Investigating CAPTCHAs Based on Visual Phenomena

Anja B. Naumann[1], Thomas Franke[2], and Christian Bauckhage[3]

[1] Deutsche Telekom Laboratories, Ernst-Reuter-Platz 7, 10587 Berlin, Germany
[2] Cognitive and Engineering Psychology, Chemnitz University of Technology
[3] Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS
anja.naumann@telekom.de

Abstract. We propose and evaluate several novel types of CAPTCHAs (test to tell computers and humans apart) that exploit characteristics of the human visual system. Perceptions caused by the effect of lightness constancy or grouping phenomena due to transparent motion are hard to emulate on computers and may thus provide novel authentication mechanisms.

Keywords: CAPTCHA, visual phenomena, optical illusions.

1 Introduction: Visual Phenomena for CAPTCHA Design

Upon registration to a service, users often are faced with a little cognitive puzzle which is supposed to be difficult to solve algorithmically and thus is meant to prevent bots from misusing the service. However, the designer of such CAPTCHAs (*completely automated public turing test to tell computers and humans apart*) faces a trade-off decision. On the one hand, the principle behind the puzzle must be difficult enough in order to resist attacks through pattern recognition algorithms. On the other hand, it must be simple enough to allow for the automatic generation of many unambiguous instances which even naive users can solve quickly. Unfortunately, attempts of automatically breaking common types of simple cognitive challenges have become more successful recently. Straightforward countermeasures to these attacks, however, have led to CAPTCHAs of decreased usability for humans. This is especially evident for challenges that require the user to read a distorted text. In reaction to a growing number of reports on successfully using optical character recognition to break this challenge (see e.g. [1]), more recent types of CAPTCHAs therefore require the user to distinguish pictures [2] or to annotate a picture using a given list of terms [3]. However, mathematical combinatorics suggests that text-based CAPTCHAs can pose a more secure challenge [2]. Furthermore, people are used to solving these and will probably better understand and accept them [4].

In this paper, we investigate a novel approach to the design of reading-based cognitive challenges. Our idea is to exploit specific capabilities of the human visual system which are hard to emulate algorithmically and therefore will increase the difficulty for machines while they are supposed to be still easy to solve for humans. The visual phenomena we used are the following:

Lightness Constancy. In the physical world, the visual appearance of objects changes under varying illumination. Nevertheless, we are not constantly puzzled, our perceptual system subconsciously compensates for these variations. Part of this effect is known as the phenomenon of lightness constancy. Under certain conditions, however, the mechanisms providing constancy may also cause illusions. In this work, we draw on four illusions that are known to be persistent and thus may apply in the context of CAPTCHA design. Details on the cognitive mechanisms behind these effects can be found in [5]. Examples are shown in Fig. 1. In practice, any number of similar pictures can be produced (e.g. using circles or ellipses instead of squares, or varying sizes). Hence, for breaking the CAPTCHAs, looking for regularities in pictures is not sufficient.

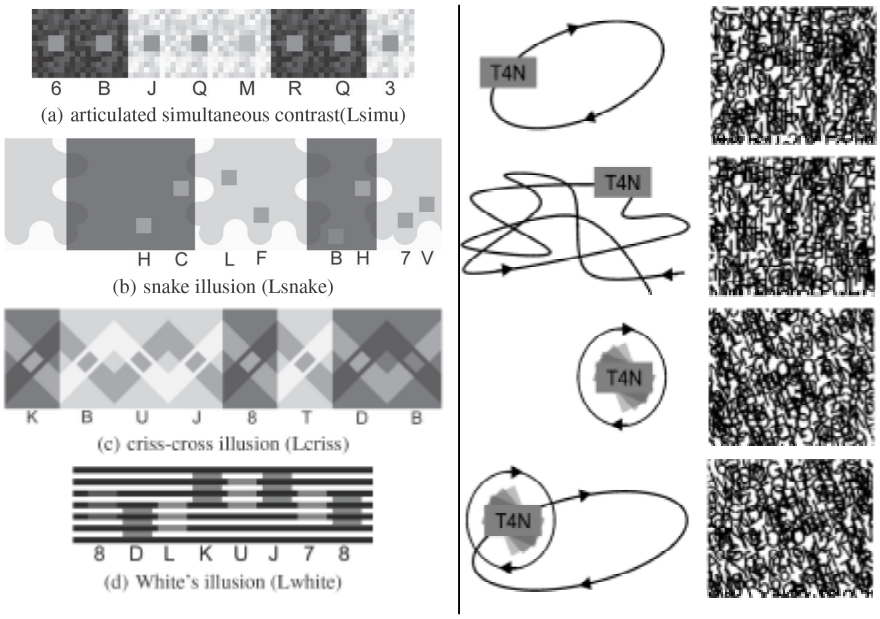

Fig. 1. Left: *Lightness illusions*. The small rectangles in 1(a) to 1(c) and the grey stripes in 1(d) are in fact all of the same brightness, even if it appears not to be the case. When asked to select the characters below the brighter rectangles, people thus select only a subset of characters.
Right: The four types of *transparent motion CAPTCHAs*. A text shown in front of a noisy background becomes legible if text and background are moving differently. From top to bottom the different motion patterns are: circular motion (*Mcircle*), random motion (*Mrand*), rotation (*Mrotate*), and circular motion plus rotation (*Mcirro*).

Motion-Defined Form. The second type of CAPTCHAs we introduce is based on the phenomenon of motion-defined form [6] which is based on perceptual grouping: since our visual system tends to group different entities that move together, sketches or letters superimposed over a noisy background of the same color become visible once they are moving. We experimented with a moving group of three characters superimposed over a moving picture of many cluttered characters (see Fig. 1.)

2 Experimental Evaluation

Evaluation Criteria. In order to assess the utility and usability of the CAPTCHAs illustrated in Fig. 1, we defined minimum requirements to be met: According to [1], humans should solve a CAPTCHA in more than 80% of the cases. Also, many interaction proofs have been reported to be solvable within 15 seconds [e.g. 2]. With respect to subjective difficulty, we demand that on a scale ranging from 1 (very easy) to 5 (impossible), a novel CAPTCHA should be at least rated to be manageable (score 3). For subjective usability, given a scale ranging from 1 (not at all problematic) to 5 (problematic), most users should assign scores lower than 3.

Setup and Procedure. A total of 28 subjects with normal vision (19-31 years; 17 female, 11 male) participated in our study. On average, they rated their computer- and Internet skills as moderate to moderately high (3.62 and 3.79 on a scale from 1 to 5). Most participants indicated that they had solved CAPTCHAs 10–50 times before, only 3 participants had solved less.

Our study was conducted in a laboratory setting. The CAPTCHAs were displayed using a web browser on a 19" CRT monitor (1024 x 768 pixels). All of them were positioned and accompanied by textual elements and entry boxes just as on a real website. They were normalized such that the entities that had to be identified (characters or rectangles) were of the same size across all experimental conditions.

When one of our lightness CAPTCHAs (see Fig. 1) was presented, the subjects were asked to only type the characters below a light or dark rectangle. The attribute light or dark was randomly changed from trial to trial. The challenges required to correctly enter 3 characters. In each image, there were 8 rectangles, 4 of which appeared in a brighter context and the remaining 4 appeared in a darker context. Also, in order to prevent simple automatic solutions, the brightness of one of the rectangles was slightly increased or decreased. For our motion CAPTCHAs (MPEG movies, 320 x 240 pixel), subjects were instructed to enter the characters that stood out through their motion. The challenges required to correctly enter 3 characters moving as a group over a differently moving cluttered background of randomly arranged characters. Speed of motion was 125 pixels per second for the *Mcircle* and *Mrand* variants. For *Mrotate*, the background was rotated at a speed of 60° per second while the foreground rotated with 160° per second. For the combined circular and rotating motion (*Mcirro*), the motion speeds were chosen as in the individual cases.

In each trial, the subjects entered what they believed was the correct answer. Their responses, i.e. response accuracies and response times were recorded. Then they were asked to subjectively rate the difficulty of the CAPTCHA. For each type of CAPTCHAs used for comparison and for each subtype of our proposed CAPTCHAs, a 10-item questionnaire was handed out to assess subjective usability. The questionnaire was referring to CATPCHA acceptance, i.e. it regarded work load, joy of use, and satisfaction, and was motivated by established questionnaires (SUS, NASA-TLX). All item scores were aggregated to one scale ranging from 1 (not at all problematic) to 5 (very problematic). Accordingly, the higher the score for a CAPTCHA the more problems in terms of acceptance by users are to be expected.

After a trial with a CAPTCHA that was not used further within the experiment (Gmail CAPTCHA), the experimenter made sure that the participants had understood

the experimental procedure. Finally, before beginning the experiments, our subjects went through a practice block for each of the considered CAPTCHAs. The following experimental trials consisted of two main blocks corresponding to the two types of considered CAPTCHAs and were presented in random order. The motion and lightness trials consisted of four sub-blocks that were presented in random order. A complete within-subjects design was used in the study.

Results and conclusion. In general, the results we obtained revealed a positive impression of the newly developed CAPTCHAs. For all of them, the response accuracy was at least 80%, except for the *Lcriss* variant (69%). The motion CAPTCHAs were generally solved reliably more accurately than 80%, however, for the lightness CAPTCHAs it was only the *Lwhite* variant (88%). Response times were significantly shorter than 15 seconds for all newly developed CAPTCHAs (5.2 to 12.4s; $t(28)=-46.74$ to -5.34, $p<.001$). In particular, the motion CAPTCHAs stand out for their remarkably short response times. What is more, all but one (*Mcirro*: 3.6 out of 5; $t(28)=4.56$, $p<.001$) of the CAPTCHAs satisfied the criterion of not being rated worse than manageable in terms of subjective difficulty. Finally, all but one (*Mcirro*: 3.8 out of 5; $t(28)=5.50$, $p<.001$) of our CAPTCHAs did satisfy the criterion of not being rated worse than partly problematic and therefore sufficient in terms of subjective usability. Hence, except for two variants, the proposed CAPTCHAs satisfy the criteria discussed above. The low response accuracy for *Lcriss* appears to be problematic and suggests that this variant should be further developed to meet the criteria. The difficulty of *Mcirro* to satisfy the subjective variables points to potential problems in terms of acceptability. In this paper, we could demonstrate that focusing on the strengths of human visual perception by utilizing perceptual phenomena and visual illusions provides a feasible and viable avenue to suitable and usable CAPTCHAs. Next step will be to attempt to attack our approach using sophisticated machine vision techniques. From our experience, our CAPTCHAs pose severe for standard vision approaches. Currently we are experimenting with rather involved machine learning methods in order to further evaluate the robustness of our approach.

References

1. Chellapilla, K., Simard, P.Y.: Using Machine Learning to Break Visual Human Interaction Proofs (HIPs). In: Proc. Advances in Neural Information Processing Systems, pp. 265-272 (2004)
2. Elson, J., Douceur, J., Saul, Asirra, J.: A CAPTCHA that Exploits Interest-aligned Manual Image Categorization. In Proc. ACM Conf. on Computer and Communications Security, pp. 366-374 (2007)
3. Datta, R., Li, J., Wang, J.: IMAGINATION: A Robust Image-based CAPTCHA Generation System. In: Proc. Int Conf. on Multimedia, pp. 331-334 (2005)
4. Kolupaev, A. and Ogijenko, J. CAPTCHAs: Humans vs. Bots. IEEE Security & Privacy, 6, 1, 68–70 (2008)
5. Hoffman, D.: Visual Intelligence. W.W. Norton, NY (1998)
6. Regan, D.: Detection and Discrimination of Motion-defined and Luminance-defined Two-dimensional Form. In: Proc. York Conf. on Spacial Vision in Humans and Robots (1991)