Rodney Beede
CSCI5722 Computer Vision
Fall 2010 – Project Description

This project will address the issue in computer security of the SPAM prevention technique known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). CAPTCHA attempts to address the problem of unwanted messages or SPAM in e-mails, blogs, and online forum web sites by providing a visual challenge question that only a human could decipher instead of a computer. Many spammers use automated systems known as bots to send millions of solicitations a month so CAPTCHA was devised as a way of reducing these unwanted messages.

A CAPTCHA works by requiring the user to type in some combination of letters, numbers, or words that are displayed in an image. This image, however, is distorted via bending, curving, random lines, and random noise in the background so that regular OCR computer algorithms would be unable to successfully parse them whereas a human could.

This project will analyze the current effectiveness of these systems as a security measure in distinguishing a computer from a human as well as how spammers have adapted automated methods with computer vision algorithms to defeat this measure. The expected contribution isn't to recommend one CAPTCHA system over another but to provide information on whether the trouble of implementing a CAPTCHA is worth it based on the advancements in computer vision algorithms to render them ineffective.

A collection of real-world CAPTCHA images will be collected from various sites and categorized by the CAPTCHA implementations they use. Each image will be processed by optical character recognition algorithms and software[i] to judge the effectiveness of the image obscurity. All the images will then be analyzed by vision algorithms designed to defeat the CAPTCHA protection. Some of the current state of the art software and algorithms for both implementing CAPTCHA and defeating CAPTCHA are described below.

reCAPTCHA [ii] is a technique where the words come from old transcripts, books, and other printed materials that are desirable to be transcribed into electronic form. Since OCR techniques have more difficulty reading these older texts manual transcription by humans is necessary. To capitalize on humans transcribing words to solve the CAPTCHA challenge reCAPTCHA presents users with images from those texts to transcribe thus not only providing a useful validation of a human versus a machine but also assisting in the transcribing process. If OCR cannot recognize the words then how is the human's answer validated? This is accomplished by presenting two words: one with a known answer (the control word) and one without a known answer (the word to be transcribed from text). If the control word is answered correctly it is assumed a human entered it and thus also provided the unknown word as well.

Multiple humans may get the same unknown word with each one's answer being compared to the others for accuracy.

Machine learning to break HIPs [iii]: This technique relies on segmentation of the individual characters and then using machine learning to distinguish the individual characters.

EZ-Gimpy[iv] is the CAPTCHA used by Yahoo. A technique for breaking it was demonstrated by Mori which used shape context matching in order to decipher the words.

Strong CAPTCHA Guidelines[v] provides a very good overview of CAPTCHA implementation considerations as well as some example source code that was used to demonstrate a 17.5% success rate in defeating reCaptcha using simple OCR techniques and segmentation.

anti-recaptcha v0.1[vi] by Benjamin Wegener is a php program that is designed to defeat reCaptcha. In his paper[vii] he describes the basic techniques he used to clean up the images so they could be read by OCR software. This is the newest technique that was published in Oct 2010 and has yet to be addressed with any prevention techniques.

[i] http://www.goodocr.com/

[ii] reCAPTCHA: Human-Based Character Recognition via Web Security Measures
Luis von Ahn, Benjamin Maurer, Colin McMillen, David Abraham, Manuel Blum
12 SEPTEMBER 2008 VOL 321 SCIENCE
http://www.captcha.net/

[iii] Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)
Kumar Chellapilla, Patrice Y. Simard
http://research.microsoft.com/en-us/um/people/kumarc/pubs/chellapilla_nips04.pdf
(NIPS'2004), MIT Press.

[iv] Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA
Greg Mori, Jitendra Malik
Computer Vision and Pattern Recognition 2003

[v] Strong CAPTCHA Guidelines v1.2
Jonathan Wilkins
December 21, 2009
http://bitland.net/captcha.pdf

[vi] http://thebotnet.com/programming/35077-php-source-code-antirecaptcha/
http://wegeneredv.de/arc

[vii] security risks for online services by relying on reCAPTCHA
Benjamin Wegener
October 22, 2010
http://wegeneredv.de/antirecaptcha.pdf