International Journal of Smart Security Technologies
Volume 9 • Issue 1

CAPTCHA Robustness:
AI Approach for Web Security

Abhishek Sharma, MyConcierge Pte. Ltd., India*
Shilpi Sharma, Amity University, Noida, India
Saksham Gulati, Illinois Institute of Technology, USA

ABSTRACT

Human verification is important to avoid spamming over the internet. The internet has grown tremendously in the last decade. Introduction to preference personalization makes the users experience and attract more people. This has deemed it necessary to verify that some of the actions are carried out by a human rather than a computer program. Methods like Captcha and ReCaptcha have been extensively used to overcome this challenge, but with the advancements in machine leaning and artificial intelligence, these techniques have started to become obsolete. So, to address this issue, the authors propose a phase-based human verification process using a combination of neural network and machine learning.

KEYWORDS

Captcha, Gesture Recognition, Human Verification, Neural Engine

1. INTRODUCTION

Verifying a user to be human has been a long requirement in the computer world and information technology. Advancements in technology have eased the process to create automation scripts and programs that can perform varied operations. Automation makes the process doing tedious and repetitive tasks quick, error free and accurate, but it can often be used for malicious purposes. An automation program can be executed to sign up a lot of accounts on some social networking platform and use them to grow someone's followers. Hence it is vital to detect if an action or a transaction is being caried out by a machine or a human.

Several strategies have been invented over the years to verify if the user is a human or a bot. The most popular of those is CAPTCHA which distinguishes bot from humans by creating words in camouflage in an image that can only be understood by a person. Another variation of it is called reCAPTCHA, which used images to realize the same target but using asking users to select images of a particular object or thing.

Although effective but these techniques have now started to become outdated and can be outsmarted by the modern bots. There are already many tutorials and videos posted by various

DOI: 10.4018/IJSST.299038 *Corresponding Author

people on how these verification programs can be bypassed. Also, the significant growth in artificial intelligence and machine learning in the last decade, will rendered these methods obsolete in not-so-distant future and will need to be replaced.

There have been some inventions to create alternatives to the existing human verification methods. In (Moradi & Keyvanpour, 2015), the author lists down the difficulties with the exiting Captcha methods and also discusses other techniques of human verification. One such techniques called is called rtCAPTCHA (Uzun, 2018), that uses facial and voice to distinguish a genuine user from a program.

In this paper we propose a new method for human verification through digital image processing. We aim build a method to confirm that the interaction is taking place with a human by leveraging the cameras and webcams on their devices.

2. LITERATURE REVIEW

Firstly, we aim to study and understand how the current version in actually attacked. The concept of captcha was introduced in 2000 and technology has taken a massive leap since then. Even before the machine learning era, all that was needed to overcome a traditional text-based captcha was a decent enough OCR.

In (Yan & El Ahmad,), an attack on Microsoft's captcha was conducted to test its strength. It was found that it can be attacked using a cheap attack based on segmenting. A more efficient attack on the yahoo captcha is described in (Gao et al., 2012). Although the attack specified in this publication is performed on the captcha from one provider, the concept can be applied to another captcha provides like google and Microsoft.

The only way captchas are able to defend against these attacks is applying background noise and make the characters more unreadable. This might work against a simple OCR but against a program that leverages machine learning, even these enhancements may not be enough. An experimental study is done conducted in (Alqahtani & Alsulaiman, 2020), where attacks using machine learning were performed on Google reCAPTCHA. The experiment showed how easily machine learning can be used to attack existing captcha. (Wang et al., 2019) show how a deep CNN program can be trained to identify different variation of a captcha. The most complete solution is presented in (Wang et al., 2020). The neural network developed by this method was tested on 20+ captcha variations and yielded a result of over 95%.

As mentioned before there have been techniques developed to overcome this challenge. Another attempt for captcha is mentioned in (Almazyad et al., 2011), where a combination of an image and text are used to make the process difficult for a bot. Another variation is designed to use characters in 3D shapes in (Imsamai & Phimoltares, 2010). Although it may be effective against an OCR but a NN can easily be designed to beat this variation.

A text-based captcha are basically testing the user's ability to comprehend distorted text, but a some other implementation have been proposed to test a user's cognitive skills. In (Gao, 2010), the captcha requires a user to solve a simple jigsaw puzzle. In (Vikram et al.,), the user is asked to map semantically similar images. In (Goswami et al., 2014), a user is asked to select face of real person from a set of pictures that also included animated and cartoon faces.

Our implementation will be using the face/hand detection for human verification. It will consist of two phases - Human Detection Phase and Verification Phase. For the Human Detection Phase, one layer will be implemented using HAAR cascades and another later with a Neural Network. One of the most effective implementation of face detection is MTCNN(Zhang et al., 2016), which is able to simultaneously also detect face features with high performance. In (Navabifar, 2011), the authors test 4 different CNN algorithms for face detection. An RCNN is used in (Sun et al., 2018) and (Jiang & Learned-Miller, 2017), that yields quick results for face detection. A different approach is described in (Farfade et al., 2015), which does not rely on face feature to detect faces, in fact it only requires a single model to be able to detect face in different orientations.