IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 6.252

Volume 2, Issue 1, December 2022

Deep Learning based CAPTCHA Solver for Vulnerability Assessment

Nithin K Shine, Arunava Mukherjee, Sradha N
Department of Electronics and Communication/Computer Engineering
Vellore Institute of Technology, Chennai, Tamil Nadu, India

Abstract: *Captcha or Completely Automated Public Turing test to tell Computers and Humans Apart. Almost every website now has process of checking whether the website is being crawled by some sort of automated bots or not. Earlier there was too much attacks on the website using bots which used to cause a lot of harm to the big companies through Denial-of-Service attacks. CAPTCHA helped websites a lot in preventing the attacks via bots but now the world is much more advanced and with some lines of codes attackers can break distinct types of captchas and that is what this project is. This project proves the point that now captchas are just a matter of hindrance that decreases the human experience with the various websites as even sometimes they cannot enter the captcha that a bot can easily break and waste the valuable time of human. This project "Deep Learning based CAPTCHA solver for Vulnerability Assessment" proves this point by breaking the various sorts of captchas like numerical, alphanumerical, circle captcha, captcha v2 etc. with noise like line, dots, etc. The above stated points are proved by getting fairly good accuracies. LSTM based Convolutional neural network is used for this purpose; some captchas were easy to break with only a few layers while some took pretty big networks..*

Keywords: Captcha

I. INTRODUCTION

With the help of the bots used for cracking the captchas the attackers try to perform cyber-attacks like Distributed denial-of-service which does not help the attacker in getting any sort of private information of the company or any data which the attacker may sell and get some good amount of money but just disturbs the normal traffic of the website , it becomes really difficult for one to distinguish between the sort of traffic is coming and the companies suffer from a lot of financial loss. Their servers get loaded with a lot of traffic that reduces human experience with the reputed websites. Similarly, there are a lot of attacks that can be pulled off with the help of these bots which definitely needs to be avoided but not with captchas that can be easily be cracked with the help of some bots.

Generally, these attacks take us to situations when bots act as humans, and tries to automate services to send a good amount of access databases, influence the online pools, unwanted emails, or surveys. In November 2020, Barracuda Networks, a leading provider of cloud-enabled security solutions, have

detected millions of bad bots' attacks on e-commerce websites in India. In March 2018, Google shut down its popular text CAPTCHA scheme reCAPTCHA which obviously proves that it is disturbing to humans to prove repeatedly that they are humans.

Some of the common captchas that the websites use is numerical or alphanumerical. Similarly, circle captcha, fish eyed captcha are also common. This project "Deep Learning based CAPTCHA solver for Vulnerability Assessment" focuses on breaking these CAPTCHAs along with the development of novel LSTM based CNN model that helps break CAPTCHAs with noisy lines and dots that is there to make it difficult for bots to crack the captcha. This project reveals the vulnerability of CAPTCHA system by proving that the text CAPTCHAs are getting difficult to solve by humans, while the attackers produce more powerful CAPTCHA breaker every single day. It is just a race between the captcha developers and the hackers, the developers produce some unique sort of captcha and the hackers just find the way out to crack it.

DOI: 10.48175/IJARSCT-7732

The efficiency of the existing system in breaking CAPTCHAs with noises is very less to address this issue we use LSTM network. LSTM networks resolve this issue as it allows the network to learn from long-term dependencies. It does this by replacing the single neural network layer found in an unstacked RNN with four neural network layers that interact with each other. Thus, the novel neural network algorithm is developed incorporating Stacked Long Short-Term Memory (LSTM) with which we aim to break CAPTCHA containing noise like lines and dots more efficiently.

II. PROPOSED SYSTEM

The CAPTCHAs were cracked with the help of Convolutional Neural Network(CNN). CNNs are reducing the gap between the humans and machines day by day. The help the machine to view the world as a human having various max pooling, dense, fully connected, and other layers too.

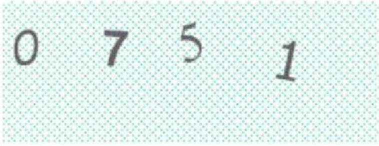

Figure 1: Numerical CAPTCHA

For numeric CAPTCHAs the network was trained with 500,000 randomly generated CAPTCHAs using Python Image Captcha Library and randomly generated numerical CAPTCHAs with the fixed lengths of five numeric. Keras, an open-source high-level Neural Network library is used. This is the summary of the model used for breaking the numerical captcha.

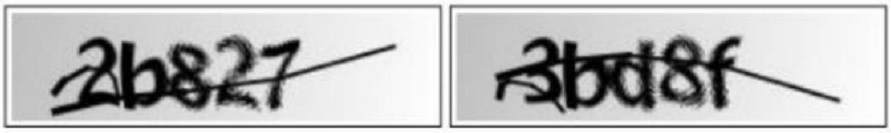

Figure 2: Sample of CAPTCHA version-2 dataset

Captcha version-2 can also be breaked with this proposed system. The numeric and alphabets in which the human gets confused like “I” and “1” and “O” and “0” can be totally avoided which is a good approach. It is clear that there is a great challenge in classifying the labels of such dataset. The reason behind this is the presence of certain amount of noise in the dataset in terms of clutter and scratch.

An Alex Net type model is used which can detect even those CAPTCHAs which are occluded by noise. The Alexnet has eight layers with learnable parameters. The model consists of five layers with a combination of max pooling followed by 3 fully connected layers and Relu activation is used in each of these layers except the output layer.

Using relu as an activation function accelerates the speed of the training process by almost six times. Dropout layers are also used, that prevent the model from overfitting.

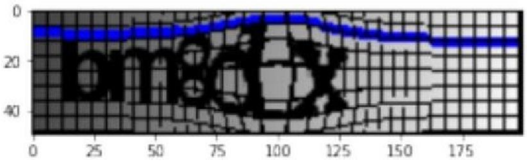

Figure 3: Fished eye CAPTCHA

There is a lot of variety of fished eye CAPTCHA. This type of CAPTCHA poses a challenge to machine learning systems. There is grid, a line and bold letters which is occluded by lines of distinct colours. The deep learning model keras model needs to learn each of the representation of the CAPTCHA dataset.

By adopting a Long Short-Term Memory (LSTM) architecture for the Neural Network and Connectionist Temporal Classification (CTC) loss for the loss function, we can read in a sequence and predict a sequence. A neural network architecture called Stacked Long Short-Term Memory (LSTM) is used for the same.

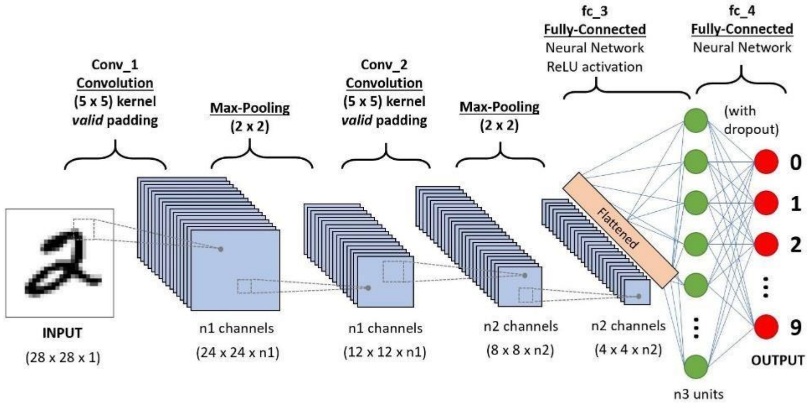

Figure 4a: Convolutional Neural Network architecture

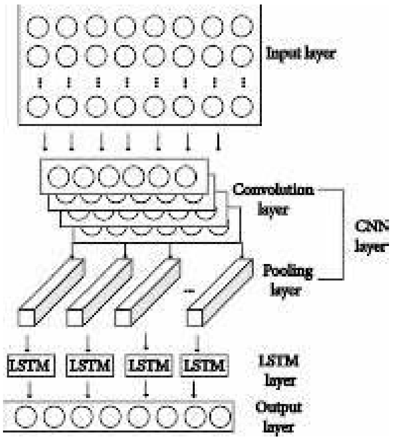

Figure 4b: LSTM based CNN model architecture

While Cross Entropy Loss compares a single input with a single output, Connectionist Temporal Classification (CTC) loss lets you compare an input sequence with an output sequence without the need to align them together. Previously, in order to classify sequences like CAPTCHA images, people have used rules to segment the characters with a bounding box first before recognising each digit individually, like in our previous MNIST classifier. Now, using CTC loss, we are able to train the classifier end-to-end, without any immediate steps.

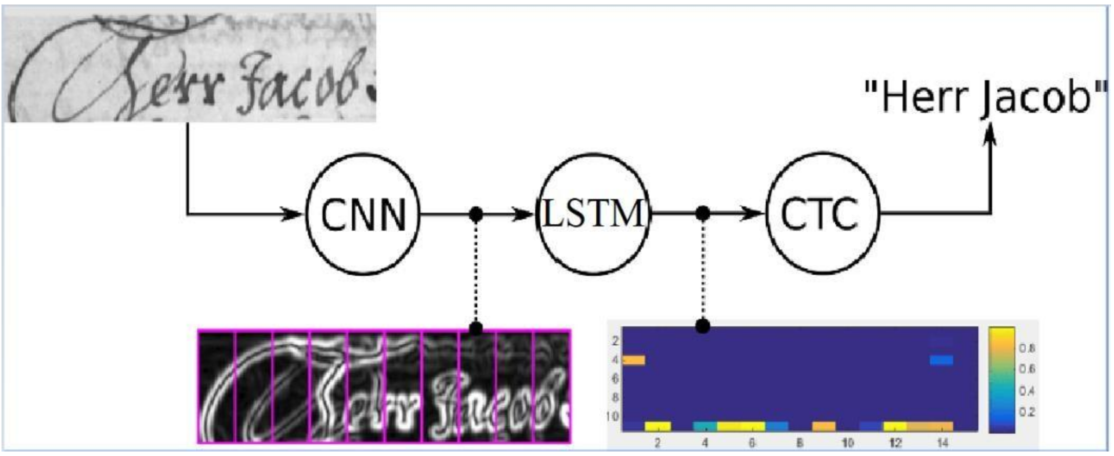

Figure 5: Flow diagram for LSTM based CNN model used

The idea behind CTC loss is to make a classification at each step in the sequence. In our case, each column of pixels in the CAPTCHA image is a step in the sequence and is read from left-to-right. The classifier can choose from the available labels (in our case, 0-9), plus a special BLANK label (denoted by "-") meaning that the classifier couldn't make a prediction.

An example of what the classifier may predict from sequentially classifying a 32-pixel wide CAPTCHA image: --00000-11---1122222

The classifier will have probabilities for each possible label at each step in the sequence, these can be multiplied together to get an overall probability for each of the valid sequences. The quantity for the loss function to optimise then, is the sum of the overall probabilities for all valid sequences.

ALGORITHM:

1. Import necessary libraries.
2. Input data files and list the files in the input directory.
3. Decode the text into indice of char list.
4. Split the dataset for training and testing.
5. Create convolutional layer with keras conv2D library
6. Create pooling layer and specify kernel size. Also create the Batch normalisation layer.
7. Create bidirectional LSTM layer and specify number of units.
8. Train the model
9. Test the model
10. Predict outputs on validation images
11. Use CTC decoder

IV. RELATED WORKS

Elie Bursztein et al segmented and recognized difficulties that are attacked simultaneously by machine learning with new single-step solution to captchas. This method can take advantage of knowledge and context that is not available when the two procedures are carried out sequentially by combining them. In addition, this does away with the requirement for any hand-crafted elements, enabling our so solution to generalise to new captcha schemes where the prior approach could not. [1]

Jiawei Su et al proposed a unique differential evolution-based technique for producing one-pixel adversarial perturbations (DE). Due to the built-in characteristics of DE, it can trick more types of networks and requires less hostile information (a black-box attack). The findings demonstrate that, on average, altering just one pixel can perturb 67.97% of the natural images in the Kaggle CIFAR-10 t test dataset and 16.04% of the ImageNet (ILSVRC 2012) test images to at least one target class. [2]

Mahdi Rezaei et al described the methods for object detection and object recognition that are important for the rest of the book. This concentrated on approaches to supervised and unsupervised learning. The chapter contained examples and different applications for each method, as well as technical information and assessments of each method's advantages and disadvantages. Information is offered to assist in choosing the best object detection method for computer vision applications, such as driver assistance systems. [3]

Suphannee Sivakorn et al did a thorough examination of reCAPTCHA and investigated how each request-related factor affects the risk analysis process. This found weaknesses through extensive experimentation that enable attackers to easily sway the risk analysis, get around limitations, and launch significant attacks. Then, developed a brand-new, low-cost method for semantically annotating photos using deep learning technology. With only 19 seconds needed per challenge, this algorithm is incredibly efficient, automatically resolving 70.78% of the picture reCAPTCHA challenges. We also use our method to successfully crack the Facebook image captcha, with an accuracy rate of 83.5%. [4]

B. Jhu et al suggested a cutting-edge IRC called Cortcha that is scalable to accommodate large-scale applications. It depends on recognising objects by taking advantage of the context around them, a process that computers struggle with but that people excel at. It is possible to create challenges using an endless variety of different types of objects, which can completely stop machine learning attacks from learning. The photographs in Cortcha's image database do not need to be labelled. Fully automated image collecting and CAPTCHA creation are also possible. This usability experiments show that Cortcha provides a slightly higher human accuracy rate than Google's text CAPTCHA, but on average takes longer to answer a challenge. [5]

Ping Wang et al presented an integrated attack architecture with a variety of attack modules and transfer learning techniques. Using this methodology, it thoroughly assesses the accuracy and effectiveness of known assaults on 20 CAPTCHA schemes. Its next look into the robustness of these widely-used schemes and learn about the consequences of previously unrecognised attacks. [6]

Kumar Chellapilla et al suggested that the future of creating more robust human-friendly HIPs is segmentation-based reading tasks. An illustration of a segmentation-based HIP is shown, along with a preliminary evaluation of its effectiveness and user-friendliness. [7]

REFERENCES

[1]. Elie Bursztein, Jonathan Aigrain, Angelika Moscicki, and John C. Mitchell. The end is nigh: Generic solving of text-based captchas. In Proceedings of the 8th USENIX Conference on Offensive Technologies, WOOT'14, Berkeley, CA, USA, 2014. USENIX Association.

[2]. J. Su, D. V. Vargas, and K. Sakurai, One Pixel Attack for Fooling Deep Neural Networks, IEEE Transactions on Evolutionary Computation 23 (2019) 828841.

[3]. Rezaei, Mahdi, and Reinhard Klette. ”Object Detection, Classification, and Tracking”. Springer International Publishing, 2017.

[4]. Suphannee Sivakorn, Iasonas Polakis, and Angelos D. Keromytis. I am robot: (deep) learning to break semantic image captchas. 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Mar 2016

[5]. Bin B. Zhu, Jeff Yan, Qiujie Li, Chao Yang, Jia Liu, Ning Xu, Meng Yi, and Kaiwei Cai. Attacks and design of image recognition captchas. In Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS'10, pages 187-200, New York, NY, USA, 2010. ACM.

[6]. Algwil, Abdalnaser, Dan Ciresan, Beibei Liu, and Jeff Yan. ”A security analysis of automated Chinese turing tests.” In Proceedings of the 32nd Annual Conference on Computer Security Applications, pp. 520-532. 2016.

[7]. K. Chellapilla, K. Larson, P. Y. Simard, and M. Czerwinski. Building Segmentation Based Human- Friendly Human Interaction Proofs (HIPs), . In H. S. Baird and D. P. Lopresti, editors, Human Interactive Proofs 1Berlin, Heidelberg2005.Springer Berlin Heidelberg.

DOI: 10.48175/IJARSCT-7732