Visually Perceived Images to Tell Computers And Humans Apart

Ahmad Alamgir Khan
Senior IT Consultant
Muscat, Oman

***Abstract*— A CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used in computing to determine whether or not the user is human. This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. [1]**

In the recent years, a number of research projects have proven that it is possible to defeat the CAPTCHA. In October 2013 Vicarious [2] claimed that by leveraging core insights from machine learning and neuroscience, the Vicarious AI algorithm achieves success rates up to 90% on modern CAPTCHAs from Google, Yahoo, PayPal, Captcha.com, and others. This advancement renders text-based CAPTCHAs no longer effective as a Turing test. Mori et al. [3] published a paper in IEEE CVPR 03 detailing a method for defeating one of the most popular CAPTCHAs, EZ-Gimpy, which was tested as being 92% accurate in defeating it.

This research paper presents a novel approach to defend against the bots. VIPITCHA (Visually Perceived Images to Tell Computers and Humans Apart) is an approach based on reading the text and recognizing optical illusionary images. An optical illusion [4] (also called a visual illusion) is characterized by visually perceived images that differ from objective reality. The information gathered by the eye is processed in the brain to give a perception that does not tally with a physical measurement of the stimulus source. There are three main types: literal optical illusions that create images that are different from the objects that make them, physiological ones that are the effects on the eyes and brain of excessive stimulation of a specific type (brightness, colour, size, position, tilt, movement), and cognitive illusions, the result of unconscious inferences.

Optical illusions can only be perceived by humans. Since, optical illusions are visual images that differ from reality - the eyes and brain 'see' something that doesn't quite match the physical measurement of the image. Since the images differ from reality, it make it difficult to be manipulated by any AI algorithms or OCR softwares. The advantage is taken of such fact; a challenge-response is initiated by Server where user is provided with optical illusion images embedded with text. The user has to recognize the images that create the illusions from the set of images and enter the text for the verification.

General Terms--Preventing Bots, VIPITCHA, Artificial Intelligence, Optical Illusion et al.

Keywords--Bots, Botnets, Spambots, VIPITCHA - Visually Perceived images to Tell Computers and Humans Apart, CAPTCHA, Optical or Visual illusion, and Human visual perception.

I. INTRODUCTION

An Internet bot, also known as web robot, WWW robot or simply bot is a software application that runs automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. Another, more malicious use of bots is the coordination and operation of an automated attack on networked computers, such as a denial-of-service attack by a botnet. Internet bots can also be used to commit click fraud and more recently have seen usage around MMORPG games as computer game bots. A spambot is an internet bot that attempts to spam large amounts of content on the Internet, usually adding advertising links. [5]

According to the Incapsula [6], Bot traffic is up to 61.5% of all website traffic, the majority of website traffic (51%) was generated by non-human entities, 60% of which were clearly malicious.

The absence of inherent security features in the current web technologies have made it possible for attackers to exploit the flaws and take the significant advantage. There are several techniques to combat such attacks yet none have proven to be 100% full proof.

According to BBC [7], a network of thousands of computers stealing millions of dollars from advertisers by generating fake advert viewings has been discovered. British web analytics firm Spider.io claims the "Chameleon" botnet is made up of 120,000 home PCs and costs advertisers $6m (£3.9m) per month. Spider.io said that Chameleon simulated clicks on adverts on over 200 sites. The firm said the botnet was responsible for up to nine billion false ad views every month.

Not identifying Human to Computer has the global economy impact and is risky too. It can become part of networks of bots which can launch a devastating attack on any innocent victim. According to Microsoft's Richard Boscovich [8] Bamital botnet were being used for identify theft; it would hijack user searches, tricking users into clicking links on online advertisements. While the Bamital botnet defrauded the entire online advertising platform, which is what allows the Internet and many online services to be free, what’s most concerning is that these cybercriminals made people go to sites that they never intended to go and took control of the computer away from its owner.

In this paper, the VIPITCHA (Visually Perceived Images to Tell Computers and Humans Apart) aims to put forward a new approach to overcome the limitation of existing defense mechanisms.

The paper is structured as follows: Section 2 provides a brief overview of the different types of methods to prevent automated bots and their limitations. Section 3 presents an example that shows how the VIPITCHA works, and provides details about its implementation. Section 4 presents future work and concludes the article.

II. TYPES OF PREVENTION METHODS

CAPTCHA, reCAPTCHA, Asirra (Animal Species Image Recognition for Restricting Access) and etc. Below are some major categories:

A. CAPTCHA

A CAPTCHA [9] is a challenge-response test most often placed within web forms to determine whether the user is human. The purpose of CAPTCHA is to block form submissions by spambots, which are automated scripts that post spam content everywhere they can.

How secure is CAPTCHA?

Vicarious [2] claimed that by leveraging core insights from machine learning and neuroscience, the Vicarious AI algorithm achieves success rates up to 90% on modern CAPTCHAs from Google, Yahoo, PayPal, Captcha.com, and others.

B. reCAPTCHA

reCAPTCHA [10] is a user-dialogue system originally developed by Luis von Ahn, Ben Maurer, Colin McMillen, David Abraham and Manuel Blum at Carnegie Mellon University's main Pittsburgh campus, and acquired by Google in September 2009. Like the CAPTCHA interface, reCAPTCHA asks users to enter words seen in distorted text images onscreen. By presenting two words it both protects websites from bots attempting to access restricted areas [2] and helps digitize the text of books.

How secure is reCAPTCHA?

On 27 June 2012, Claudia Cruz, Fernando Uceda, and Leobardo Reyes (a group of students from México) published a paper [11] showing a system running on reCAPTCHA images with an accuracy of 82%. However, reCAPTCHA frequently modifies its system to confuse hackers.

C. Asirra

Microsoft Research Project [12] - Asirra (Animal Species Image Recognition for Restricting Access) is a HIP (Human Interactive Proof) that works by asking users to identify photographs of cats and dogs. This task is difficult for computers, but our user studies have shown that people can accomplish it quickly and accurately. Many even think it's fun!

How secure is Asirra?

Philippe Golle from Palo Alto Research Center [13], described a classifier which is 82.7% accurate in telling apart the images of cats and dogs used in ASIRRA. This classifier allows us to solve a 12-image ASIRRA challenge with probability 10.3%. This success probability is significantly higher than the estimated for machine vision attacks. While low in absolute terms, it nevertheless poses a threat to ASIRRA if safeguards are not deployed to prevent machine adversaries from requesting, and attempting to solve, too many CAPTCHAs.

D. NuCaptcha

NuCaptcha [14] introduces video technology to text-based Captchas.

The NuCaptcha Security Platform is a CAPTCHA-based solution that uses motion video to authenticate human web interactions. Features of the NuCaptcha Security Platform are:

Displays in video format - Video technology has the dual benefit of making it more difficult for software to attack while simultaneously making it easier for humans to read.

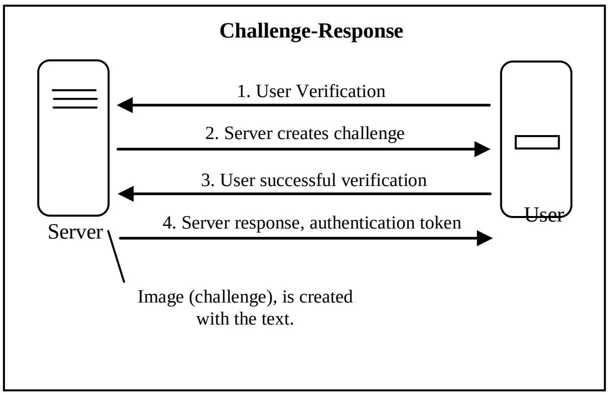
How secure is NuCaptcha?

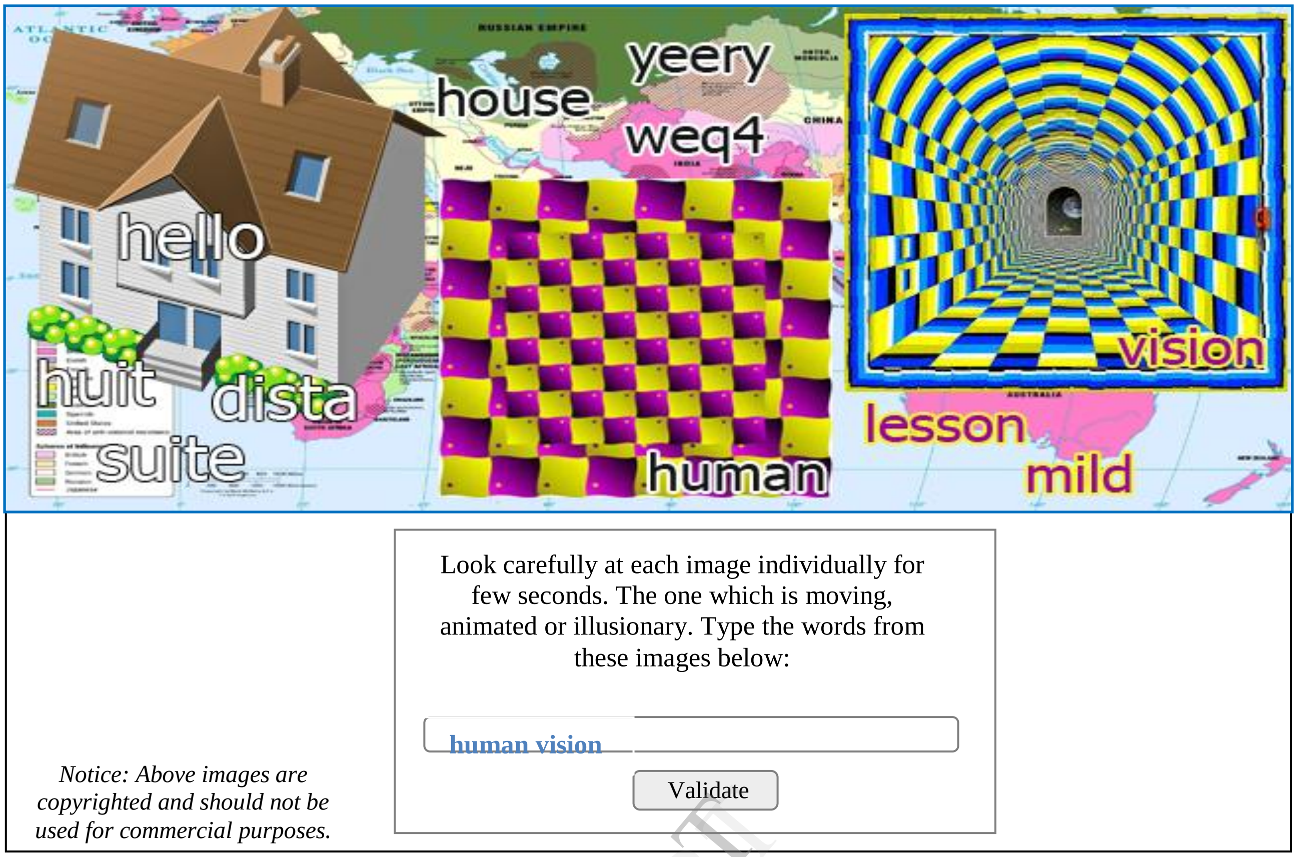
The research team from Stanford University, led by Elie Bursztein [15] created software that takes multiple snapshots of the NuCaptcha image over time which allowed for still image analysis. Once the software believed it had the full message in a frame, the resultant image was turned to black and white and the background removed to make deciphering the code easier. After that, character analysis software was used to break down the individual numbers and letters. Then, all that was left to do was knit them together as typewritten text and enter the whole string into the input box. Bursztein says the process is ninety percent accurate.

The focus of this paper is to use the above mentioned information to defend against the attacks using VIPITCHA.

III. VIPITCHA

VIPITCHA (Visually Perceived Images to Tell Computers and Humans Apart) is an approach based on reading the text and recognizing optical illusionary images. During user verification, the Server will generate an image (challenge) from the list of random images. The list contains optical illusion and normal images. The challenge is generated in a way that 3 optical illusionary images are included at minimum from the list. The total number of 6 or more random images can be used. After the successful creation of challenge (image), random text is added with some noise for distortion. The noise is added so that the AI or OCR softwares will not be able to extract the meaningful text or in other words launch the brute force attack.


Challenge-Response
1. User Verification
2. Server creates challenge
3. User successful verification
4. Server response, authentication token
Server
User
Image (challenge), is created with the text.



Look carefully at each image individually for few seconds. The one which is moving, animated or illusionary. Type the words from these images below:

human vision

Notice: Above images are copyrighted and should not be used for commercial purposes.

Fig. 2. VIPITCHA - Optical illusions with embedded text with 3 images

A. *Optical Illusions with Embedded Text*

We can see from the figure 2, it is clearly seen that it possible to use the human visual system perception and provide a very reliable protection against the bots and other various other types of attacks. There are three images which are being randomly selected from the list of images which are easily recognizable. The text below the images is entered for validation. It could be noticed that there is some extra text or noise added so to make it difficult for AI and OCR softwares.

GIF/Flash animation could also be used but they can be easily manipulated as Computer and Human see the same image. GIF or Flash will be similar to *NuCaptcha* motion video which is known to be breakable with 90% accuracy. In VIPITCHA, Computer sees the images which are different from humans eyes and brain; they 'see' something that doesn't quite match the physical measurement of the image. It will be difficult if not impossible to break VIPITCHA. It is to say that the biological makeup of human eye and brain coordination will be impossible to mimic by computers using available technologies of today.

However, VIPITCHA must be carefully created so that it becomes easy to recognize the illusionary images without putting much strain on human eyes. The success of it also depends on the proper implementation; care should be taken to overcome the brute force attack by adding sufficient noise. The illusionary images do put strain on eyes, if they are viewed for long period of time or are having very disturbing images.

IV. CONCLUSION AND FUTURE WORK

By using VIPITCHA it can be assured that automated attack by Bots can be prevented with much accuracy. Many other types of attacks as mentioned above can also be prevented, therefore preventing loss of money and time. However, future work needs to be done to provide more secure form of VIPITCHA that will be difficult to break. It is the start of new research topic which is required to be addressed by many Researchers, Academician and security professionals. It should be explored further by the help of neuroscience, understanding of human perception and human visual system. And in no other way to exploit it.

The Internet is used by billions of people worldwide, it should be noted that people with some form of visually impairment or deficiency need to be addressed, while maintaining symmetry of ease and security.

Users have to be made aware of the risks they face on internet, and they should responsibly use the internet for their benefit. Humans tend to do mistakes and those mistakes are exploited by malicious people. It is highly recommended that good antivirus/spyware/malware software be installed on user machines and are regularly updated. The operating system and other software security updates are very important too, they must be regularly updated. With due care of using internet user can reap the benefits of the internet technology. Users should properly verify their actions and should know the consequence of them. It is important to be aware of dangers of internet attacks and their devastating effects.

REFERENCES

[1] CAPTCHA – Wikipedia, Free Encyclopedia, http://en.wikipedia.org/wiki/CAPTCHA Accessed *March 12, 2014*

[2] Vicarious Solves CAPTCHA, http://news.vicarious.com/ *Published: November 13th 2013*

[3] Breaking a Visual CAPTCHA, UC Berkeley Vision Group, Simon Fraser University http://www2.cs.sfu.ca/~mori/research/gimpy/ *Accessed: 11 March 2014*

[4] Optical Illusion – Wikipedia, Free Encyclopedia, http://en.wikipedia.org/wiki/Optical_illusion *Accessed: March 10th 2014*

[5] Internet bot – Wikipedia, Free Encyclopedia, http://en.wikipedia.org/wiki/Internet_bot *Last Modified: March 2nd 2014*

[6] Bot Traffic Report 2013, by Igal Zeifman http://www.incapsula.com/blog/bot-traffic-report-2013.html

[7] Botnet steals 'millions of dollars from advertisers', http://www.bbc.com/news/technology-21860360 *Published: 20 March 2013*

[8] Bamital Botnet that hijacks online searches, http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx *Published: 6 February 2013 12:33: PM*

[9] CAPTCHA Drupal Group, https://drupal.org/project/captcha *Last Modified: 04 November 2013*

[10] ReCAPTCHA – Wikipedia, Free Encyclopedia, http://en.wikipedia.org/wiki/ReCAPTCHA *Accessed: 12 March 2014*

[11] Pattern Recognition. México. pp. 155–165. ISBN 978-3-642-31148-2. Archived from the original on 30 June 2012.

[12] Asirra - Microsoft Research Project, http://research.microsoft.com/en-us/um/redmond/ projects/asirra/ *Accessed: March 12, 2014*

[13] Machine Learning Attacks against the ASIRRA CAPTCHA, http://eprint.iacr.org/2008/126.pdf *Published: February 28, 2008*

[14] NuCaptcha: Video Technology to text based http://www.crunchbase.com/company/nucaptcha *Added: 18 December 2010*

[15] Stanford Research Team Cracks NuCaptcha http://phys.org/news/2012-02-stanford-team-animated-nucaptcha.html *Published: February, 2012*