IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

Enriching Auto Image Captcha Generation through AI

Sakshi Ramesh Malunjkar[1], Payal Bhimaji Malunjkar[2], Rutuja Rajendra Kolhe[3], Sayali Eknath Kunjir[4], Prof. Pavan B. Shinde[5]
UG Student, Department of Information Technology[1,2,3,4]
Lecturer, Department of Information Technology[5]
Amrutvahini Polytechnic, Sangamner, Maharashtra, India

Abstract: *There has also been a considerable rise in the burden on numerous websites and web-based apps due to the huge expansion in the volume of the World Wide Web and the variety of subscribers on this network. This load comes from the user's end, resulting in an unanticipated state that leads to undesirable outcomes at the web server's end, such as a breakdown or an information leakage scenario. As a result, hence the necessity to minimize server load as well as the risk of networking assaults, which escalates as the number of users increases. The unintended effects, such as information leakage and server crashes, are produced by two primary factors: first, user overloading, and second, a growth in the volume of autonomous programs or robots. To circumvent the limitations of most traditional techniques to captcha production, this suggested model employs a flexible picture captcha generating methodology. To counteract this impact, we developed a system that generates captcha using a random object insertion mechanism. Convolutional neural networks are used in the presented methodology to effectively generate the captcha. The experimental outcomes have been indicative of the improved performance offered by the proposed approach.*

Keywords: Convolution Neural Network, CAPTCHA generation, Image Processing

I. INTRODUCTION

The World Wide Web has been utilized for the distribution of knowledge and information throughout the globe since its creation. The internet is a global network that integrates all devices to allow for efficient and meaningful interaction. The web is home to a large number of web pages, which serve as the principal method of collaboration and dissemination of knowledge. There are also a variety of web-based apps and other web pages that are used on the digital platform for a variety of reasons.

The improved accessibility of the online website resulted in a significant surge in the number of subscribers. As the percentage of subscribers grew, more people with unscrupulous intentions began to exploit the online interface for their malevolent purposes. Data leak and identity fraud are two examples, both of which cause a great deal of difficulty to other consumers.

To bring down internet sites using a variety of methods, including DDOS assaults and other measures that impair them. DoS assaults are huge and coordinated attacks that are undertaken expressly to use the website's whole resources to the point where it is depleted and can no longer serve. An incomprehensibly high number of users is necessary for this goal, which is met by building automated programs known as botnets. These programmed bots keep bombarding the webpage with requests, eventually exhausting all of the website's facilities and bandwidth. As a result, the website is forced to go offline, and genuine users are unable to access it. This is an extremely unfavorable situation that results in a significant deterioration in the level of the web page's consumer experience.

These assaults are quite popular, and assailants favor them since they are simple to set up, and the programmed bots can be simply copied a repeatedly to demolish the webpage. As a result, the captcha platform has been developed to combat these sorts of assaults. Captcha stands for a fully automated public Turing test that distinguishes computers from humans. This is an interactive verification criterion for determining if the visitors are a bot or a person. Captcha enables a website to determine if it is engaging with an automated system or a person. This essentially eliminates the difficulties caused by automated programs that hunt web sites. The majority of Captchas are text-based challenges that use tactics like deformation and letter adhesion, among others, to make it tough for an automated computer to solve yet quite simple for an individual to decode.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

The majority of these writings are presented in picture format, with several sorts of images available for categorization by the website's visitor. All of these tests are extremely tough for automated computers to answer, yet they are rather simple for a person to decode without very much difficulty.

Although most text-based Captchas are largely language-dependent, moving to an image-based Captcha is typically favoured for human identity verification. Humans create these images physically to make things easier to add tags and other elements for easy identification. All of this is normally stored in a database, which is inherently insecure since it is vulnerable to a variety of intrusions that can jeopardize the entire system. As a result, automatic captcha production is chosen over human database development, which has a number of flaws as well as a large cost.

Some of the approaches used to generate picture captchas are based on tasks that are nearly impossible for a machine to complete. Some visual captcha approaches, for instance, rely on the identification of features in an image. Features are extremely tough for even the most well-trained computer programs to recognize without a great deal of effort. Humans, on the other hand, are incredibly skilled at recognizing objects in a matter of milliseconds. This is due to the fact that humans have a part of the brain specialized to image recognition.

This gap between both the machine and the human can provide a very valuable edge that picture captcha solutions can take full advantage of. Another method is to use integers that have been heavily deformed and manipulated for identifying purposes. This is due to the fact that highly specialized optical character recognition for OCR techniques does not have a high enough precision to be useful for an automated bot. Humans, on the other side, can discern warped proportions with ease, allowing for a clear separation between the two sorts of customers depending on the image captcha.

Part 2 of this study paper focuses on the review of previous research projects, while section 3 delves into the specifics of the Captcha generation process. Section 4 discusses the suggested technique's assessment, and section 5 concludes the research by discussing the scope of future improvements.

II. LITERATURE SURVEY

Song Gao [1] emphasizes that the frequency of assaults on various internet webpages and other online services has increased, and that practically every web site depends heavily on CAPTCHAs to combat distinctive kinds of data breaches. For greater than 10 years, offensive-defensive development in CAPTCHA security, focused on computerized or auto-attacks, have advanced the understanding toward constructing safe CAPTCHAs. In this study, researchers continue this longstanding avenue of research by concentrating specifically on a recently developed variety of CAPTCHAs known as Moving-object or MO CAPTCHAs. When opposed to conventional text-based CAPTCHAs, MO CAPTCHAs incorporate a textual verification task within dynamically mobile elements in an aim to optimize both protection and accessibility.

Tao Zhang [2] "Completely Automated Public Turing Test to Tell Computers and Humans Apart" is abbreviated as CAPTCHA. It is a comprehensive automated application that can tell the difference between a user and a technology or a human. It protects webpages from being hacked. In particular, there seems to be a difficulty with captchas, which are tough for machines to solve yet simple for humans. Because most captcha are composed up of a collection, words, and Chinese characters, individuals started to try to break it. The classification of depending on the discipline is also known as captcha authentication. The classification method successfully employs a mix of planned occurrences that can be attacked and compromised. Therefore, the authors in this publication have proposed the use of Deep Learning to achieve the captcha recognition.

Nicolaus Boby Ardhita [3] defines the captcha concept as one of the most important parts of a website's real identity verification. It is intended to be a challenge that only individuals can resolve, yet machine learning is not quite up to the task. With the rapid advancement of AI algorithms in latest generations, CAPTCHA implementations have been a source of concern, since the algorithm may be 'trained' to resemble humans, allowing it to overcome CAPTCHA challenges. Furthermore, recent advances in Deep Learning (also known as deep neural networks) have made it easier to tackle real-world challenges. CAPTCHAs can be cracked using an AI system, according to a few studies. As a result, the authors recommend employing Expectation over Transformation as a strategy for creating robust pictures that may be employed in a variety of applications. The discriminator created by this approach are quite small and operate well on real-world item photos.

T. Kalaichelvi [4] Here a new encapsulation strategy that employs an innovative algorithm can achieve secrecy with the recipient is described. Rather than straightforwardly broadcasting our secret message utilizing conventional steganography

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

methodologies like Least Significant Bit algorithms, which are vulnerable to various steganalysis techniques, we will use an integration scheme with CAPTCHA verification to recognize the intended receiver. Again when the appropriate recipient has indeed been determined, the secret information will be successfully gathered and processed. Because the suggested solution uses pre-defined cryptographic operations algorithms to decipher the CAPTCHA, attackers will find it virtually hard to reconstruct the original CAPTCHA sequence, rendering communication more private and dependable.

S. Ezhilarasi [5] CAPTCHAs are totally designed for the protection of web - based operations at every level of online execution, according to the description. Various combinations of CAPTCHA have been developed, each with its own set of drawbacks. The suggested study, an image processing test in cybersecurity, Image Classification and Annotation oriented Decision CAPTCHA for subjective interpretation, discovered that the number of sections of the population the CAPTCHA to be simple to solve and that they had a higher success rate in logging in. The level of background complexity is low. It protects against DDoS (Distributed Denial of Service) assaults that are one of the most common internet assaults.

Navjot Rathour [6] explains that the paradigm of CAPTCHA has been one of the most useful methodologies that have been designed to achieve effective prevention of extensive attacks that are performed by the use of automated programs or bots. These attacks can cripple a network and have the ability to render the entire webpage unresponsive for the regular consumers or visitors to the website. There have been various improvements in the process of mitigating these effects to carry out major attacks on the server through automatically clearing the captcha. These approaches have increased the vulnerability of the system considerably which has resulted in the development of stronger and more resilient captchas. The approach stipulated in this research article has elaborated on the breaking of the text based captcha thorough the use of cross correlation.

Ashwani Kumar [7] explains captcha and its applications, which were created to protect automated chatbots and other programs from undermining numerous online applications and other ways. The objectives of this work is to create a full Captcha pipeline applications using the most up-to-date techniques, frameworks, and foundations, as well as Convolutional Neural Networks for smart identification. The challenge of extracting information from a paper image is difficult. Graph drawing is required for eliminating mistakes while selecting right characteristics for productive performance in various stages of pipeline construction. It also necessitates the development of algorithms and models on occasion.

Haiqin Weng [8] examine the safety concerns that prominent real-world image captchas face. The researchers suggest several proof-of-concept assaults targeting click-based slide-based captchas, and captchas selection-based captchas, to accomplish this goal. The researchers measured their assaults against common real-world captcha techniques, such as those offered by tencent.com, Google.com, and others, and found that they all worked. The assaults were also contrasted to prior approaches, online image identification solutions, and captcha-solving assistance that use human labor, according to the scientists. These cyberattacks create a substantial and reasonable threat to a variety of real-world image captchas, according to the findings. The method has helped in the development of several strategies for improving captchas.

Yu Hu [9] convey that the CAPTCHAs is a method of testing being used differentiate amongst people and devices in distributed environment. The research on CAPTCHA recognition can effectively discover holes in the integrity of the CAPTCHA, therefore eliminating certain harmful incursion in the networks. According to the CAPTCHA of pictures character distortion and adhesion, a CAPTCHAs identification technique based on convolutional neural networks is suggested in this study, and all characters in the image may be detected without segmentation. The entire network is segmented, allowing it to recognize the different personality lengths of the CAPTCHA image with small modifications. A multi task technical cooperation prototype is implemented to enhance network learning percentage and prototype generalization ability, and the entire network is presented to enhance the network learning rate and prototype generalization capabilities.

Tam V. Nguyen [10] SCAPTCHA is a system that uses object segmentation compositions to produce safe CAPTCHA pictures. To expand understanding about image-based CAPTCHA, the uniqueness is pulled both from object recognition and cybersecurity. This study provides a revolutionary cross - functional and cross approach for developing CAPTCHA material in specific. The findings of the study are used to build architectural standards and recommendations for the construction of CAPTCHA technologies. This is useful due to the paradigms effective realization of the secure captchas that can be effective in achieving the collages for the purpose of improving the security using the image processing approaches.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

III. PROPOSED METHODOLOGY

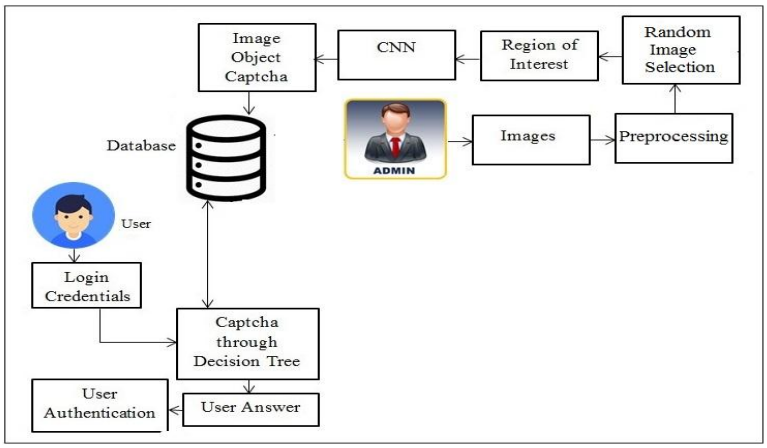

Figure 1: Proposed System Overview

The Proposed methodology for image captcha generation has been depicted in the system overview diagram given above. The presented technique for the captcha generation has been elaborated in much detail in the subsequent steps of the procedure that are illustrated below.

Step 1: *Random Object Insertion CAPTCHA generation through CNN* – In this step of the procedure the image captcha is generated through the use of two distinct image folders. One of the folders contains main captcha image and the other folder contains the object images that are inserted of embedded into the captcha image. The generation of the captcha image is initiated through the selection of an image from the captcha folder. This selected image is then resized to a fixed size of 170X170. The second folder containing the objects is then selected from which a random image is taken and resized to a size of 40X40.

The dimension of the images allows for the insertion of a maximum of 16 object images into the captcha base image. The object images are embedded into the captcha image are randomly and their positions are maintained in the form of a list. The base image is divided in the form of a fixed grid which is then used for the purpose of object image insertion. The random class of java is utilized to identify and estimate the number and the position of the object images in the main image. The estimation of the border of the object image to be inserted into the main image is identified using the first layer of the CNN.

CNN First Layer: In this step of the procedure the BufferedImage class of java is being utilized for the purpose of reading the random object image. This is image object is then subjected to the right shift operations to extract the respective RGB values of the image. The presence of the value of 255, 255, 255 is checked in the extracted values for RGB to identify any non-white pixels. The random object insertion for the generation of the captcha image is achieved through the replacement of the non-white pixels and their respective positions in the main image. The entire procedure is illustrated in the algorithm 1 given below.

ALGORITHM 1: Random Image object Captcha Generation

// Input: Image IMG, Random Image R_I
// Input: Random Positions A, B
// Output: captchaImage CAP_I
getCaptchaImage (IMG, R_I,A,B)
1: Start
2: CAP_I = IMG
3: ***for*** i = 0 to size of Width of R_I
4: ***for*** j=0 to size of Height of R_I
5: $P_S = R_{I[i][j]}$ RGB
6: R= P_S >> 16 & H_D
7: G= P_S >> 8 & H_D

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

8: B= P_S >> 0 & H_D
9: ***if*** (R ≠ 255 AND G ≠ 255 AND B ≠255), ***then***
10: CAP_I = CAP_I .setRGB (A+i, B+j, P_S)
11: ***end if***
12: ***end for***
13: ***end for***
14: **return** CAP_I

The randomness of the captcha is increased considerably through the use of the automatic and random generation of the questions that are stored in the database.

Step 2: *Captcha through Decision Tree and User Authentication* – The system initiates the database search once the user commences the login procedure and extracts the number of rows. This list is then subjected to random selection of the captcha details from the rows. The random image insertion captcha along with the respective question is provided to the user through the interactive graphical user interface through the swings framework. The user then views the captcha and answers the question which is then evaluated and if the answer is correct the user is authenticated and successfully logs into the system. An example of the captcha generation output is provided in the figure 2 given below.

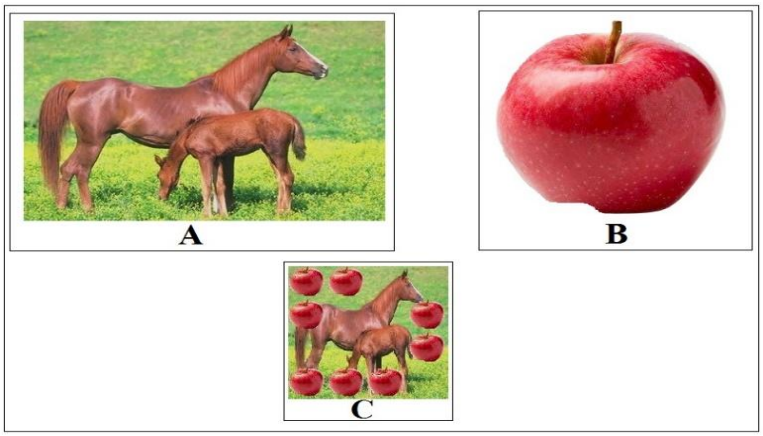

Figure 2: CAPTCHA input and output images.

The figure 2 above demonstrates an example of how the Random Object Insertion CAPTCHA generation procedure is performed. Firstly the image A is the main image or the base image of the captcha in which the random object is inserted. The image given in B is the image to be inserted into the main image, this is the object image that is supposed to be inserted. Once the objects have been inserted in random numbers at random locations, it results in the image C. This is the final captcha with the question, "How many apples are there in the image?". Once the user successfully correct answer that is 8, only then the login will be performed.

IV. Result and Discussions

The proposed methodology for security through CAPTCHA creation is coded in the java programming language. The development for this approach is performed on a machine running windows using the NetBeans IDE. The captcha information is being stored in the database through the use of the MySQL Database server. The development laptop has a configuration of 8 GB of RAM as primary memory along with 500GB of storage which is powered by an Intel Core i5 processor.

The presented approach is effectively evaluated through the use of extensive experimentation which is elaborated in detail in the section given below. The CAPTCHA in the presented approach is achieved through the use of random object insertion which is subjected to evaluation by a human subject. The output achieved by the image CAPTCHA approach is assessed for its accuracy and confirmed by a human evaluator. The evaluation is performed through the use of MRR or Mean Reciprocal Ratio which takes the human input as the assessment criteria for the system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

The submitted captcha output is assigned a rank in MRR that varies from 1 to 6 dependent on the correctness of the CAPTCHA creation engine for the specified pictures. If the human user provides a rank 1 for the CAPTCHA achieved then it designates its rank as 1, if rank 2 is provided then it indicates rank as ½, for rank 3 it is $^1/_3$, ¼ and finally for rank 5 as 0. Thus, the mean rank will be calculated for the collection of experiments through MRR as specified by the equations 1 and 2.

$$S = \sum_{i=1}^{n} 1 /(Ranki) \quad \_\_\_\_\_ (1)$$

$$MRR=S/N \quad \_\_\_\_\_ (2)$$

Where n – Number of Trails

MRR is measured for the image CAPTCHAS generated by random object insertion. This investigation is performed for a number of different users and the attained outcomes of the MRR assessment procedure is then logged in the Table 1 below Table 2 and. Table 1 illustrates the experimental outcomes for a single user and on the other hand the Table 2 displays the outcomes combined for 5 different users.

CAPTCHA for a user	1	2	3	4	5	6	7	8	9	10	MRR
Random Object Insertion	1	1	1	0.5	1	1	1	1	1	1	0.95

Table 1: Recorded MRR for a Single User

No. of users	Random Object CAPTCHA
1	1
2	1
3	0.95
4	0.95
5	1

Table 2: Recorded MRR for Consolidated 5 Users

Our suggested approach for Image CAPTCHA creation provides an aggregate MRR of 0.98. This MRR finding suggests an acceptable and satisfying outcome for the very first application of picture CAPTCHA generation capability through random object insertion.

V. Conclusion and Future Scope

The presented technique discusses about the image captcha generation technique through random object insertion. It has been discovered that conventional image CAPTCHA systems used limited strategies for the production of picture captchas, making them highly redundant. As a result, the strategy described in this paper outlines a novel way to Captcha creation via random object insertion. One of the most successful and challenging approaches to circumvent via the use of computer vision methodology is the introduction of random objects in a picture for the goal of identity verification. The user must count the amount of insertions and recognize the inserted item, which is added using convolutional neural networks. The empirical findings obtained a score of upwards of 0.98 using the mean reciprocal ratio. This demonstrates that the proposed strategy performs much better for such a novel captcha generation system when implemented for the first time.

This CAPTCHA generating approach may be put on numerous online apps and transformed into an API for seamless incorporation on these webpages and online domains in the long term for future research.

References

[1]. S. Gao, M. Mohamed, N. Saxena and C. Zhang, "Emerging-Image Motion CAPTCHAs: Vulnerabilities of Existing Designs, and Countermeasures," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 1040-1053, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2719031.

[2]. T. Zhang, H. Zheng and L. Zhang, "Verification CAPTCHA Based on Deep Learning," 2018 37th Chinese Control Conference (CCC), 2018, pp. 9056-9060, doi: 10.23919/ChiCC.2018.8482847.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

[3]. N. B. Ardhita and N. U. Maulidevi, "Robust Adversarial Example as Captcha Generator," 2020 7th International Conference on Advance Informatics: Concepts, Theory and Applications (ICAICTA), 2020, pp. 1-4, doi: 10.1109/ICAICTA49861.2020.9429048.

[4]. T. Kalaichelvi and P. Apuroop, "Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication," 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 495-499, doi: 10.1109/ICCES48766.2020.9138073.

[5]. 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.

[6]. N. Rathour, K. Kaur, S. Bansal and C. Bhargava, "A Cross Correlation Approach for Breaking of Text CAPTCHA," 2018 International Conference on Intelligent Circuits and Systems (ICICS), 2018, pp. 6-10, doi: 10.1109/ICICS.2018.00014.

[7]. A. Kumar and A. P. Singh, "Contour Based Deep Learning Engine to Solve CAPTCHA," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 723-727, doi: 10.1109/ICACCS51430.2021.9441737.

[8]. H. Weng et al., "Towards understanding the security of modern image captchas and underground captcha-solving services," in Big Data Mining and Analytics, vol. 2, no. 2, pp. 118-144, June 2019, doi: 10.26599/BDMA.2019.9020001.

[9]. Y. Hu, L. Chen and J. Cheng, "A CAPTCHA recognition technology based on deep learning," 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2018, pp. 617-620, doi: 10.1109/ICIEA.2018.8397789.

[10]. T. V. Nguyen, Z. Huang, S. Bethini, V. S. P. Ippagunta and P. H. Phung, "Secure Captchas via Object Segment Collages," in IEEE Access, vol. 8, pp. 84230-84238, 2020, doi: 10.1109/ACCESS.2020.2989258.