IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SURVEY ON DEEP LEARNING TECHNIQUES IN BREAKING TEXT-BASED CAPTCHAS AND DESIGNING IMAGE-BASED CAPTCHA

[1]Mr. Rohit Sharad Pore, [2]Mr. A. M. Dyade, [3]Mr. Vinayak. M. Sale

[1]SY M. Tech SVERI's COLLEGE OF ENGINEERING, PANDHARPUR

[2, 3]ASSIST. PROF. CSE DEPT. SVERI's COLLEGE OF ENGINEERING, PANDHARPUR

Abstract— **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 a deep dive survey on 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. We propose 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.**

Keywords— recognition; text-based CAPTCHA; convolutional neural network; deep learning

1. INTRODUCTION

The Completely Automated Public Turing test to tell Computers and Human Apart (CAPTCHA) [1–4] is a type of test to differentiate between humans and computer programs on Internet websites. CAPTCHA attempts to provide security against bots and can appear in many forms, including text, image, audio and video. Conducting research on recognizing CAPTCHA images is important because it helps identify weak points and loopholes in the generated CAPTCHAs and consequently leads to the avoidance of these loopholes in newly designed CAPTCHA-generating systems, thus boosting the security of the Internet.

Text-based CAPTCHAs are still a much popular and powerful tool against malicious computer program attacks due to their extensive usability and easy implementation. The majority of text-based CAPTCHAs consist of English uppercase letters (A to Z), English lowercase letters (a to z), and numerals (0 to 9). Other new large character sets, such as Chinese characters, have been used recently in text-based CAPTCHAs [5]. Numerous mechanisms have been developed to secure and strengthen text-based CAPTCHAs including background noise, text distortion, rotating and warping, variable string length, and merging of characters. However, due to the rapid evolution of deep learning in the past few years, CAPTCHA recognition systems have become more competent than before in breaking most of the current defence mechanisms of text-based CAPTCHAs [4][5]. As a result, sophisticated security mechanisms need to be developed to make text-based CAPTCHAs more robust against malicious attacks.

Deep learning techniques demonstrate an excellent ability to extract meaningful features from input images and have numerous applications in various areas, such as image restoration [1] and object detection [3]. These powerful characteristics of deep learning techniques make them a good choice for building robust CAPTCHA recognition networks to perform attacks against text-based CAPTCHAs. Although several CAPTCHA recognition algorithms use traditional digital image processing techniques in their implementation, these techniques still suffer from drawbacks (e.g., weak feature extraction ability and easily influenced by noise in input images). As a result, these techniques are being gradually replaced by the powerful deep learning approaches.

2. LITERATURE SURVEY

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.

3. PROPOSED TECHNIQUE

Previous image-based Captchas have describes various issues: some schemes require humans to manually select source images or add labels to images; some are based on a database, and if the database is compromised, they become vulnerable; some schemes incur a high transmission cost; and, most importantly, almost all of them have been proven to be unsecure. To overcome these issues, proposes a novel image-based Captcha named Style Area Captcha (SACaptcha), which is based on semantic information understanding, pixel-level segmentation and deep learning techniques.

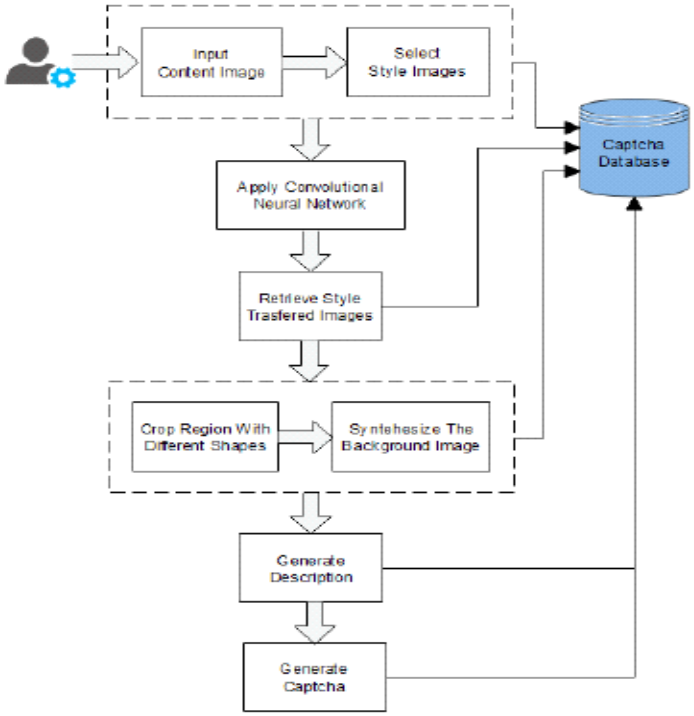

Fig 1 System Architecture

The proposed system describes in given fig.1. In this work, select single input content image. After create the number of foreground style-transferred regions in each Captcha image to 4 to 7 the style transfer images. The shape of each region is randomly selected: it can be a rectangle, a triangle, a circle or other irregular shapes such as a heart, a leaf, a moon and so on.

One of these style-transferred images is synthesized with the original image. Randomly crop regions with different shapes from other style-transferred images and relocate them in the synthetic background to generate a Captcha. After, generate a brief description to guiding users on how to pass the test. The output is the generated SACaptcha.

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.

4. 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.

5. Future Work

In the upcoming work we propose 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. This will find its application in Applications in surveillance and security, Google Applications, Microsoft Applications to name a few.

6. 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.