IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204131 |

Survey Paper on Designing Image Based Captcha Using Machine Learning

Prof.R.L.GHULE, Bansode Prashant Arjun, Hajare Jaydeep Somnath , Raut Raju Vijaykumar, ShindeVishal Uttam

Department of Computer Engineering, S.B. Patil College of Engineering, Indapur, India

ABSTRACT: The capacity of programmers to infiltrate computer systems using computer attack programs and bots prompted to the development of Captchas, or Completely Automated Public Turing Tests to Tell Computers and Humans Apart. The Text Captcha is the most well-known Captcha conspire given its simplicity of development and ease of use. However, the hackers and programmers have reduced the expected security of Captchas, leaving websites open to attack. Text Captchas are still broadly utilized on the grounds that it is trusted that the attack speeds are moderate, regularly two to five seconds for each picture, and this isn't viewed as a basic risk. In this paper, a novel image-based Captcha known as Style Area Captcha (SACaptcha) is proposed, which depends on semantic data understanding, pixel-level segmentation and deep learning techniques. Experimental demonstrated that text Captchas are no longer secure, the proposed SACaptcha shows the development of image-based Captchas using deep learning techniques for increasing the security purpose.

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

I. INTRODUCTION

The substantial and automated access to Web resources through robots has made it essential for Web service providers to make some anticipation about whether "user" is a human or a robot. A Human Interaction Proof (HIP) like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) offers a way to make such a distinction. Captcha is a reverse Turing test used by Web service providers to secure human interaction assumed services from Web bots. Several Web services that include but are not limited to free e-mail accounts, submission of e-mail, online polls, chat rooms, search engines, blogs, password systems, etc. use Captcha as a defensive mechanism against automated Web bots. This paper presents various aspects of Captcha methods that include its types, generation methods, robustness against attacks and various usability aspects. It presents a review of existing Captcha schemes besides relative merits of text and image based on them. It illustrates working of Captcha and general methods used for their generation besides security and usability issues of Captcha methods. It provides guidelines to improve security control of Captcha methods against various possible attacks and guidelines to improve their usability. Also study the text based Captcha solving by deep learning techniques. The attackers easily retrieve the text using OCR technique from text-based Captcha. The proposed a new image-based Captcha technique known as Style Area Captcha (SACaptcha) that is based on the neural style transfer technique. To pass the test, users are required to click foreground style-transferred regions in an image based on a brief description. Unlike earlier image-based Captchas, SACaptcha relies on human understanding of semantic information and pixel-level segmentation, which seems to be more difficult for machines to solve.

III. 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 analysed 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

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204131 |

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 labour. 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.The Paper [6] We systematically study the design of image recognition CAPTCHAs (IRCs) in this paper. We first review and examine all IRCs schemes known to us and evaluate each scheme against the practical requirements in CAPTCHA applications, particularly in largescale real-life applications such as Gmail and Hotmail. Then we present a security analysis of the representative schemes we have identified. For the schemes that remain unbroken, we present our novel attacks. For the schemes for which known attacks are available, we propose a theoretical explanation why those schemes have failed. Next, we provide a simple but novel framework for guiding the design of robust IRCs. Then we propose an innovativeIRC called Cor-cha that is scalable to meet the requirements of large-scale applications. Cor-cha relies on recognizing an object by exploiting its surrounding context, a task that humans can perform well but computers cannot. An infinite number of types of objects can be used to generate challenges, which can effectively disable the learning process in machine learning attacks. Cor-cha does not require the images in its image database to be labelled. Image collection and CAPTCHA generation can be fully automated. Our usability studies indicate that, compared with Google's text CAPTCHA, Cor-cha yields a slightly higher human accuracy rate but on average takes more time to solve a challenge. The Paper [8] Recent advances in deep learning (DL) allow for solving complex AI problems that used to be considered very hard. While this progress has advanced many fields, it is considered to be bad news for Completely Automated Public Turing tests to tell Computers and Humans Apart (CAPTCHAs), the security of which rests on the hardness of some learning problems. In this paper, we introduce DeepCAPTCHA, a new and secure CAPTCHA scheme based on adversarial examples, an inherit limitation of the current DL networks. These adversarial examples are constructed inputs, either synthesized from scratch or computed by adding a small and specific perturbation called adversarial noise to correctly classified items, causing the targeted DL network to misclassify them. We show that plain adversarial noise is insufficient to achieve secure CAPTCHA schemes, which leads us to introduce immutable adversarial noise—an adversarial noise that is resistant to removal attempts. In this paper, we implement a proof of concept system, and its analysis shows that the scheme offers high security and good usability compared with the best previously existing CAPTCHAs. The Paper [9] Over the last decade, it has become well-established that a captcha's ability to withstand automated solving lies in the difficulty of segmenting the image into individual characters. The standard approach to solving captchas automatically has been a sequential process wherein a segmentation algorithm splits the image into segments that contain individual characters, followed by a character recognition step that uses machine learning. While this approach has been effective against particular captcha schemes, its generality is limited by the segmentation step, which is hand-crafted to defeat the distortion at hand. No general algorithm is known for the character collapsing anti-segmentation technique used by most prominent real world captcha schemes The Paper[10] Convolutional networks are powerful

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204131 |

visual models that yield hierarchies of features. We show that convolutional networks by themselves, trained end-to-end, pixels to-pixels, exceed the state-ofthe-art in semantic segmentation. Our key insight is to build "fully convolutional" networks that take input of arbitrary size and produce correspondingly-sized output with efficient inference and learning. We define and detail the space of fully convolutional networks, explain their application to spatially dense prediction tasks, and draw connections to prior models. We adapt contemporary classification networks (Alex Net [19],the VGG net [31], and Google Net [32]) into fully convolutional networks and transfer their learned representations by fine-tuning [4] to the segmentation task. We then define a novel architecture that combines semantic information from a deep, coarse layer with appearance information from a shallow, fine layer to produce accurate and detailed segmentations. Our fully convolutional network achieves state-of-the-art segmentation of PASCAL VOC (20% relative improvement to 62.2% mean IU on 2012), NYUDv2,and SIFT Flow, inference takes less than one fifth of second for a typical image

II. 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. CONCLUSION

The proposed a novel image-based Captcha named SACaptcha using neural style transfer techniques. Most early image-based Captchas are based on the problem of image classification, whereas SACaptcha relies on problems of semantic information understanding and pixel-level segmentation. This is a positive attempt to improve the security of Captchas by utilizing deep learning techniques. The future work will promote more-effective ways to enhance 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.
6. B. B. Zhu, J. Yan, Q. Li, C. Yang, J. Liu, N. Xu, M. Yi, and K. Cai," Attacks and design of image recognition captchas", image recognition CAPTCHA, IRC, object recognition,2010
7. M. Mohamed, N. Sachdeva, M. Georgescu, S. Gao, N. Saxena, C. Zhang, P. Kumaraguru, P. C. van Oorschot, and W.- B. Chen," A threeway investigation of a gamecaptcha: automated attacks, relay attacks and usability", Dynamic Cognitive Game (DCG) captchas,2015

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204131 |

8. M. Osadchy, J. HernandezCastro, S. Gibson, O. Dunkelman, and D. PerezCabo," No bot expects the deepcaptcha! introducing immutable ´ adversarial examples, with applications to captcha generation" CNN, Adversarial examples, HIP,2017
9. E. Bursztein, S. Bethard, C. Fabry, J. C. Mitchell, and D. Jurafsky," How good are humans at solving captchas? a large scale evaluation",2011
10. J. Long, E. Shelhamer, and T. Darrell," Fully convolutional networks for semantic segmentation",CNN,2015

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details