A CAPTCHA BASED ON THE HUMAN VISUAL SYSTEMS MASKING CHARACTERISTICS

Rony Ferzli, Rida Bazzi**, and Lina J. Karam**

*Department of Electrical Engineering, Arizona State University, Tempe AZ 85287-5706
**Department of Computer Science & Engineering, Arizona State University, Tempe AZ 85287-8809
{rony.ferzli, bazzi, karam}@asu.edu

ABSTRACT

In this paper, a CAPTCHA is presented based on the masking characteristics of the Human Visual System (HVS). Knowing that noise can be masked by high activity regions and showing that edges can be masked by noise for a human observer while still being detected by machines, the suggested CAPTCHA is composed of English alphabets that are picked randomly and written with a combination of texture and edges with added noise such as to deceive the machine by randomly changing the visibility of characters for humans. The proposed CAPTCHA is highly legible and robust to brute-force attacks and sophisticated Object Character Recognition (OCR) segmentation algorithms.

1. INTRODUCTION

A CAPTCHA, as defined by the CAPTCHA Project [1], is "a test, any test, that can be automatically generated, which most humans can pass, but that current computer programs cannot pass". CAPTCHA stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart" and is inspired from Turing work. Turing [2] was the first researcher to investigate machine intelligence aiming to provide a method to assess whether or not a machine can think. In the original proposed Turing Test, a human interrogator was allowed to ask a series of questions to two players, one of which was a machine and the other a human. Both players pretended to be the human and the interrogator had to distinguish between the two based on their answers. In the CAPTCHA case, the interrogator is not a human but rather a machine.

A CAPTCHA can have various applications; it can be used to prevent "bots" from automatic sign up for free email service (i.e: Yahoo [www.yahoo.com]) or other services such as Paypal [www.paypal.com]. A CAPTCHA can also offer a solution to block worms and spam. It may be needed to block search engine robots from indexing a private website. It can also be used to prevent password dictionary attacks by denying the computer to scan through the entire word dictionary. Many other applications exist including chat rooms and popular webspace servers such as rapidshare [www.rapidshare.de].

Originally, research on CAPTCHAs was motivated by many incidents on the web. For example, in 1997, Altavista, the most popular search engine at that time, was receiving automated submission of a large number of Uniform Resource Locators (URL) in order to bias the website ranking. In 2000, Yahoo had a similar problem with machines joining online chat rooms and posting ads. Since then, many CAPTCHAs were suggested that can roughly be categorized into two groups; the first one contained CAPTCHAs that are legible but easy to break, while the second one included unbreakable CPATCHAs that are not always solvable by humans.

Knowing that noise can be masked by texture [3] and showing in this work that edges can be masked by noise for humans but can still be detected by computers, a resilient-to-attacks human-solvable CAPTCHA is proposed by exploiting the masking characteristics of the human visual system.

This paper is organized as follows. Section 2 presents an overview of available CAPTCHAs. The HVS masking properties are discussed in Section 3. The proposed perceptual-based CAPTCHA is presented in Section 4. Finally, a conclusion is given in Section 5.

2. CAPTCHA: AN OVERVIEW

This section presents an overview of published and patented CAPTCHAs that are based on text, image, or a combination of the two. Good CAPTCHAS should be generated such that they satisfy the following desirable properties [1]:

- The test must be generated automatically (i.e: the interrogator is a machine).
- The answer to the test should be quick and easy.
- The test should accept all human users.
- The test should reject all machine users.
- The test should resist attacks even if the algorithm is known.

Some of the existing popular CAPTCHAs include the following:

- *Altavista CAPTCHA [4]*: characters are generated randomly where the appearance is also randomized. For example, each character is rendered using selected fonts, different spacing between the characters, or different

stretching. The whole string can also follow a random path. Finally, a noisy or maze type background can be added as shown in Fig. 1(a). Though the number of machine attacks were reduced initially by 95%, algorithms were quickly developed to break this CAPTCHA due to isolated characters than can be segmented easily.

- *GIMPY [5]*: this CAPTCHA is the fruit of collaboration between Yahoo and Carnegie Mellon University (CMU) where the term "CAPTCHA" was first used. The developed algorithm picks English words at random and transforms them into an image after severe deformation and image occlusion with some overlapping. The user is challenged to read some number of words correctly (not necessarily all displayed words). An example is shown in Fig 1(b). It was found that users experienced difficulties with this type of CAPTCHA due to its complexity [6]; so, the algorithm was quickly replaced by EZ-Gimpy which uses only one English word, which was better tolerated by users (Fig. 1(c)). Yahoo used this CAPTCHA until it was broken by Mori et al. [7] in 2003. Fig 1(d) shows the current Yahoo CAPTCHA which is still unbreakable but could be sometimes hard to read as shown in Fig 1(d). No information is provided concerning the new CAPTCHA.

- *PessimalPrint [8]:* its lexicon contains only 70 common English word which are between 5 to 8 characters (Fig. 1(e)). The algorithm uses the Braid [9] degradation model simulating physical defects caused by copying and scanning of printed text. An example of degradation includes salt and pepper noise, condensed fonts and skewed characters. The algorithm is usually easy to beat since it uses a very small dictionary and is vulnerable to brute force attacks.

-*BaffleText [6]*: is a reading-based CAPTCHA that uses random masking to degrade images of non-English pronounceable character strings. The parameters controlling the mask include shape, radius, density of black pixels in the mask; the generated mask can be either added or subtracted. The generated CAPCHTA could be hard to read as shown in Fig 1(f) and could be broken using advanced Object Character Recognition (OCR) segmentation techniques along with morphological algorithms.

-*ScatterType [10]*: randomly synthesized images of text strings rendered in machine-print typefaces. Within the image, characters are fragmented using horizontal and vertical cuts, and the fragments are scattered by vertical and horizontal displacements. In contrast with the other described CATCHAs, no physics-based image degradations, occlusions, or extraneous patterns are performed. The algorithm seems hard to beat but the problem is that human legibility is only around 53%.

Other CAPTCHAs such as the ones based on images [1, 11] exist but are less popular since they require more complex answer from user; for example, four images are provided to the user and should guess the common object across the images. It is critical that human users not to find CAPTCHA excessively difficult or irritating.

3. HVS MASKING PROPERTIES

In this work, we are interested in exploiting the masking properties of the HVS. Masking is generally defined as any interference between two or more visual signals or stimuli that results in an increase or decrease of their visibility [3].

We are mainly interested in noise masking and edge masking properties. The first characteristic of the HVS is noise masking where regions of non-regular and highly changing luminance in an image (i.e: texture), are able to mask other signals (i.e: noise).

This phenomenon was measured and modeled in numerous experiments using sinusoidal patterns and noise stimuli. A set of psychophysical experiments were conducted in [3] on

(a) AltaVista

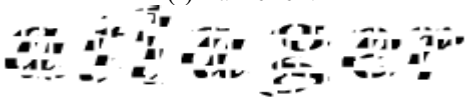
(b) GIMPY

(c) EZ-GIMPY

(d) New Yahoo CAPTCHA

(e) PessimalPrint

(f) BaffleText



(g) ScatterType

Figure 1. Different described CAPTCHA

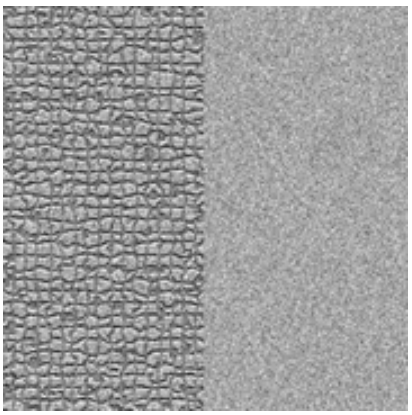


Figure 2. Noise perception when added to regions with different activities. The Gaussian noise has the same variance in both regions.

the visibility of different types of noise in natural images. The obtained results reveal that higher level of noise is detected on a plain background while, on the other hand, a clear masking effect was observed with high activity images. In particular, noise thresholds increased significantly with image activity. Winkler & Susstrunk [3] showed that observers seem to use only a small part of the image for making their decision. Fig. 2 shows an example where an image is split into textured and smooth regions. The same amount of gaussian noise is injected to the two regions; the noise is more visible in the region with constant gray scale level.

A second HVS masking property that we investigated as part of this work is edge masking. An experiment is conducted, as part of this work, showing that, when adding a certain amount of noise, the edges will not be continuous and will be hidden by noise to the human observer, but can still be "seen" by the machine.

Fig. 3 shows an example of a noisy edge image where a Gaussian noise with a variance equal to 0.235, was added to an image with a diagonal edge. Surprisingly enough, humans are not able to see the edge due to the added Gaussian noise. Can the machine vision defeat the human vision? Performing the Hough transform and displaying the longest detected line, the machine was able to spot the edge and its proper orientation. This idea can be investigated in a reverse Turing test where the interrogator will identify the machine and not the human. Note that similar results were obtained for uniform and salt & pepper noise.

As part of this work, subjective testing needs to be performed to calculate the noise variance required to mask edges at different orientations and contrast ratios. An initial subjective testing was conducted and can be summarized as follows:

1. Subjects were given a set of instructions before starting such as how to conduct the experiments, and what is the objective of the experiment.
2. Images similar to Fig.3 (a) were displayed. The subject needs to examine the image and identify the edge if possible. The first exposed image has the highest variance of 0.4 and is decreased by 0.04 each time a new image is displayed. Once the subject identifies the edge, the variance value is recorded.

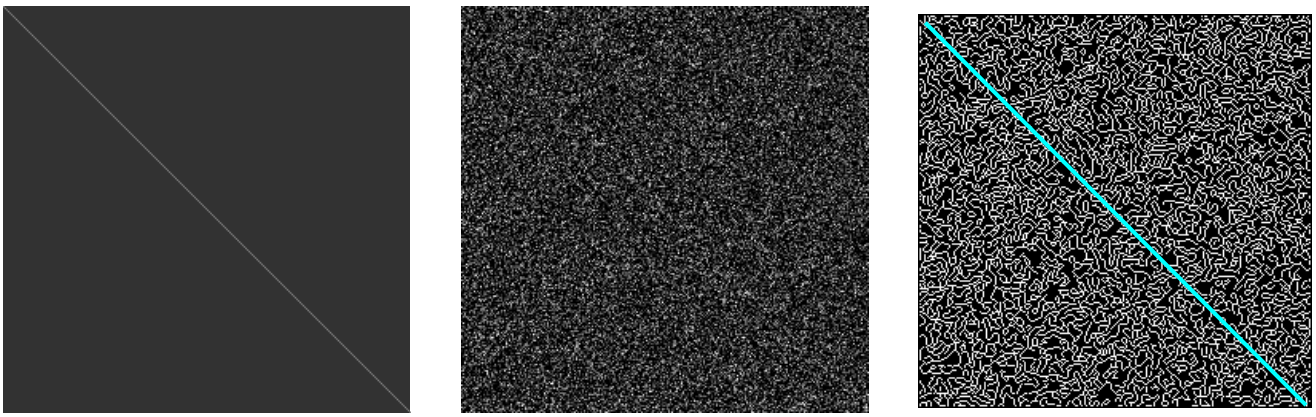
Six subjects, with normal to corrected-normal vision participated in the experiment. The collected edge masking information as well as the HVS-based texture masking effect will be used for the construction of the proposed CAPTCHA.

4. PROPOSED PERCEPTUAL-BASED CAPTCHA

In our proposed CAPTCHA generating scheme, visual perceptual-based CAPTCHAs are formed by exploiting the noise and texture masking properties of the HVS. The visual CAPTCHA is formed by adding noise and texture throughout the image in different amounts in order to control the masking so that letters (or patterns) can be made visible or invisible depending on the amount of masking. So, in some places, the noise is masked by texture while, in other places, the noise is itself masking edges. The machine can see the unseen and can detect both masked and unmasked edges and noise. This makes it harder for the machine to estimate the amount of injected noise and to predict what the human observer can see or not see.

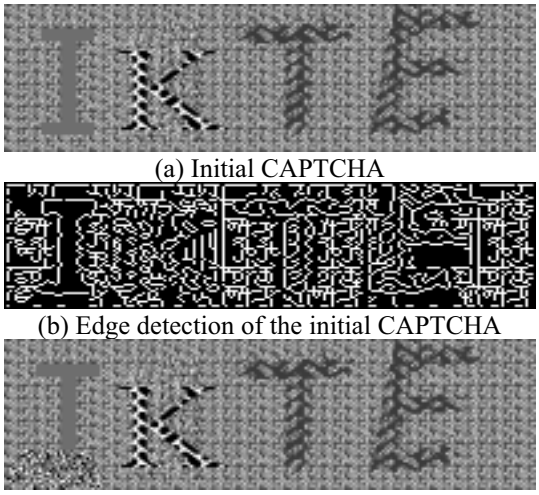
An example of the proposed CAPTCHA is shown in Fig. 4. Figs. 4(a) and (b) show the initial CAPTHA before adding the noise and the Canny edge detection output respectively. Fig. 4(c) shows the perceptual CAPTCHA that will be provided to users. The characteristics of this CPATCHA can be summarized as follows:

- The character 'I' is written using smooth edges and can be easily detected by a machine as shown in Fig. 4(b). Nevertheless, with the addition of noise throughout the images in different amounts it is hard for the machine to tell whether high activity regions are due to noise or texture and whether the letter is seen or not seen by the user (i.e: 'I' ot 'T').
- The character 'K' is written using a texture different from that of the background texture. Again, it is hard for the machine to tell which character is made out of texture.
- The characters 'T' and 'E' have a texture close to the background one and have a handwritten style.
- It is clear from Fig. 4(b) that the edge detector will fail for three out of the 4 characters. Being able to detect the character 'I' is desirable since, when adding noise, and due to the noise masking properties, the letter will be invisible to the user but detectable to the machine as discussed in Section 3; however, the machine will not be able to decide whether the character is seen since the high variance may be due to the texture or noise as shown in Fig. 4(c). In addition, to make it harder, the added noise can be structured (i.e., by using noise to write a character 'O' on top of 'I').



(a) Original image with diagonal edge (b) Human vision , edge image with gaussian noise (variance = 0.235) (c) Machine vision, line detection using Hough transform

Figure 3. Comparison of human and machine vision when Gaussian noise is added to an edge image.



(a) Initial CAPTCHA

(b) Edge detection of the initial CAPTCHA

(c) Final CAPTCHA with added noise

Figure 4. Proposed CAPTCHA

Though this is not sufficient by itself in proving the robustness of the proposed CAPTCHA to future attack algorithms, we can be assured that it will not be deciphered by current implemented segmentation or pattern recognition techniques and by current CAPTCHA detection techniques [12].

5. CONCLUSION

Taking advantage of the masking properties of the HVS, we propose a CAPCHTA based on characters that are formed using a mixture of textures and edges with added noise. Since the HVS reacts differently to the presence of noise in texture or edges, it will be hard to the machine to predict the perceived characters.

6. REFERENCES

[1] M. Blum, L. A. von Ahn, and J. Langford,, *The CAPTCHA Project*, "Completely Automatic Public Turing Test to Tell Computers and Humans Apart," www.captcha.net, *Dept. of Computer Science, Carnegie-Mellon Univ.*, November, 2000.

[2] A. Turing, "Computing Machinery and Intelligence," *Mind*, Vol. 59(236), pp. 433–460, 1950.

[3] S. Winkler, and S. Susstrunk, "Visibility of Noise in Natural Images", *Proc. IS&T/SPIE Electronic Imaging* 2004: Human Vision and Electronic Imaging IX, vol. 529, p. 121-129, 2004.

[4] M. D. Lillibridge, M. Abadi, K. Bharat, and A. Z. Broder, "Method for Selectively Restricting Access to Computer Systems," *U.S. Patent No. 6,195,698*, Feb. 2001.

[5] L. V. Ahn, M. Blum, and J. Langford, "Telling Humans and Computers Apart Automatically," *Commun. ACM*, 47(2):pp. 56-60, Feb 2004.

[6] M. Chew and H. S. Baird, "BaffleText: a Human Interactive Proof," *Proc., 10th SPIE/IS&T Document Recognition and Retrieval Conf.* , January 23–24, 2003.

[7] M. Greg and J. Malik, "Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA," *IEEE Computer Vision and Pattern Recognition*, vol. 1, pp. 134-331, 2003.

[8] A. L. Coates, H. S. Baird, and R. Fateman, "Pessimal Print: a Reverse Turing Test," *Proc., IAPR 6th Intl. Conf. on Document Analysis and Recognition,* Seattle, WA, September 10-13, pp. 1154-1158, 2001.

[9] H. S. Baird, "Document Image Defect Models," *in Structured Document Image Analysis*, pp. 546-556, Springer Verlag: New York, 1992.

[10] H. S. Baird and T. P. Riopka, "ScatterType: a Reading CAPTCHA Resistant to Segmentation Attack", *Proc. SPIE*, vol. 5676, no. 1, pp 197-201, Jan. 2005.

[11] M. Chew and J. D. Tygar., "Image Recognition CAPTCHAs", *7th Info. Security Conference*, vol. 3225 of *Lecture Notes in Coomp. Sc.*, Springer-Verlag, Oct. 2004.

[12] Online CAPTCHA test; www.pwntcha.net/test.html.