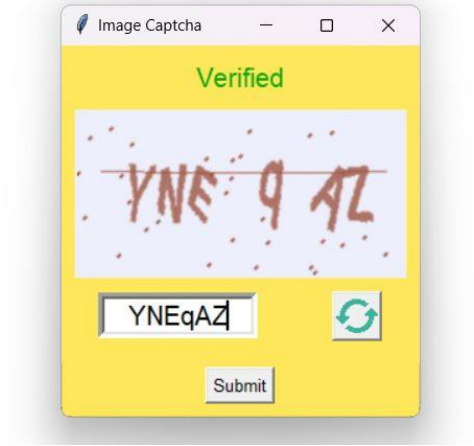

Fig. 3 Textbased1

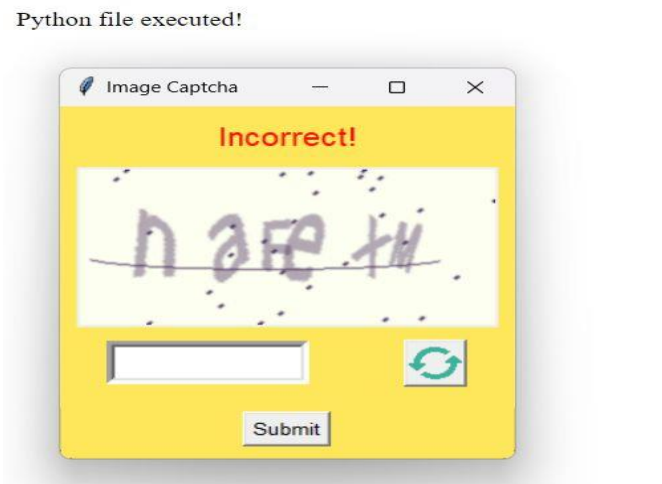

Fig. 4 Text-based 2

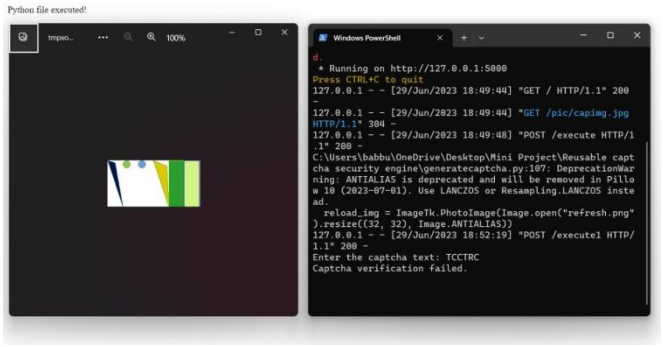

Fig. 5 Image-based 1

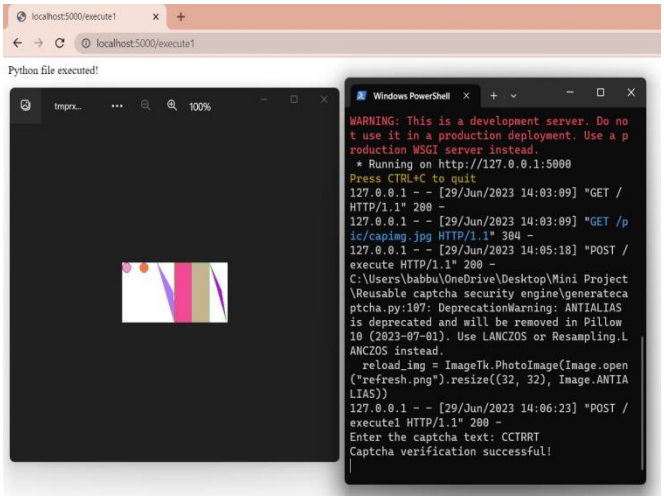

Fig. 6 Image-based 2

VI. CONCLUSION

In this research, we investigated the challenging AI issues that underlie the currently used CAPTCHAs and discovered that the traditional CAPTCHA methods have been shown to be vulnerable. By using both a holistic assault and a modular approach to thoroughly examine the security of one representative visual reasoning scheme, Tencent's VTT CAPTCHA, we were able to attain success rates of 67.3% and 88.0%, respectively. We also ran supplemental experiments on three different visual reasoning systems to gauge the robustness of our strategy. Our high completion rates demonstrate that the most recent attempt to apply challenging, unique AI problems (visual reasoning) for CAPTCHAs has not yet been successful. Further, we summarised three principles for future vision-related CAPTCHA design, and we think that applying common sense to CAPTCHA design in particular has promising prospects.

VIII. FUTURE DEVELOPMENTS

Better Image Recognition: As technology develops, image recognition algorithms may get more complex and precise, which could result in more reliable CAPTCHA systems.

Biometric CAPTCHAs: In order to further increase security, CAPTCHAs may contain biometric information, such as fingerprint or facial recognition.

Behavior-based CAPTCHAs: Future CAPTCHA systems may examine user behaviour, such as mouse movements, typing patterns, or surfing habits, to ascertain whether a user is human or a robot rather of depending exclusively on static tests.

VII. ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of the task would be put incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

We wish to express our deep sense of gratitude to Dr. Ganesh Regulwar , Associate Professor, Project Supervisor, Department of Information Technology, Vardhaman College of Engineering, for his able guidance and useful suggestions, which helped us in completing the project in time. We are particularly thankful to Dr. G. Suryanarayana, the Head of the Department, Department of Information Technology, his guidance, intense support and encouragement, which helped us to mould our project into a successful one.

We show gratitude to our honorable Principal Dr. J.V.R. Ravindra, for providing all facilities and support. We avail this opportunity to express our deep sense of gratitude and heartful thanks to Dr. Teegala Vijender Reddy, Chairman and Sri Teegala Upender Reddy, Secretary of VCE, for providing a congenial atmosphere to complete this project successfully. We also thank all the staff members of Information Technology department for their valuable support and generous advice. Finally thanks to all our friends and family members for their continuous support and enthusiastic help.

References

[1] vonAhn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008). reCAPTCHA: Human-Based Character Recognition via Web Security Measures. Science, 321(5895), 1465-1468.

[2] Elson, J., Douceur, J. R., Howell, J., & Saul, J. (2007).Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization. In Proceedings of ACM Conference on Computer and Communications Security (CCS).

[3] Yan, J., & El Ahmad, A. S. (2008). A Low-Cost Attack on a Microsoft CAPTCHA. In Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS).

[4] Bursztein, E., Bethard, S., Fabry, C., & Mitchell, J. C. (2014). The End is Nigh: Generic Solving of Text-Based CAPTCHAs. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS).

[1]