Can't You Tell I am a Human? A Comparison of Common Text and Image CAPTCHAs Using a Low-Fidelity Methodology

Hannah Marie Maurstad Eriksen
Oslo Metropolitan University, 0130
Oslo, Norway
h.mme@outlook.com

Lars Hoel
Oslo Metropolitan University, 0130
Oslo, Norway
larshoel@hotmail.com

Caroline Sofie Jetteberg
Oslo Metropolitan University, 0130
Oslo, Norway
caroline@jetteberg.no

Amalie Christine Leiknes
Oslo Metropolitan University, 0130
Oslo, Norway
amalie.leiknes@hotmail.com

Frode Eika Sandnes
Oslo Metropolitan University, 0130
Oslo, Norway
frodes@oslomet.no

ABSTRACT

Many websites employ CAPTCHAs to limit web robot traffic. Although CAPTCHA challenges may improve security they come at the cost of reduced usability and accessibility. This study set out to explore users' performance with two common types of CAPTCHAs that rely on image and text challenges. The results show that participants resolved image challenges faster than text challenges. Image challenges were also preferred over text challenges. Overall, each challenge took approximately 10 seconds to solve, and preferences scores were moderate. The error rates were high, but no significant difference was observed. We therefore argue for new methods capable of separating humans from robots that do not rely on user intervention.

CCS CONCEPTS

• **Human-centered computing**; • **Accessibility**; • **Accessibility technologies**;

KEYWORDS

CAPTCHA, Challenge, Security, Usability, Accessibility

ACM Reference Format:
Hannah Marie Maurstad Eriksen, Lars Hoel, Caroline Sofie Jetteberg, Amalie Christine Leiknes, and Frode Eika Sandnes. 2022. Can't You Tell I am a Human? A Comparison of Common Text and Image CAPTCHAs Using a Low-Fidelity Methodology. In *10th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion (DSAI 2022), August 31–September 02, 2022, Lisbon, Portugal.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3563137.3563179

1 INTRODUCTION

Many websites employ CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) challenges to prevent automated scripts, web-crawlers, and web robots' access to websites. The general principle behind a CAPTCHA is to provide users with challenges that are easy for humans to solve, while being hard for machines to unravel [43] using pattern matching and image and video processing techniques [21]. The term CAPTCHA is a playful variation on "Caught ya!". CAPTCHAs have become recognizable iconic symbols that signal to users what is expected similar to how the iconic nature of QR-codes communicates the availability of information through camera scanning [20].

According to Kaur et al. [24] the first CAPTCHA appeared in 1996 on the Alta-Vista web server just two years after the birth of the web. It was attributed to Moni Naor. Since then, numerous schemes and challenge types have been proposed, yet only a few of these are commonly used on popular websites. These include the text challenge that typically displays a distorted image of a word, which the user must recognize and enter in a text field. Image challenges comprise the other, where the user typically must select a subset of images in a grid which contains a certain object.

Such challenges attempt to counteract a common security problem, namely, the unintentional access to websites. Most of the research literature seems to focus on these security aspects. However, such challenges also affect usability and accessibility, usually in a negative manner. The problems associated with these challenges are even addressed by the World Wide Web Consortium (W3C) in the Web Content Accessibility Guidelines (WCAG2.1, section 1.1.1 non-text content). Although there are some studies that have addressed CAPTCHA usability and accessibility, they seem fewer in numbers, and much focus has been on audio challenges. In this study we wanted to explicitly compare the most used challenges and therefore focused on those relying on text and images. We distinguish between text challenges and image challenges, although strictly speaking the typical text challenges are in fact images of distorted text. However, much of the literature makes similar distinctions [18, 24, 40]. Hasan et al. [18] refer to such text CAPTCHAs as gimpy CAPTCHAs.

This paper is organized as follows: The next section presents related work, followed by a description of the methodology. Then, the results and discussion are presented. Finally the paper is closed by concluding remarks.

DSAI 2022, August 31–September 02, 2022, Lisbon, Portugal

ACM ISBN 978-1-4503-9807-7/22/08.
https://doi.org/10.1145/3563137.3563179

2 RELATED WORK

There has been a vast interest in CAPTCHAs since they first appeared in the late 90s [9, 18, 30]. A range of different types of challenges have been proposed including those based on text, images (pix CAPTCHAs), audio, video, and puzzles [40], or more specific challenges such as baffle texts [18] and Bongo challenges [24].

The research into CAPTCHAs can be divided into three areas, namely proposals of new tests [8, 12], revealing test security weaknesses [7, 26, 46] and tests from the users' perspectives. Examples of novel CAPTCHA proposals include challenges involving determining the orientation of images [17] and improved video-based tests [29]. Researchers have demonstrated weakness of common challenges such as simple visual CAPTCHAs [16, 28, 44], the reCAPTCHA [5] and the use of deep learning to break challenges [41]. The proposal of new tests and strategies for breaking these bear similarities to an arms race [45].

Studies addressing the user perspectives of CAPTCHAs have primarily addressed usability or accessibility issues. Nonvisual and audio challenges have been proposed as an alternative to the common visually intensive tests that are not accessible for low-vision users [1, 39]. Non-visual alternatives will render such web-sites unusable to such cohorts of users. Although several audio schemes exist, Kuzma et al. [25] found that out of 150 online forums, very few provided accessible alternative challenges. Also, audio CAPTCHAs have been criticized for being hard to use [31, 39]. Several improvements have therefore been proposed such as combining visual and audio cues [2, 31] and personalized tests based on accessibility information available at social media sites [22]. In addition to challenges resulting from low vision [10, 33, 38], there are users with reduced cognitive function [36] or reduced reading skills [11]. There is still little work on the use of other modalities such as touch [27] for CAPTCHAs.

CAPTCHAs are not only difficult to use for individuals with reduced functioning. Fidas et al. [13] conducted a survey involving 210 participants. Their results confirmed that such tests were perceived as being difficult. They proposed that language could pose a particular challenge and that native language CAPTCHAs should be used when this could be determined from the browser. Bamday and Shah [4] explicitly addressed English versus local languages on Indian website CAPTCHAs. Gafni and Nagar [14, 15] conducted a questionnaire study of users' perceptions of challenges involving 212 participants. In their study they compared five challenge types. Their results showed that the participants were most familiar with text challenges but also disliked these. Image and quiz challenges were perceived as the most fun. About half of the participants were unable to complete tests based on arithmetic tasks. Gafni and Nagar also found age to be a factor where young participants were more tolerant to the challenges, faster and more accurate, while older participants generally found the tests annoying. Bursztein et al. [6] conducted a large-scale study of 13 image and audio challenge categories and 318,000 different challenges using Amazon Mechanical Turk workers. They found that only 1% of the participants chose audio challenges. They also found many non-native English speakers were slower when using English-language challenges. Older participants were slower, yet more accurate than younger participants. PhD holders were found to be the most accurate in solving audio challenges. The authors used agreement rate for their assessments and found that different challenge types varied in agreement rate. For image challenges the agreement rate was 71%, while for audio challenges the agreement rate was 31%.

3 METHOD

3.1 Experimental design

A within-group experimental design was chosen with CAPTCHA type as independent variable and response time, error rate, and preference as dependent variables. The independent variable had two levels, namely image and text.

3.2 Participants

A total of 24 participants were recruited for the experiment of which 10 were female and 14 were male. The age of the participant ranged from 20 to 30 years. All the participants were physically recruited among the students at Oslo Metropolitan University campus. All indicated that they were familiar with Google reCAPTCHA. The experiment was conducted during the COVID-19 pandemic which limited data collection. All the participants had undergone a minimum of infection prevention training.

3.3 Equipment

A low-fidelity approach [35] was adopted to simulate the real CAPTCHA experience while ensuring replicability. Actual CAPTCHAs would have presented random challenges which would make it more difficult to fairly compare the results of different participants. Participants entered text CAPTCHAs using Microsoft Word, while the image CAPTCHAs were realized using the drawing function in Word. All the experiments were conducted using a Mac laptop computer with an external mouse. A smartphone stopwatch was used for measuring response times. Infection prevention was ensured by providing participants disposable gloves and anti-bac.

3.4 Materials

Two types of image CAPTCHAs were used. One of the image types showed a grid of six images and the users were asked to indicate which image contained a particular object such as chairs. An example of the second image type showed images of a road split into 20 boxes and the users were asked to select all boxes with cars. The text CAPTCHAs contained various graphical representations of text. Unfortunately, we do not have the permissions to reproduce the images used. In total 20 challenges were prepared, of which 10 were images challenges and 10 text challenges.

3.5 Procedure

Each participant was presented with each of the 10 text challenges and 10 image challenges. To respond to the text challenges the participant wrote the word they could see. Participants were asked to respond to the image challenges by marking each valid box. The presentation order for the set of text challenges and image challenges were randomized. Participants were asked to proceed at a comfortable tempo. After the experiments, the participants were

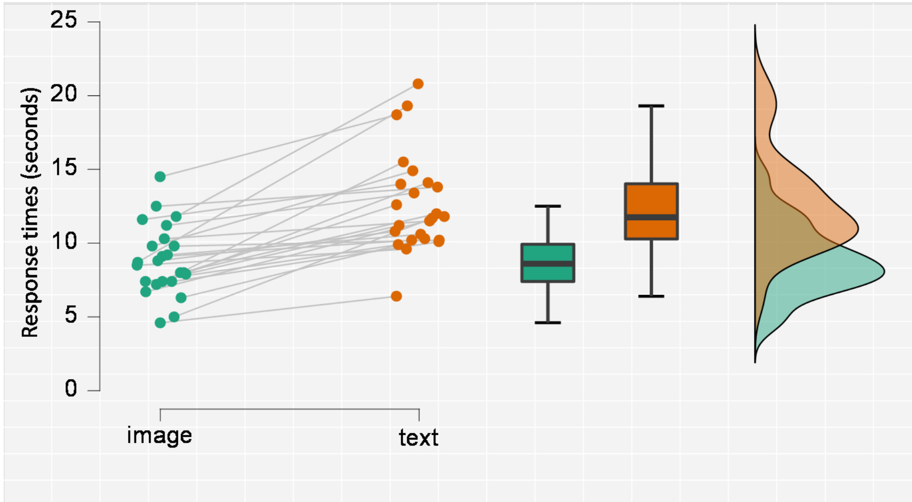

Figure 1: Raincloud plot showing the distribution of response times (seconds) for image and text challenges.

asked to respond to two simple 5-item Likert questions regarding their preferences for text and image challenges, respectively.

The experiments were conducted in a secluded meeting room on campus with two of the authors present to administer the experiment. Participants were invited on an individual basis. Each session lasted between 5-7 minutes including briefing.

The experiment was conducted during a single session. There was therefore no need to link participants across sessions [34] and the experiment could therefore be conducted anonymously.

3.6 Analysis

The mean response time for each CAPTCHA type was computed for each participant. Shapiro Wilk tests revealed that the response times deviated from normal distribution and were therefore analyzed using a Wilcoxon signed rank test. The error rate distribution did not deviate from normal distribution and observations were therefore analyzed using a paired t-test. The Likert responses are ordinal and were therefore analyzed using a non-parametric Wilcoxon signed-rank test. The statistical tests were conducted using JASP version 0.16.0.0 [23].

4 RESULTS

The time to respond to image challenges (M = 8.8, SD = 2.4) was shorter than the time to respond to text challenges (M = 12.6, SD = 3.4) and the difference was significantly different (W = 0.0, p < .001). The response times are plotted in Figure 1.

The error rate associated with image challenges (M = 17.9%, SD = 11.8%) was somewhat lower than the error rate for text challenges (M = 21.2%, SD = 16.0%), but this difference was not statistically significant ($t(23)$ = 0.915, p = .370). The error rates are plotted in Figure 2.

The preference score for image challenges (M = 3.8, SD = 0.8) was higher than the preference scores for text challenges (M = 2.9, SD = 1.3) and the difference was significantly different (W = 141.0, p = .015). The preference scores are plotted in Figure 3.

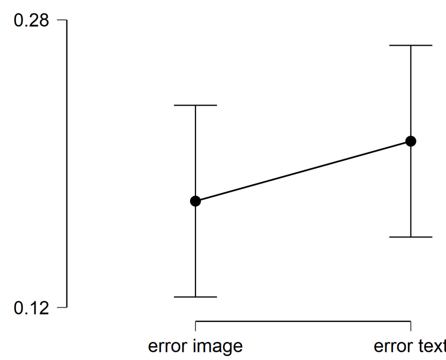

Figure 2: Mean error rates (range between 0 and 1). Error bars show 95% confidence intervals.

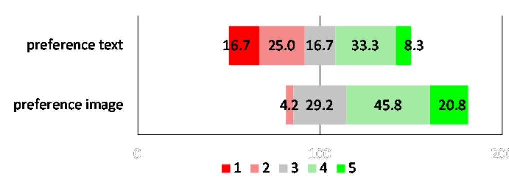

Figure 3: Diverging stacked bar graph showing the percentage distribution of preferences (Likert scale from 1 to 5).

5 DISCUSSION

The mean response-time difference between the two challenge types was relatively large as text challenges took nearly 50% longer than image challenges. One reason why the participants performed tasks faster and preferred image challenges over text challenges may be that making direct selections [42] by clicking on an image is a simpler task than the text-copy task which requires both effort, concentration, and skill [3, 32, 37]. Observations of response times and preferences agree with the results of Bursztein et al. [6] who also ranked image challenges higher than text challenges. The absolute duration needed to resolve challenges, that is, around 10 seconds, was perceivable to users. The question is whether the donation of 10 seconds to help the website solve its problems is tolerable, as CAPTCHAs do not benefit users directly.

Although the participants preferred image challenges, it must be noted that the mean response to text challenges were close to neutral. Moreover, the mean preference score for images was closer to neutral than top score, suggesting that participants were not fully satisfied with either of the methods. Although there was no significant difference in error rates between the two challenge types it is evident that the error rate is high (around 20%). Clearly, interactions that are resulting in an error with every fifth trial is likely to cause frustration and dissatisfaction with users.

The challenge types explored herein were chosen due to their perceived prevalence on commonly used websites. We do not know the reason why these types of challenges are common. Although one reason could be that these represent the most successful challenges, more likely it is related to the technology market where promoted technology also gains market share. Given the high error rates and moderate preference scores one may question the CAPTCHA paradigm altogether. Why should users be burdened with resolving issues that should be solved technically out of the users' sight? In general, one should strive to simplify online forms and reduce input errors [19].

5.1 Limitations

One weakness of this study was the small sample size comprising just 24 participants from a limited cohort of computer literate students. Thus, our sample size makes up only a tenth of similar studies (see for example [13, 14]).

Factors that may have affected the results is that the participants may have felt being watched by the experimenters during the session, thereby somewhat inhibiting their performance. Moreover, a Mac keyboard was used. Although it has the conventional Qwerty layout it may have been experienced as somewhat unfamiliar to participants that regularly use Windows keyboards. However, this is considered a negligible source of bias.

6 CONCLUSIONS

A comparison of the common CAPTCHA mechanism widely used on websites was conducted. The results show that participants both performed the challenges faster and preferred image CAPTCHAs over text CAPTHAs. However, the image challenges are not accessible to individuals without vision. In general, such challenges were commonly viewed as a nuisance and website designers should look for other mechanisms than CAPTCHAs to separate genuine human visitors from web robots. Preferably, users should not be burdened by such mechanisms thereby preventing compromising usability and accessibility for security.

REFERENCES

[1] K. Aiswarya and K. S. Kuppusamy. 2015. A study of audio captcha and their limitations. International Journal of Science and Research 4 (2015), 918-923.
[2] Mrim Alnfiai. 2020. Evaluating the accessibility and usability of a universal CAPTCHA based on gestures for smartphones. Universal Access in the Information Society 20 (2020), 817–831. DOI: https://doi.org/10.1007/s10209-020-00730-x
[3] Thomas Bekken Aschim, Julie Lidahl Gjerstad, Lars Vidar Lien, Rukaiya Tahsin, and Frode Eika Sandnes. 2019. Are split tablet keyboards better? A study of soft keyboard layout and hand posture. In: Proceedings of the IFIP Conference on Human-Computer Interaction. Springer, Cham, 647-655. DOI: https://doi.org/10.1007/978-3-030-29387-1_37
[4] M. Tariq Banday and Nisar A. Shah. 2011. Challenges of CAPTCHA in the accessibility of Indian regional websites. In Proceedings of the Fourth Annual ACM Bangalore Conference (COMPUTE '11). Association for Computing Machinery, New York, NY, USA, Article 31, 1–4. https://doi.org/10.1145/1980422.1980453
[5] Samuel S. Brown, Nicholas DiBari, and Sajal Bhatia. 2017. I Am 'Totally' Human: Bypassing the reCaptcha. In: Proceedings of the 13th International Conference on Signal-Image Technology & Internet-Based Systems. IEEE, 9-12.). DOI: https://doi.org/10.1109/SITIS.2017.13
[6] Elie Bursztein, Steven Bethard, Celine Fabry, John C. Mitchell, and Dan Jurafsky. 2010. How good are humans at solving CAPTCHAs? A large scale evaluation. In: Proceedings of the IEEE symposium on security and privacy. IEEE, 399-413. DOI: https://doi.org/10.1109/SP.2010.31
[7] Elie Bursztein, Matthieu Martin, and John Mitchell. 2011. Text-based CAPTCHA strengths and weaknesses. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). Association for Computing Machinery, New York, NY, USA, 125–138. https://doi.org/10.1145/2046707.2046724
[8] Ritendra Datta, Jia Li, and James Z. Wang. 2005. IMAGINATION: a robust image-based CAPTCHA generation system. In Proceedings of the 13th annual ACM international conference on Multimedia (MULTIMEDIA '05). Association for Computing Machinery, New York, NY, USA, 331–334. https://doi.org/10.1145/1101149.1101218
[9] N. Divyashree, and S. T. Kumar. 2016. A survey on CAPTCHA categories. Int. J. Eng. Comput. Sc. 5(2016), 16458-16462.
[10] Aline Darc Piculo dos Santos, Fausto Orsi Medola, Milton José Cinelli, Alejandro Rafael Garcia Ramirez, and Frode Eika Sandnes. 2021. Are electronic white canes better than traditional canes? A comparative study with blind and blindfolded participants. Universal Access in the Information Society 20 (2021), 93–103. DOI: https://doi.org/10.1007/s10209-020-00712-z
[11] Evelyn Eika and Frode Eika Sandnes. 2016. Assessing the Reading Level of Web Texts for WCAG2. 0 Compliance—Can It Be Done Automatically? In: Advances in Design for Inclusion. Springer, Cham, 361-371. DOI: https://doi.org/10.1007/978-3-319-41962-6_32
[12] Ahmad Salah El Ahmad, Jeff Yan, and Lindsay Marshall. 2010. The robustness of a new CAPTCHA. In Proceedings of the Third European Workshop on System Security (EUROSEC '10). Association for Computing Machinery, New York, NY, USA, 36–41. https://doi.org/10.1145/1752046.1752052
[13] Christos A. Fidas, Artemios G. Voyiatzis, and Nikolaos M. Avouris. 2011. On the necessity of user-friendly CAPTCHA. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11). Association for Computing Machinery, New York, NY, USA, 2623–2626. https://doi.org/10.1145/1978942.1979325
[14] Ruti Gafni and Idan Nagar. 2016. CAPTCHA–Security affecting user experience. Issues in Informing Science and Information Technology 13 (2016), 063-077.
[15] Ruti Gafni and Idan Nagar. 2016. CAPTCHA Impact on user experience of users with learning disabilities. Interdisciplinary Journal of e-Skills and Lifelong Learning 12 (2016), 207-223.
[16] Philippe Golle. 2008. Machine learning attacks against the Asirra CAPTCHA. In Proceedings of the 15th ACM conference on Computer and communications security (CCS '08). Association for Computing Machinery, New York, NY, USA, 535–542. https://doi.org/10.1145/1455770.1455838
[17] Rich Gossweiler, Maryam Kamvar, and Shumeet Baluja. 2009. What's up CAPTCHA? a CAPTCHA based on image orientation. In Proceedings of the 18th international conference on World wide web (WWW '09). Association for Computing Machinery, New York, NY, USA, 841–850. https://doi.org/10.1145/1526709.1526822
[18] Walid Khalifa Abdulla Hasan. 2016. A survey of current research on captcha. Int. J. Comput. Sci. Eng. Surv. 7 (2016), 141-157.
[19] Knut Åge Hofseth, Lars Kristian Haga, Vegard Sørlie, and Frode Eika Sandnes. 2019. Form feedback on the web: a comparison of popup alerts and in-form error messages. In: Innovation in Medicine and Healthcare Systems, and Multimedia, Springer, Singapore, 369-379. DOI: https://doi.org/10.1007/978-981-13-8566-7_35
[20] Yo-Ping Huang„ Yueh-Tsun Chang, and Frode Eika Sandnes. 2010. Ubiquitous information transfer across different platforms by QR codes. Journal of Mobile Multimedia 6 (2010), 003-014.
[21] Yo-Ping Huang, Liang-Wei Hsu, and Frode-Eika Sandnes. 2007. An intelligent subtitle detection model for locating television commercials. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 37 (2007), 485-492. DOI: https://doi.org/10.1109/TSMCB.2006.883428t
[22] Hassan Ishfaq, Waseem Iqbal, and Waleed Bin Shahid. 2015. Attaining accessibility and personalization with Socio-Captcha (SCAP). In: Proceedings of the 12th International Bhurban Conference on Applied Sciences and Technology. IEEE, 307-311. DOI: https://doi.org/10.1109/IBCAST.2015.7058521
[23] JASP Team (2020). JASP (Version 0.14.1)[Computer software].

[24] Kiranjot Kaur and Sunny Behal. 2014. Captcha and its techniques: a review. International Journal of Computer Science and Information Technologies 5 (2014), 6341-6344.

[25] Joanne Kuzma, Sue Barnes, and Klaus Oestreicher. 2011. CAPTCHA accessibility study of online forums. International Journal of Web Based Communities 7 (2011), 312-323.

[26] Shujun Li, S. Amier Haider Shah, M. Asad Usman Khan, Syed Ali Khayam, Ahmad-Reza Sadeghi, and Roland Schmitz. 2010. Breaking e-banking CAPTCHAs. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10). Association for Computing Machinery, New York, NY, USA, 171–180. https://doi.org/10.1145/1920261.1920288

[27] Ming-Wei Lin, Yun-Maw Cheng, Wai Yu, and Frode Eika Sandnes. 2008. Investigation into the feasibility of using tactons to provide navigation cues in pedestrian situations. In Proceedings of the 20th Australasian Conference on Computer-Human Interaction: Designing for Habitus and Habitat (OZCHI '08). Association for Computing Machinery, New York, NY, USA, 299–302. https://doi.org/10.1145/1517744.1517794

[28] G. Mori and J. Malik. 2003. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. In: Proceedings of 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. IEEE. https://doi.org/10.1109/CVPR.2003.1211347

[29] M. Kameswara Rao, M. S. V. K. Maniraj, and B. Sneha Ganga. 2014. Improved video captcha. Journal of Emerging Technologies in Web Intelligence 6 (2014), 416-416.

[30] Mira K. Sadar, Pritish A. Tijare, and Swapnil N. Sawalkar. 2015. Review on Captcha: Graphical Password for Security. International Journal of Research in Advent Technology 3 (2015), 80-84.

[31] Graig Sauer, Harry Hochheiser, Jinjuan Feng, and Jonathan Lazar. 2008. Towards a universally usable CAPTCHA. In: Proceedings of the 4th Symposium on Usable Privacy and Security.

[32] Frode Eika Sandnes. 2005. Evaluating mobile text entry strategies with finite state automata. In Proceedings of the 7th international conference on Human computer interaction with mobile devices & services (MobileHCI '05). Association for Computing Machinery, New York, NY, USA, 115–121. https://doi.org/10.1145/1085777.1085797

[33] Frode Eika Sandnes. 2016. What do low-vision users really want from smart glasses? Faces, text and perhaps no glasses at all. In: International Conference on Computers Helping People with Special Needs. Springer, Cham, 187-194. DOI: https://doi.org/10.1007/978-3-319-41264-1_25

[34] Frode Eika Sandnes. 2021. HIDE: Short IDs for Robust and Anonymous Linking of Users Across Multiple Sessions in Small HCI Experiments. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21). Association for Computing Machinery, New York, NY, USA, Article 326, 1–6. https://doi.org/10.1145/3411763.3451794

[35] Frode Eika Sandnes and Evelyn Eika. 2017. Head-mounted augmented reality displays on the cheap: a DIY approach to sketching and prototyping low-vision assistive technologies. In: International Conference on Universal Access in Human-Computer Interaction. Springer, Cham, 167-186. DOI: https://doi.org/10.1007/978-3-319-58703-5_13

[36] Frode Eika Sandnes and Maud Veronica Lundh. 2015. Calendars for Individuals with Cognitive Disabilities: A Comparison of Table View and List View. In Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility (ASSETS '15). Association for Computing Machinery, New York, NY, USA, 329–330. https://doi.org/10.1145/2700648.2811363

[37] Frode Eika Sandnes, Haavard W. Thorkildssen, Alexander Arvei, Johannes O. Buverud. 2004. Techniques for fast and easy mobile text-entry with three-keys. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences. IEEE. DOI: https://doi.org/10.1109/HICSS.2004.1265675

[38] Frode Eika Sandnes and Anqi Zhao. 2015. An interactive color picker that ensures WCAG2. 0 compliant color contrast levels. Procedia Computer Science 67 (2015), 87-94. DOI: https://doi.org/10.1016/j.procs.2015.09.252

[39] Sajad Shirali-Shahreza and M. Hassan Shirali-Shahreza. 2011. Accessibility of CAPTCHA methods. In Proceedings of the 4th ACM workshop on Security and artificial intelligence (AISec '11). Association for Computing Machinery, New York, NY, USA, 109–110. https://doi.org/10.1145/2046684.2046704

[40] Ved Prakash Singh and Preet Pal. 2014. Survey of different types of CAPTCHA. International Journal of Computer Science and Information Technologies 5 (2014), 2242-2245.

[41] Suphannee Sivakorn, Iasonas Polakis, and Angelos D. Keromytis. 2016. I am robot:(deep) learning to break semantic image captchas. In: Proceedings of the 2016 IEEE European Symposium on Security and Privacy. IEEE, 388-403. DOI: https://doi.org/10.1109/EuroSP.2016.37

[42] Nils Andreas Baumgarten Skogstrøm, Anne Igeltjørn, Kjetil Madsen Knudsen, Aissatou Dendembo Diallo, Daria Krivonos, and Frode Eika Sandnes. 2018. A comparison of two smartphone time-picking interfaces: convention versus efficiency. In Proceedings of the 10th Nordic Conference on Human-Computer Interaction (NordiCHI '18). Association for Computing Machinery, New York, NY, USA, 874–879. https://doi.org/10.1145/3240167.3240233

[43] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford. 2003. CAPTCHA: Using hard AI problems for security. In: International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 294-311. DOI: https://doi.org/10.1007/3-540-39200-9_18

[44] Xing Wu, Shuji Dai, Yike Guo, and Hamido Fujita. 2019. A machine learning attack against variable-length Chinese character CAPTCHAs. Applied Intelligence 49 (2019), 1548-1565. DOI: https://doi.org/10.1007/s10489-018-1342-8

[45] Jeff Yan and Ahmad Salah El Ahmad. 2008. A low-cost attack on a Microsoft captcha. In Proceedings of the 15th ACM conference on Computer and communications security (CCS '08). Association for Computing Machinery, New York, NY, USA, 543–554. https://doi.org/10.1145/1455770.1455839

[46] Yang Zhang, Haichang Gao, Ge Pei, Sainan Luo, Guoqin Chang, Nuo Cheng. 2019. A survey of research on captcha designing and breaking techniques. In: Proceedings of the 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering. IEEE, 75-84. DOI: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00020