iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** VI **Month of publication:** June 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.35532

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VI Jun 2021- Available at www.ijraset.com*

# Designing Image Based Captcha using Machine Learning

Piyush Sable[1], Sakhlen Patel[2], Vipulkumar Bahilam[3], Rutuja Deshmukh[4], Nitesh Waghmare[5], Dr. Nikhil Karande[6]
[1, 2, 3, 4, 5]Student, [6]Associate Professor, G.H. Raisoni Institute of Engineering and Technology, Pune

***Abstract:*** ***Captchas, or Completely Automated Public Turing Tests to Tell Computers and Humans Apart, were created in response to programmers' ability to breach computer networks via computer attack programmes and bots. Because of its ease of development and use, the Text Captcha is the most well-known Captcha scheme. Hackers and programmers, on the other hand, have weakened the assumed security of Captchas, leaving websites vulnerable to assault. Text Captchas are still widely used since it is assumed that the attack speeds are moderate, typically two to five seconds for each image, and that this is not considered a significant concern. Style Area Captcha (SACaptcha) is a revolutionary image-based Captcha suggested in this paper, which relies on semantic data comprehension, pixel-level segmentation, and deep learning approaches. The suggested SACaptcha highlights the creation of image-based Captchas utilising deep learning techniques for boosting the security purpose, demonstrating that text Captchas are no longer secure.***

***Keywords: Captcha, text-based, security, deep learning, convolutional neural network, image-based.***

## I INTRODUCTION

Due to the widespread and automatic access to Web resources by robots, it is now necessary for Web service providers to anticipate whether the "user" is a person or a robot. A Human Interaction Proof (HIP) such as the Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) can help with this. Captcha is a reverse Turing test that Web service providers employ to protect human interaction from Web bots. Captcha is used as a defence mechanism against automated Web bots by a variety of Web services, including but not limited to free e-mail accounts, e-mail submission, online polls, chat rooms, search engines, blogs, password systems, and so on. This paper discusses several elements of Captcha systems, including their types, generation methods, assault resistance, and usefulness. It includes a comparison of existing Captcha techniques as well as the relative benefits of text and image-based Captcha schemes. It demonstrates how Captcha works and the general ways for generating them, as well as security and usability difficulties with Captcha approaches. It contains advice for improving the security of Captcha systems against various assaults, as well as advice for improving their usability. Deep learning algorithms can also be used to solve text-based Captchas. Using OCR, the attackers can simply get the text from a text-based Captcha. Style Area Captcha (SACaptcha), a novel image-based Captcha technique based on the neural style transfer technique, was proposed. Users must click foreground style-transferred parts in an image based on a brief explanation to pass the exam. Unlike previous image-based Captchas, SACaptcha focuses on human interpretation of semantic information and pixel-level segmentation, which machines appear to find more difficult to answer.

## II. RELATED WORK

A main feature [1] of such hollow CAPTCHAs is to use contour lines to form connected characters with the aim of improving security and usability simultaneously, as it is hard for state-of-the-art character recognition programs to segment and recognize such connected characters, which are however easy to human eyes. The analysis provides a set of guidelines for designing hollow CAPTCHAs, and a method from comparing security of different schemes. Advantages are: It improves usability. It finds a segmentation resistant mechanism that is secure and user-friendly simultaneously. Disadvantages are: Need to better design for getting better security.

In [2] paper, systematically analyzed the security of the two-layer Captcha. A novel two-dimensional segmentation approach is proposed to separate a Captcha image along both vertical and horizontal directions, which helps create many single characters and is unlike traditional segmentation techniques. Advantages are: It is a simple and effective method to attack the two-layer Captcha deployed by Microsoft, and achieves a success rate of 44.6%. It decreases time spent on data preparation and reduces manual labor. Disadvantages are: Need to design better two-layer or multi-layer Captchas with higher security levels than their predecessors.

The paper [3] introduces a novel approach to solving captchas in a single step that uses machine learning to attack the segmentation and the recognition problems simultaneously.
The algorithm to exploit information and context that is not available when they are done sequentially. Advantages are: The breadth of distortions proposed algorithm is able to solve shows that it is a general solution for automatically solving captchas. It removes the need for any hand-crafted component, making given approach generalize to new captcha schemes. Disadvantages are: Need to perform reverse Turing tests.
The paper [4] presents a fast, fully parameterizable GPU implementation of Convolutional Neural Network variants. All structural CNN parameters such as input image size, number of hidden layers, number of maps per layer, kernel sizes, skipping factors and connection tables are adaptable to any particular application. We applied our networks to benchmark datasets for digit recognition (MNIST), 3D object recognition (NORB), and natural images (CIFAR10). Advantages are: The best adaptive image recognizers. No unsupervised pretraining is required. The implementation is 10 to 60 times faster than a compiler optimized CPU version. Disadvantages are: It requires more computing power.
A novel approach for automatic segmentation and recognition of CAPTCHAs with variable orientation and random collapse of overlapped characters is presented in [5] paper.
The main purpose of this paper is to reduce vulnerability of CAPTCHAs from frauds and to protect users against cyber- criminal activities as well as to introduce a novel approach for recognizing either handwritten or damaged texts in ancient books, manuscripts and newspapers. Advantages are: It provides better segmentation of reCAPTCHAs. The required time for reCAPTCHA word breaking using extended approach is four times less than in approach of version 2011. Robust technique. Disadvantages are: Need to protect users against cyber-criminal activities and Internet threats.

## III. OPEN ISSUES

Lot of work has been done in this field because of its extensive usage and applications. In this section, some of the approaches which have been implemented to achieve the same purpose are mentioned. These works are majorly differentiated by the algorithm for Captcha systems.
Captcha robustness is to prevent automated attacks from achieving a success rate higher than 1%.
Increases the security of the image-based Captcha using SACaptcha.
Provides evidence that deep learning is a double-edged sword used to detect attack Captchas and improve the security of Captchas
To design and implement novel an image-based Captcha known as Style Area Captcha (SACaptcha) that is based on the neural style transfer techniques that are user friendly, require less server processing and offer improved security control against bots.

## IV. PROPOSED SYSTEM

Previous image-based Captchas have had a number of issues: some schemes require humans to manually select source images or add labels to images; some are based on a database, making them vulnerable if the database is compromised; some schemes have a high transmission cost; and, most importantly, almost all of them have been proven to be insecure. To address these concerns, presents Style Area Captcha (SACaptcha), a revolutionary image-based Captcha based on semantic information interpretation, pixel-level segmentation, and deep learning approaches. The proposed system is depicted in Figure 1. Select a single input content image for this project. After that, increase the number of foreground style-transferred regions in each Captcha image from 4 to 7. Each region's shape is chosen at random: it might be a rectangle, a triangle, a circle, or other irregular shapes like a heart, a leaf, or a moon. The original image is synthesised with one of these style-transferred images. To make a Captcha, randomly crop sections with different forms from other style-transferred photos and place them in the synthetic background. After that, write a quick summary to assist users in passing the test. The produced SACaptcha is the result.

### *A. Advantages*

*1)* SACaptcha are easy for humans to solve but remain difficult for computers.
*2)* SACaptcha are easy to generate and evaluate.
*3)* Improves the security of Captchas by utilizing deep learning techniques.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue VI Jun 2021- Available at www.ijraset.com*

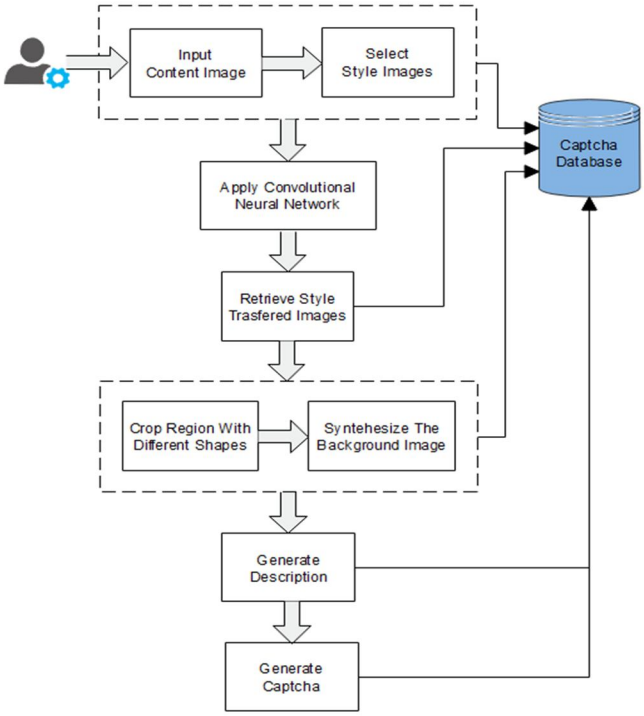



Fig 1: Proposed System Architecture

*B. Algorithm*

Algorithm1: Crop an Image$(, bottom)$
Input: image $I$, rectangle with corners $(top)$and $(-1, bottom - 1)$
Output: cropped image $I'$ of size $new - width \times new - height$

1) $new - width \leftarrow -$
2) $new - height \leftarrow bottom - top$
3) $I' \leftarrow AllocateImage(new - width, new - height)$
4) $for(x', y') \in I' do$
5) $I'(x', y') \leftarrow I(x' + y' + top)$
6) return $I'$

*C. Mathematical Model*

Content Image Selection and choose convolution layer for feature maps: Given a chosen content layer l, the content loss is defined as the Mean Squared Error between the feature map F of our content image C and the feature map P of our generated image Y.

$$\mathcal{L}_{content} = \frac{1}{2}\sum_{i,j}(F_{ij}^{l} - P_{ij}^{l})^2$$

Calculate Gram-matrix for style image: Calculate the **Gram-matrix**(a matrix comprising of correlated features) for the tensors output by the style-layers. The Gram-matrix is essentially just a matrix of dot-products for the vectors of the feature activations of a style-layer. If the feature map is a matrix F, then each entry in the Gram matrix G can be given by:

$$G_{ij} = \sum_{k} F_{ik}F_{jk}$$

The loss function for style is quite similar to out content loss, except that we calculate the Mean Squared Error for the Gram-matrices instead of the raw tensor-outputs from the layers.

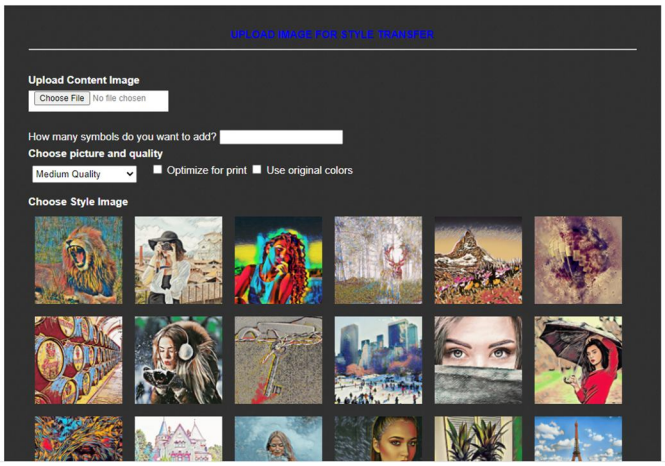
$$\mathcal{L}_{style} = \frac{1}{2}\sum_{l=0}^{L}(G_{ij}^{l} - A_{ij}^{l})^2$$

The total loss can then be written as a weighted sum of the both the style and content losses.

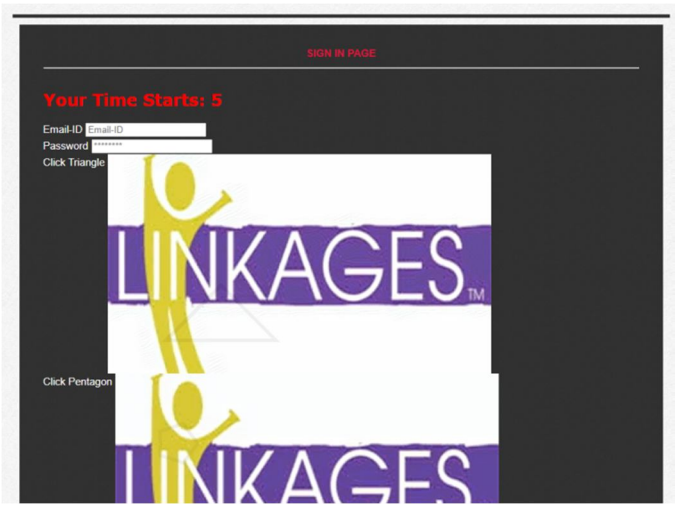
$$\mathcal{L}_{total} = \alpha\mathcal{L}_{content} + \beta\mathcal{L}_{style}$$

## V. RESULT AND DISCUSSION

### A. *Add Captcha*




### B. *Generate Captcha*

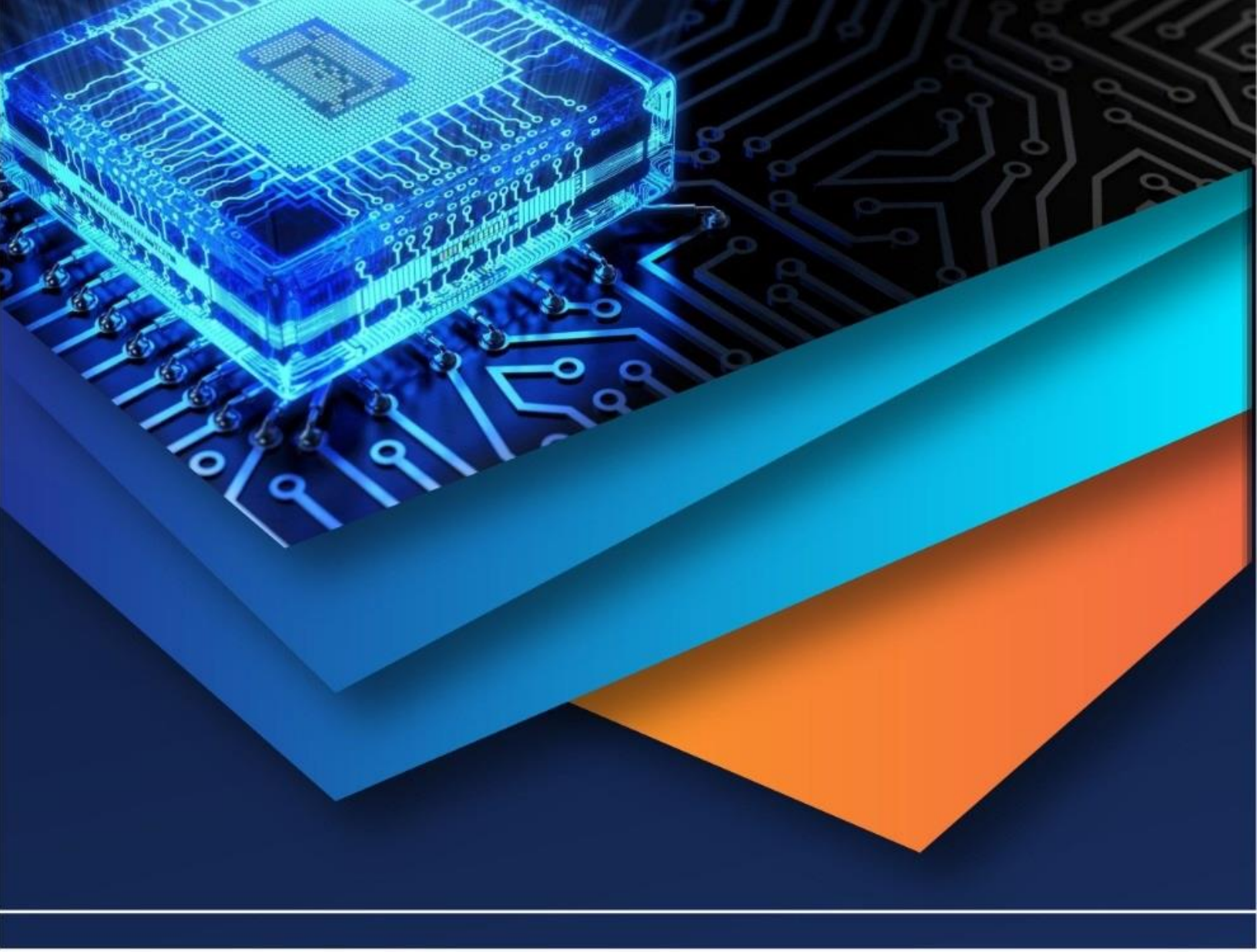


## VI. CONCLUSION

Using neural style transfer techniques, they proposed SACaptcha, a new image-based Captcha. The majority of early image-based Captchas are based on image classification difficulties, whereas SACaptcha depends on semantic information interpretation and pixel-level segmentation problems. This is a positive attempt to use deep learning techniques to improve the security of Captchas. Future research will focus on more efficient approaches to improve the security of text Captchas.

## REFERENCES

[1] H. Gao, W. Wang, J. Qi, X. Wang, X. Liu, and J. Yan, "The robustness of hollow captchas," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 1075–1086.
[2] H. Gao, M. Tang, Y. Liu, P. Zhang, and X. Liu, "Research on the security of microsoft's two-layer captcha," IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1671–1685, 2017.
[3] E. Bursztein, J. Aigrain, A. Moscicki, and J. C. Mitchell, "The end is nigh: Generic solving of text-based captchas." in WOOT, 2014.
[4] D. C. Ciresan, U. Meier, J. Masci, L. Maria Gambardella, and J. Schmidhuber, "Flexible, high performance convolutional neural networks for image classification," in IJCAI Proceedings-International Joint Conference on Artificial Intelligence, vol. 22, no. 1. Barcelona, Spain, 2011, p. 1237.
[5] O. Starostenko, C. Cruz-Perez, F. Uceda-Ponga, and V. Alarcon-Aquino, "Breaking text-based captchas with variable word and character orientation," Pattern Recognition, vol. 48, no. 4, pp. 1101–1112, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY