International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Adversarial Captcha

Soham Mirajgaonkar, Kartik Ballal, Shantanu Badgujar, Prof. Mrs.Laxmi Jadhav
Electronics and Computer EngineeringP.E.S's Modern College Of Engineering, Pune, India

Abstract: CAPTCHAs, tests to separate humans from machines, serve as a method to verify whether an interaction is being performed by a human or a computer, were developed in reaction to the vulnerability of computer networks to intrusions by programmers using bots and computer attack programs. The most popular Captcha scheme is the Text Captcha because of how simple it is to create and use. However, the presumed security of Captchas has been undermined by hackers and programmers, making websites open to attack.Given that attack speeds are generally moderate, usually ranging from two to five seconds per image and that this is not a serious worry, text captchas are nevertheless extensively utilized. This study proposes a novel image-based Captcha called Style Area Captcha (SACaptcha), which is built on deep learning techniques, pixel-level segmentation, and semantic data understanding.The proposed SACaptcha emphasises using deep learning to create neural networks neural networks image-based Captchas. Acquiring methods to enhance security and captcha systems are all covered in this paper.It compares the proving that text-based Captchas are insecure.

Key words: deep, text-based, security, and captcha Convolutional image-based learning

I.INTRODUCTION

Web service providers now need to determine if the "user" is a robot or a human due to the ubiquitous and automated access that robots have to online resources. This can be aided by a Human Interaction Proof (HIP) like the Fully Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA). Web service providers use Captcha, a reverse Turing test, to safeguard human contact against web bots. Many websites, including but not limited to free email accounts, email submission, chat rooms, search engines, blogs, password systems, and so forth, employ Captcha as a defense measure against automated Web bots.The types, generation techniques, attack resistance, and utility of various Captcha methods now in use and discusses the advantages and disadvantages of text- and image-based Captcha solutions. It illustrates the general methods for creating them, how they function, and the security techniques and usability issues associated with Captcha It offers suggestions for enhancing both the usability and security of Captcha systems against different types of attacks. Text-based Captchas can also be solved with deep learning algorithms. An attacker can easily obtain the text from a text-based Captcha by using OCR. A brand-new image-based Captcha method based on the neural style transfer methodology was proposed: Style Area Captcha (SACaptcha). To pass the test, users must click on style-transferred portions of an image by following a brief explanation. In contrast to earlier image-based Captchas, SACaptcha emphasizes pixel-level segmentation and human interpretation of semantic information—questions that robots seem to find more challenging to complete.

II.RELATED WORK

Using contour lines to create connected characters is a key component [1] of these hollow CAPTCHAs, which aim to simultaneously improve security and usability. This is because The paper [3] presents a novel method of answering captchas in one step by tackling the segmentation and recognition difficulties simultaneously with machine

learning. the algorithm to take advantage of context and information that are unavailable when carried out sequentially. Benefits include: The range of distortionsthat the suggested method can resolve indicates that it is a general solution for captcha solving automatically. It eliminates the requirement for any manually created element, enabling the provided method to be applied to new captcha schemes. The drawbacks are: It is necessary to run reverse Turing tests.

The paper [4] presents a rapid and fully configurable GPU-based implementation of different Convolutional Neural Network variations. Any specific application can be tailored to use with anyof the structural CNN parameters, including the size of the input picture, the number of hidden layers, the number of mappings per layer, the kernel sizes, the skipping factors, and the connection tables. Our networks were utilized on three benchmark datasets: CIFAR10, 3D object recognition (NORB), and digit recognition
connected characters are difficult for modern character .
software to segment and recognize, but simple for human eyes. The analysis offers a methodology for evaluating the security ofvarious systems as well as a set of rules for creating hollow CAPTCHAs. Benefits include: It enhances usefulness. It discovers a segmentation-resistant mechanism that is both safeand easy to use. The drawbacks are:
Better design is required to achieve greater security.

In the [2] paper, the security of the two-layer Captcha was thoroughly examined. In contrast to conventional segmentation algorithms, A new two-dimensional segmentation method is proposed to divide a CAPTCHA image both vertically and horizontally, enabling the extraction of multiple single characters. Benefits include: It is an easy-to-use technique with a 44.6% success rate for attacking Microsoft's two-layer Captcha. It cuts down on human labor and the amount of time needed to prepare data. The drawbacks are: It is necessary to create more secure two- or multi-layer captcha designs than the ones that came before them.
There is no need for unsupervised pretraining. The execution speed is between 10 and 60 times quicker than a CPUversion tuned by the compiler. The fact that it needs greater processing power is a drawback.

The study in reference [5] introduces a new approach for automaticsegmentation and recognition of CAPTCHAs with varying orientations and random character overlap. This work aims to decrease the susceptibility of CAPTCHAs to fraudulent operations,safeguard users from cybercrimes, and present a new method for identifying Text in old books, manuscripts, and newspapers that is handwritten or damaged. Benefits include: It offers improved reCAPTCHA segmentation. Using the enhanced strategy, reCAPTCHA word breaking takes four times less time than it did with the version 2011 approach. strong methodology. The drawbacks are: Users must be safeguarded from online risks and cybercrimes.

III.OPEN ISSUES

Because of its wide range of applications and usage, this field has seen a great deal of work. Several strategies that have been used toaccomplish the same goal are discussed in this section. The algorithm for CAPTCHA systems primarily differentiates these works.

I. Robust behavior of Captcha uses SACaptcha to increase the security of the image-based Captcha and prevent automated attacks from attaining a success rate higher than 1%. demonstrateshow deep learning is a two-edged tool that can be used to both detect and improve the security of Captchas.

II. Develop and implement Style Area Captcha (SACaptcha), a visual Captcha that leverages neural style transfer methods to deliver a user-friendly experience, minimize server processing,and offer heightened protection against automated bot activity.

III. Captcha employs sophisticated semantic data understanding, pixel-level segmentation, and deep learning techniques to generateimage-based Captchas. This approach bolsters security by making it much more difficult for

automated attacks to prevail, thereby improving website protection.

IV. PROPOSED SYSTEM

Earlier image-based Captcha schemes have encountered several challenges. Certain methods involve users manually labeling or selecting source images, which increases the complexity and time required for the process. Others rely on databases, making them susceptible to compromises if the database is breached. Additionally, many image-based Captcha schemes incur high transmission costs. However, the most significant issue is that the majority of these schemes have been proven to be insecure, leaving websites vulnerable to automated attacks. To address these challenges, this paper presents Style Area Captcha (SACaptcha), an innovative image-based Captcha solution. SACaptcha utilizes deep learning techniques, pixel-level segmentation, and semantic information interpretation to address the shortcomings of previous schemes. As illustrated in Figure 1, the proposed system simplifies the process by using a single input content image. In addition, SACaptcha boosts security by raising the count of foreground style-transferred sections in each Captcha image from four to seven, making it far more resilient to automated attacks.

Advantages:

1. While SACaptchas are simple for people to solve, they are still challenging for computers.
2. SACaptchas are simple to create and assess.
3. Uses deep learning methods to increase the security of Captchas.

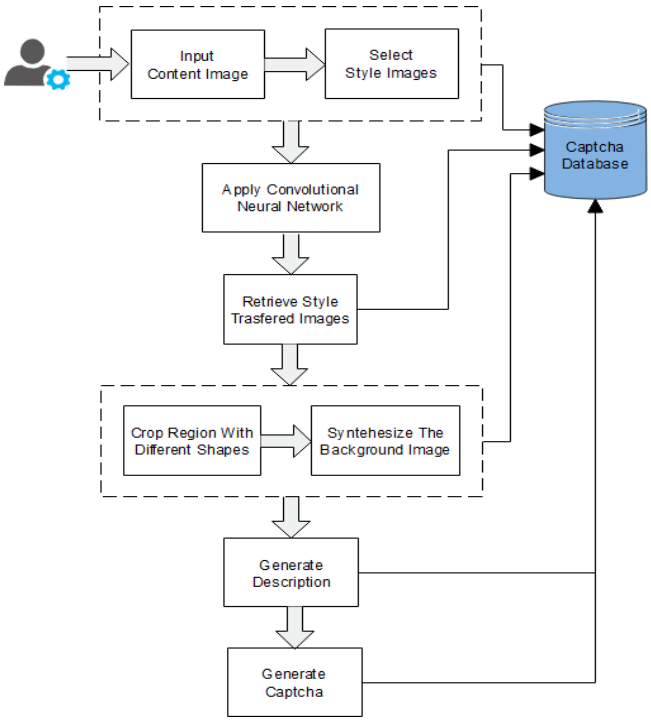


Fig 1: Block Diagram (System Architecture)

V. Algorithm

Algorithm1: Crop the Image $(I, left, top, right, bottom)$

Input: image I, with rectangular corners $(left, top)$ & $(right - 1,$

$bottom - 1)$

Output: Image (Cropped) I' of size $new - width \times new - height$

1. $new - width \leftarrow right - left$
2. $new - height \leftarrow bottom - top$
3. $I' \leftarrow AllocateImag\ (new - width, new - height)$
4. $fo\ (x\ ', y\ ') \in I\ '\ do$
5. $I\ '\ x\ '\ , y\ '\ (\ ) \leftarrow I\ x\ ' + left, y\ '\ (\ + top)$
6. return I'.

V. Mathematical Model

Choosing content images and selecting a specific convolutional layer for feature maps involves defining the content loss as the mean squared error between the feature map F from the content image C and the feature map P from

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

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

the generated image Y, based on a selected content layer l.

Calculate the Gram matrix for the fashion image: The Gram matrix is a matrix representing the correlations between the tensors from the style layers. It consists of dot products between the vectors of feature activations from a style layer. Specifically, each element in the Gram matrix G is computed based on a feature map matrix F as follows:

The style loss function is similar to the content loss function,

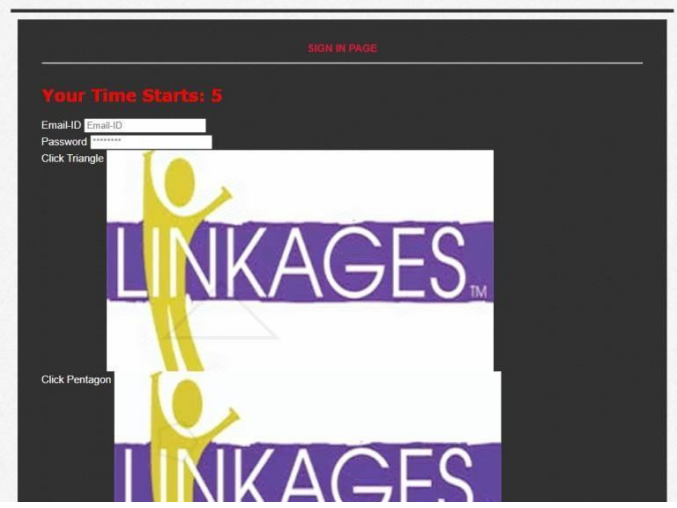
$$G_{ij} = \sum_k F_{ik} F_{jk}$$

but it uses mean squared error between the Gram matrices instead of relying on the raw tensor outputs of the layers.

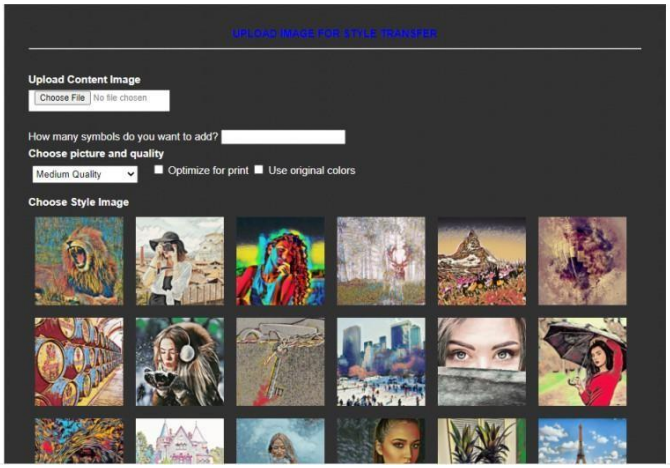
The total loss can be described as the sum of the weighted content and style losses combined.

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

VI. RESULT AND DISCUSSION



1. Add Captcha



2. Generate Captcha

VII. CONCLUSION

They proposed SACaptcha, a novel image-based Captcha that utilizes neural style transfer techniques. Unlike previous image-based Captchas that focus on image classification tasks,SACaptcha addresses pixel-level segmentation challenges andinterprets semantic data. This is a commendable effort to leverage deep learning methods to enhance Captcha security. Future studies will concentrate on more effective methods for enhancing text Captcha security.

VIII. EFERENCES

[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 SIGSACconference 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 JointConference on Artificial Intelligence

[5] . O. Starostenko, C. Cruz-Perez, F. Uceda-Ponga, and

Alarcon-Aquino, “Breaking text-based captchas with variable word and character orientation,” Pattern Recognition.