COMPUTERS & SECURITY 70 (2017) 596–617

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A CAPTCHA model based on visual psychophysics: Using the brain to distinguish between human users and automated computer bots

Seyed Mohammad Reza Saadat Beheshti [a,*], *Panos Liatsis* [b], *Muttukrishnan Rajarajan* [a]

[a] *Department of Electrical and Electronic Engineering, City, University of London, EC1V 0HB, UK*

[b] *Department of Electrical and Computer Engineering, Khalifa University of Science and Technology, Petroleum Institute, PO Box 2533, Abu Dhabi, United Arab Emirates*

ARTICLE INFO

Article history:
Received 16 September 2016
Received in revised form 14 July 2017
Accepted 13 August 2017
Available online 24 August 2017

Keywords:
CAPTCHA
Persistence of vision
Trans-Saccadic memory
Visual integration
Authentication
Security

ABSTRACT

Demand for the use of online services such as free emails, social networks, and online polling is increasing at an exponential rate. Due to this, online service providers and retailers feel pressurised to satisfy the multitude of end-user expectations. Meanwhile, automated computer robots (known as "bots") are targeting online retailers and service providers by acting as human users and providing false information in order to abuse their service provisioning. CAPTCHA is a set of challenge/response protocol, which was introduced to protect online retailers and service providers from misuse and automated computer attacks. Text-based CAPTCHAs are the most popular form, and are used by most online service providers to differentiate between the human users and bots. However, the vast majority of text-based CAPTCHAs have been broken using the Optical Character Recognition (OCR) techniques and thus, reinforces the need for developing a secure and robust CAPTCHA model. Security and usability are the two fundamental issues that pose a trade-off in the design of a CAPTCHA; a hard CAPTCHA model could also be difficult for human users to resolve, which affects its usability, and vice versa. The model developed in this study uses the unsurpassed abilities of the Human Visual System (HVS) to superimpose and integrate complex information presented in individual frames, using the mechanism of *trans-saccadic memory*. In this context, the model integrates in its design the concept of *persistence of vision*, which enables humans to see the world in a continuous fashion. Preliminary results from the proposed model based on this technique are encouraging. To ensure the usability of the proposed CAPTCHA model, we set the threshold for the ORO parameter at 40%. This ensured that our CAPTCHA strings would be recognised by human observers at a rate of over 99% (or as close to 100% as is realistic). In turn, when examining the robustness of our VICAP model to computer programme attacks, we can observe that for the traditional case of OCR recognition, based on a single-frame scenario, the Computer Recognition Success Rate (CRSR) was about 0%, while in the case of a multi-frame scenario, the CRSR could increase to up to 50%.

* *Corresponding author.*
E-mail address: beheshti@city.ac.uk (S.M.R. Saadat Beheshti).

http://dx.doi.org/10.1016/j.cose.2017.08.006
0167-4048/

1. Introduction

Nowadays, most of us are familiar with online retailer webpages asking their users to retype a selection of distorted characters from an image before allowing them access to their online services. At times, this process may be frustrating and can require a considerable amount of time and effort to visually inspect and type out these blurry characters and numbers. These distorted images are an example of CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart). CAPTCHAs (von Ahn et al., 2004) were developed to protect websites and online service providers from possible cyber-attacks originating from automated computer programs (bots), and are the principal shield in protecting websites from being abused by bots and spams. The term "CAPTCHA" was first introduced by *Luis von Ahn* in the year 2000 at Carnegie Mellon University (CAPTCHA: Telling Humans and Computers Apart Automatically, 2000–2010a). This process has also been referred to as the *"Reverse Turing Test"* (Chellapilla et al., 2005). An example of one of the famous current CAPTCHA models, known as ReCAPTCHA is shown in Fig. 1.

As demand for online services rapidly grows, it is essential to have a mechanism that cannot only recognise the users as genuine, but at the same time can also ensure that users are real humans rather than automated computer programs (or "bots"). There is a direct correlation between growing numbers of online users, and a rapid rise in the number of cyber-attacks in recent years. Automated computer attacks abuse online service providers by supplying false information to systems and acting as human users (Crimeware: Bots, 2014). Human Interactive Proofs (HIPs) or CAPTCHAs are a set of challenge/response protocols designed in the form of a challenge or a test that can be presented to the users in order to distinguish human users from computer automated programs (Chewa and Baird, 2003). HIPs are designed to be easy for human users to solve, and should be very challenging (and ideally impossible) for automated computer programs to break.

CAPTCHAs are used for a variety of online applications such as free email accounts, e-commerce, online polling, chatrooms, and many other interactive online services (CAPTCHA: Telling Humans and Computers Apart Automatically, 2000–2010b). According to von Ahn et al. (2003), the idea behind a CAPTCHA is to use the sophisticated abilities of the human perceptual system in order to resolve a problem, which cannot be addressed by computer programs. Over the past decade, various CAPTCHA models were introduced and used widely by major online service providers such as Yahoo!, Google and Microsoft as well as social networks such as Facebook, in order to provide better security against automated computer attacks.

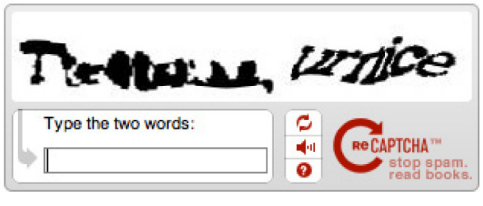

Fig. 1 – Example of one of the most popular current CAPTCHAs, known as ReCAPTCHA (Marc, 2011).

However, there has been extensive research on the security of CAPTCHAs as most CAPTCHA models have been broken using sophisticated recognition techniques. In this paper, a novel CAPTCHA model is introduced called Visual Integration CAPTCHA (VICAP), which makes use of the abilities of the human visual perception system to superimpose and integrate fleeting image frames of noisy partial information in order to create a final object, which can then be recognised by the brain. The proposed approach involves generating a sequence of image frames, which are obtained by sampling the binarized version of the original image, consisting of a string of characters, and adding in background noise to increase the security of the model. Next, the sequence of these images is played back at an appropriate frame rate so that the brain perceives it as a continuous animation, and thus, recognising the original object.

When consecutive frames are displayed at very high speeds, visual information can be integrated into the Visual Short-Term Memory (VSTM), which allows humans to perceive and complete the image of the original object. Each individual frame contains only a part of the original object pixels. Therefore, by analysing and processing a single frame, no useful information regarding the original object can be retrieved, thus rendering it unsuitable for OCR algorithms. The robustness of the proposed CAPTCHA model was tested using the state of the art CAPTCHA Breaker program. The final results demonstrate that the proposed CAPTCHA model is robust against various types of cyber security attacks.

Our main contributions to this research can be listed as follows:

- We have used the concept of visual psychophysics to design a novel CAPTCHA model, which would only be understandable for human users and not current computer recognition programmes.
- POV has been applied to the new CAPTCHA model to superimpose and integrate all the CAPTCHA images to form an object using the human brain.
- The Recognition Improvement Level (RIL) for human users has been seen to have a 50% increase in recognition success rates compared to current computer recognition programmes based on multi-frames scenarios.
- The new CAPTCHA's ability to be unrecognisable to current OCR programmes has increased by over 99% (close to 100%) based on single-frame scenarios and 50% based on multi-frame scenario compared to the current text-based CAPTCHA models.
- In terms of usability and performance, our proposed VICAP model has improved by 92% in terms of time to solve, and similarly 65% in terms of difficulty level. Furthermore, as the user satisfaction results confirm, we have achieved a 35% improvement in terms of clarity and ambiguity level of the CAPTCHA characters.

This paper is structured as follows: Section 1 will give a brief introduction regarding computer security and the importance of CAPTCHA in our daily online activities. Key background information on CAPTCHA, together with discussion of types of CAPTCHA categories, will then be discussed in Section 2. Sections 3 and 4 will present our proposed CAPTCHA model