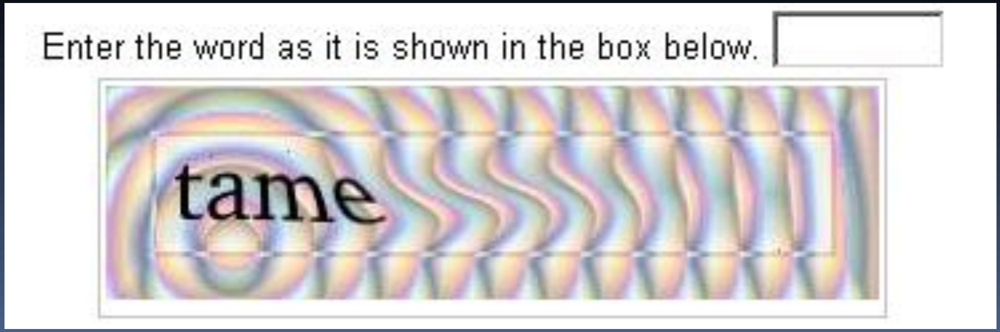
UNDERSTANDING CAPTCHA

The Need for CAPTCHAs To Prevent Abuse of Online Systems

William Sembiante
University of New Haven

What is CAPTCHA?

- Term coined in 2000 at Carnegie Mellon by Luis von Ahn, Manuel Blum, Nicholas Harper, and John Langford
- Acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart"
- Type of challenge-response test used to distinguish human users from computers
- Can be thought of as a reverse Turing test
- Program that creates tests that it itself cannot pass



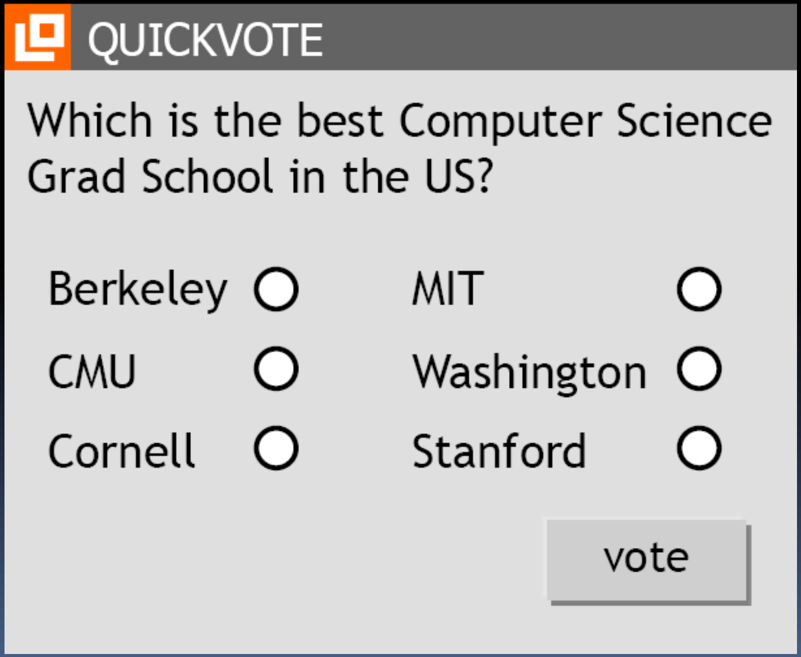
Enter the word as it is shown in the box below.

The Need for CAPTCHA

- In 1997, AltaVista was being victimized by the automatic submission of URLs to their “add-URL” service
- Chief Scientist Andrei Broder and his colleagues devised a way to prevent bots from submitting URLs
- Method was to generate random strings of text and distort them so Optical Character Recognition (OCR) programs would have difficulty reading them but humans would not
- The team simulated situations that OCR manuals reported as resulting in bad OCR
- After being in use for about a year, AltaVista reported that the system reduced spam-added URLs by 95%

The Need for CAPTCHA

- In 1999, *slashdot.org* issued an online poll asking users to pick the best computer science school in the US
- Students at MIT and Carnegie Mellon University created "voting bots" to vote for their school multiple times
- MIT finished with 21,156 votes
- Carnegie Mellon finished with 21,032 votes
- All other schools finished with less than 1,000 votes
- Proved that online polls could not be trusted unless they ensured that only humans could vote



QUICKVOTE

Which is the best Computer Science Grad School in the US?

Berkeley	○	MIT	○
CMU	○	Washington	○
Cornell	○	Stanford	○

The Need for CAPTCHA

- In September 2000, Yahoo! reported that bots were entering their online chat rooms and pointing legitimate users to advertising sites
- Yahoo! turned to CMU to help them solve their problem
- Luis von Ahn, Manual Blum, Nicholas Harper , and John Langford developed CAPTCHA
- They determined that CAPTCHAs should:
  - Present challenges that are automatically generated and graded
  - Be simple enough to be taken quickly and easily by humans
  - Accept virtually all human users and reject few
  - Reject virtually all machine users
  - Resist automatic attacks for many years to come
- US patent issued for CAPTCHA technology in April, 2001

CAPTCHA Applications

- Today CAPTCHAs prevent all sorts of online “misses” – misbehavior, mischief, misconduct
- CAPTCHA technology is used to:
  - Prevent automatic postings in Blogs, Forums, and Wikis
  - Stop scalpers
  - Protect Web site registrations
  - Protect email addresses from scrapers
  - Authenticate online polls
  - Prevent dictionary attacks
  - Stop search engine bots

CAPTCHA Guidelines

- Accessibility
  - All users need to have access to the protected site
  - For example, visually-impaired users need audio CAPTCHAs
- Image Security
  - Images must be secure enough to prevent OCR-based attacks
  - Random and thorough distortion techniques
- Script Security
  - Programs must be secure as well
  - Passwords passed in encrypted text
  - Destroy sessions after a CAPTCHA is solved
- Security After Widespread Adoption
  - Large pool of dictionary or words or images
  - Phonetic generators and nonsense words

CAPTCHA Guidelines

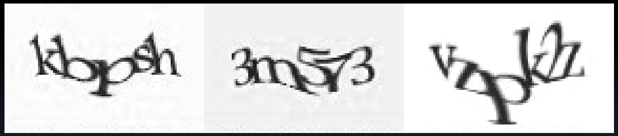
- Security from OCR is achieved by randomness:
  - Making the letters wiggly:

  - Adding noise or lines:

following
finding

  - Using a messy background:

  - Crowding or blending letters:



  - Segmenting characters:

  - Varying font thickness, color:

Breaking CAPTCHAs

- Programming Errors:
  - Not destroying sessions after a challenge is solved
    - Session ID and plaintext CAPTCHA can be resubmitted any number of times until the session expires
  - Allowing multiple guesses at the same image
    - Allows bots to make multiple guesses after incorrect machine learning attempts
  - Using a pool or dictionary of passwords that is too small
    - Allows crackers to compile a database of common or repeated challenges and their hash
  - Applying poor distortion techniques
    - Use of consistent fonts, constant glyphs, little noise, and low distortion make challenges vulnerable to OCR attacks

Breaking CAPTCHAs

- Human Solvers:
  - Sweat shops and human labor
    - Challenges relayed to human operators
    - Typical worker gets $2.50/hour
    - Solves about 720 captures/hour
    - 1/3 cent per solved CAPTCHA
  - Scraping challenges for use on high-traffic sites (Pornography Attack)
    - Challenge is copied and put on pornography site
    - User is asked to solve the test before they can see the image
    - Solution is relayed back to the target site in time to defeat the CAPTCHA

Breaking CAPTCHAs

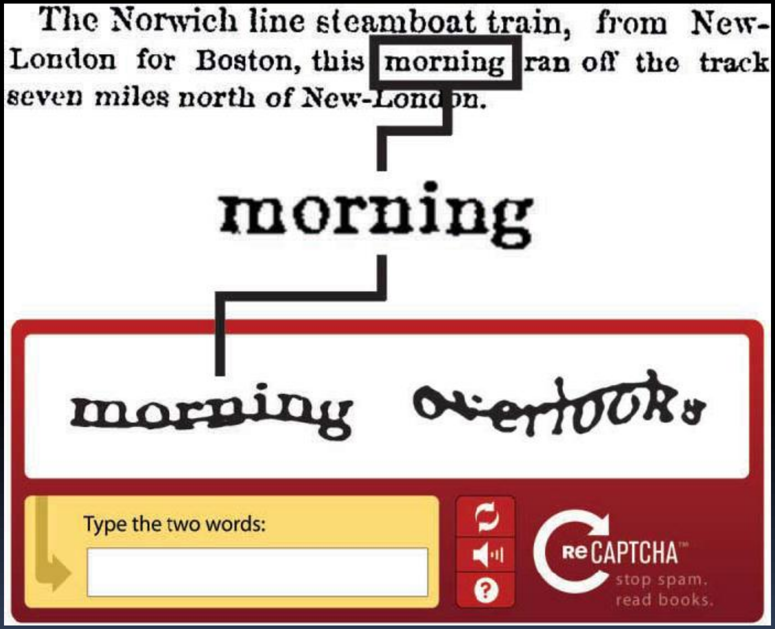
- Machine Learning:
  - Pre-processing
    - Application of algorithms to remove the effects of distortion, blurring, clutter, background noise, etc.
    - Easy problem for computers to solve
  - Segmentation
    - Splitting the image into regions which contain a single character
    - Complex and computationally expensive
  - Character Recognition
    - OCR software used to identify the characters

Breaking CAPTCHAs

- Non-OCR Based Programs:
  - PWNtcha – "Pretend We're Not a Turing Computer but a Human Antagonist"
    - Targeted Gimpy CAPTCHA
    - Exploited constant fonts, weak distortions, consistent glyphs
  - puremango .co.uk
    - Script-based attack
    - Exploited implementations that did not destroy sessions
- Breaking Audio CAPTCHAs
  - Segmentation – Splits CAPTCHA into different frequency bands, separating noise and words
  - Recognition – Frequency bands classified as words are identified using Automatic Speech Recognition (ASR) software

Advancing CAPTCHA Technology

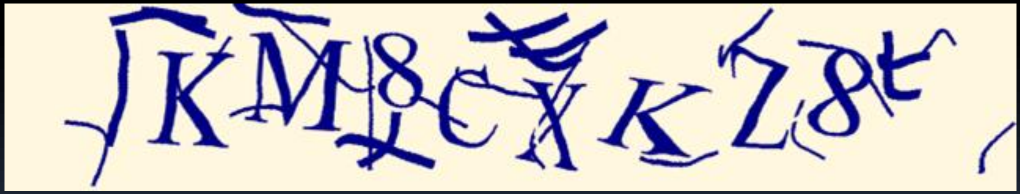
- reCAPTCHA
  - Founded by Luis von Ahn in 2008
  - Idea was to use CAPTCHAs to aid in the digitization of scanned media
  - Pairs a known word with a word that OCR programs did not recognize
  - Uses 3 different distortion techniques to prevent OCR
  - If control word is solved unknown word assumed to be correct as well
  - 3 matching guesses and word is added to dictionary
  - Achieves 99.1% accuracy rate at the word level
  - Bought by Google in September, 2009 for use in the Google Book Project



The Norwich line steamboat train, from New-London for Boston, this morning ran off the track seven miles north of New-London.

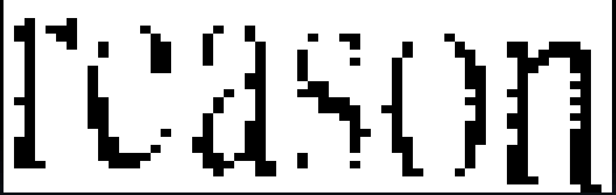
Advancing CAPTCHA Technology

- Improving Text-Based CAPTCHA
  - Private Implementations
    - Private libraries (remember ‘P’ is for “Public”)
    - Referred to as HIP (Human Interactive Proof)
    - Simard’s HIP developed at Microsoft
    - Uses 23 hardness parameters

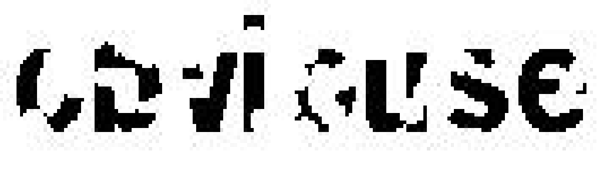


Advancing CAPTCHA Technology

- Improving Text-Based CAPTCHA (continued)
  - Palo Alto Research Center (PARC) developed 2 new CAPTCHA implementations
    - Based on image degradation or obliteration
    - Easy for humans to solve but hard for computers
    - Hard to restore and isolate characters
    - Pessimal Print

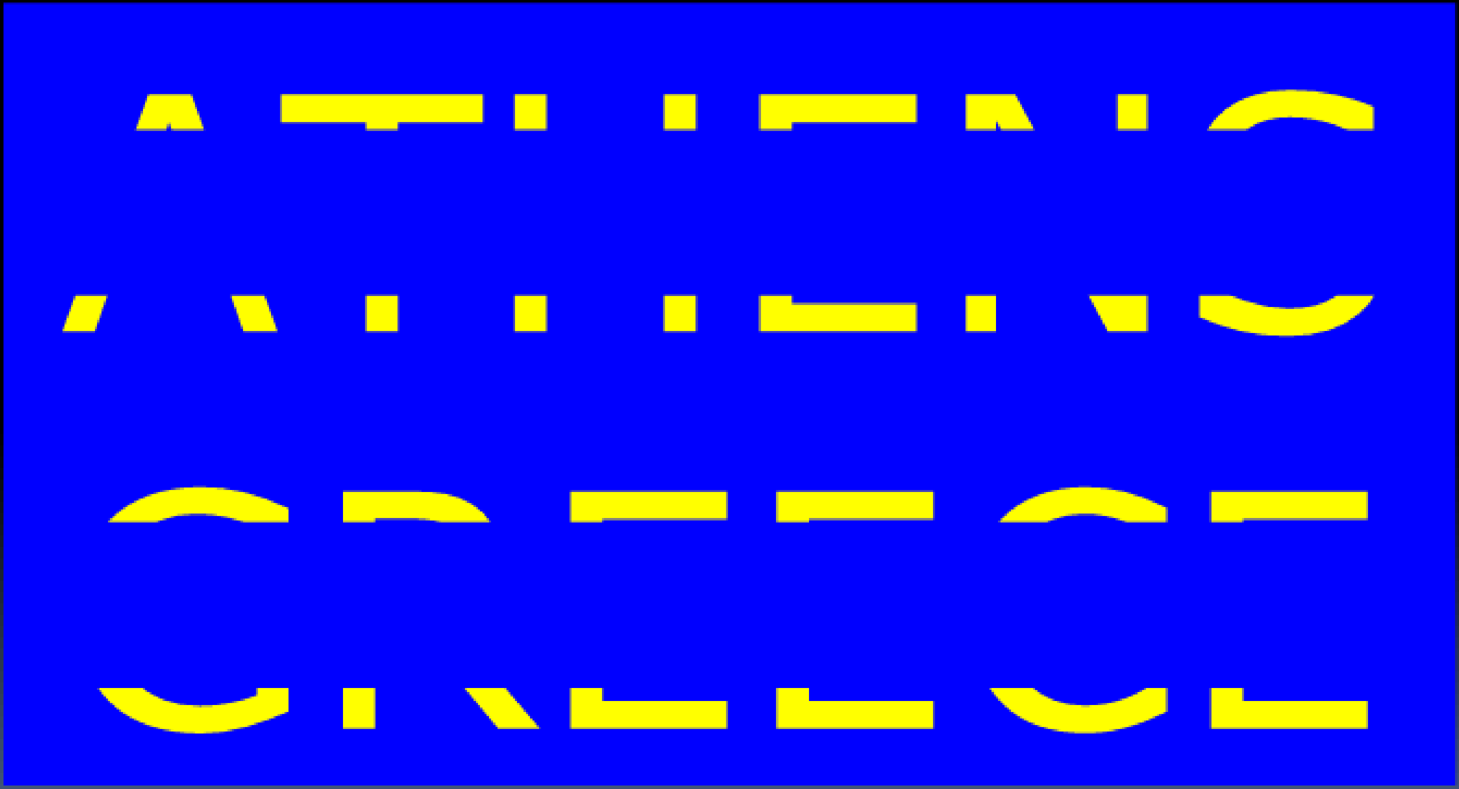


    - BaffleText



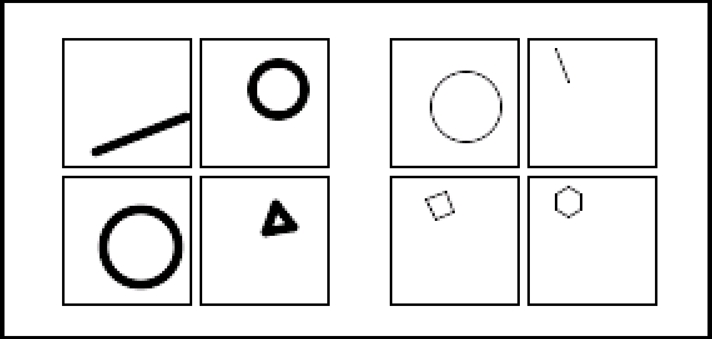
Advancing CAPTCHA Technology

- Image obliteration works because it’s hard for computers but the human eye is amazing!

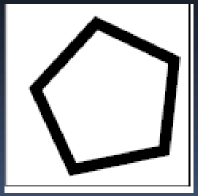


Advancing CAPTCHA Technology

- Graphic Based CAPTCHA
  - Bongo – Developed at Carnegie Mellon University
  - Test displays 2 series of shapes with a common characteristic

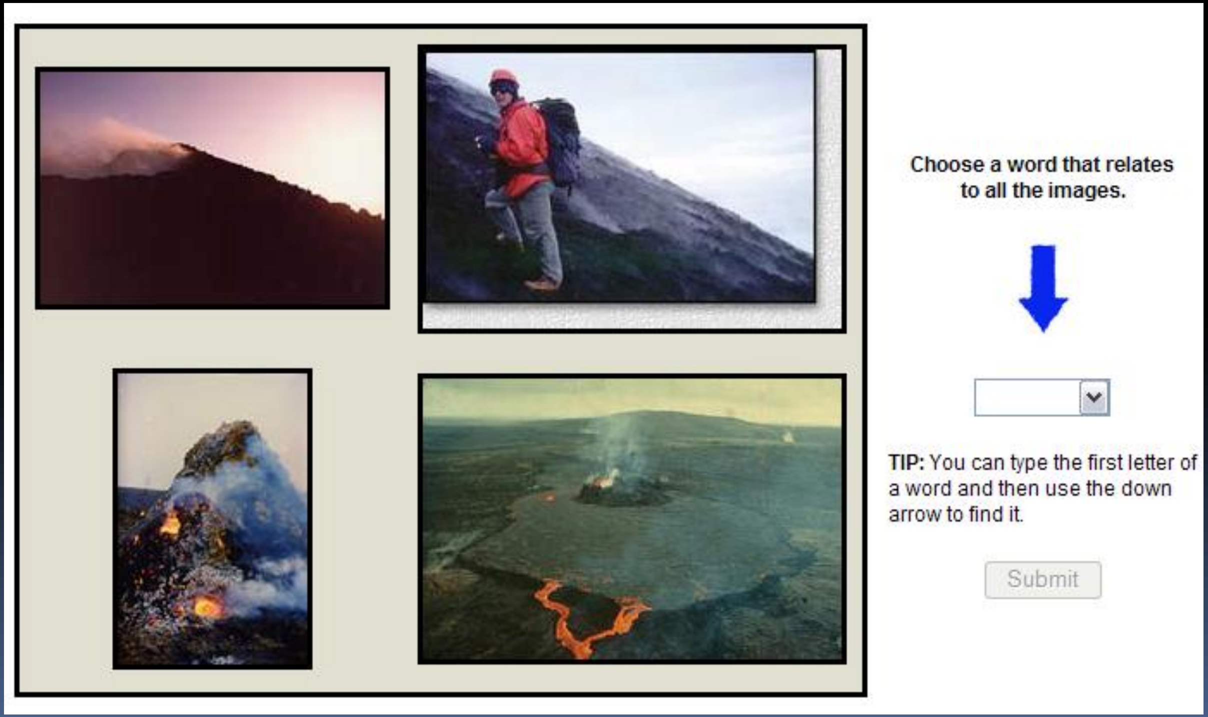


  - User is presented with 4 shapes and asked to identity which series each shape belongs to (abstract reasoning)



Advancing CAPTCHA Technology

- Image-Based CAPTCHA
    - ESP-Pix
        - Developed by Luis von Ahn and reCAPTCHA team
        - User presented with 4 distorted images and asked to identify them

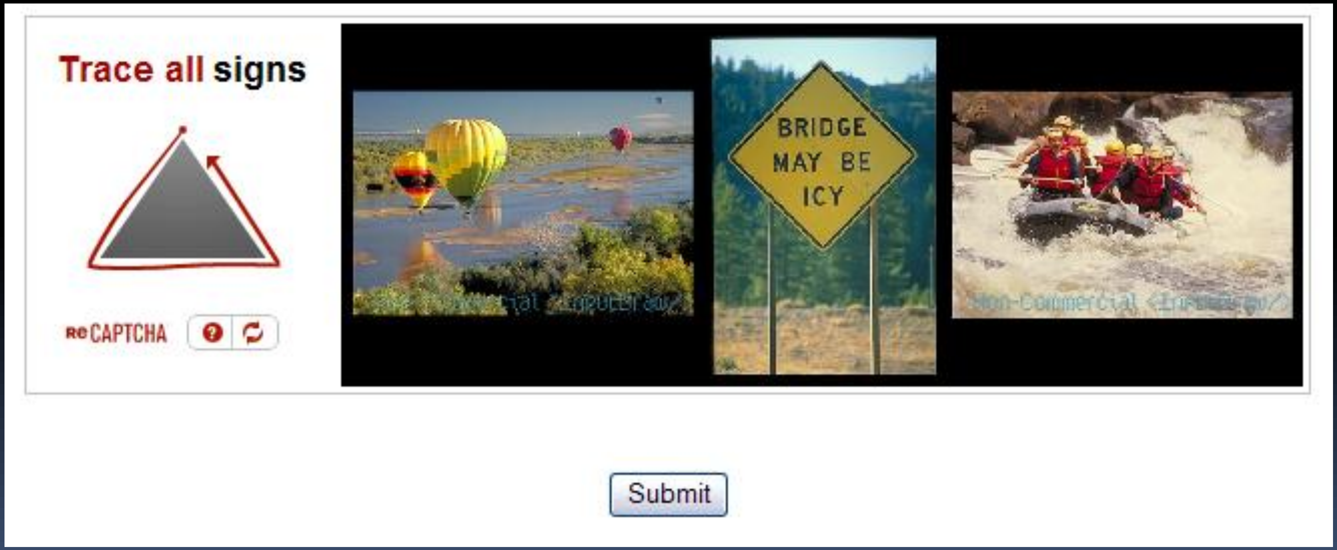


Choose a word that relates to all the images.

TIP: You can type the first letter of a word and then use the down arrow to find it.

Advancing CAPTCHA Technology

- Image-Based CAPTCHA (continued)
  - SQUIGL-Pix
    - Developed by Luis von Ahn and reCAPTCHA team
    - Presents a user with a series of distorted images and asks the user to indentify the correct image by tracing it



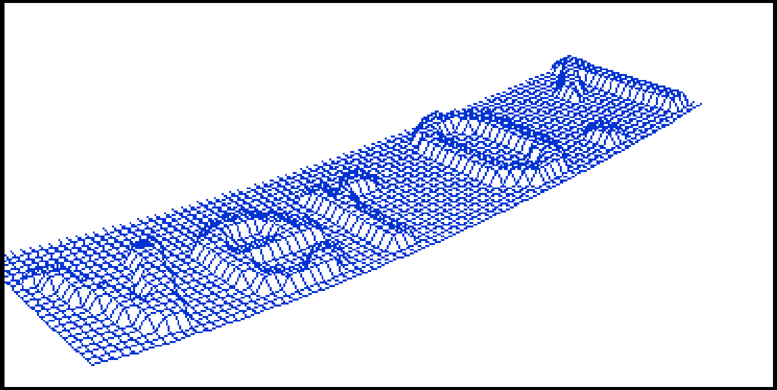
Trace all signs

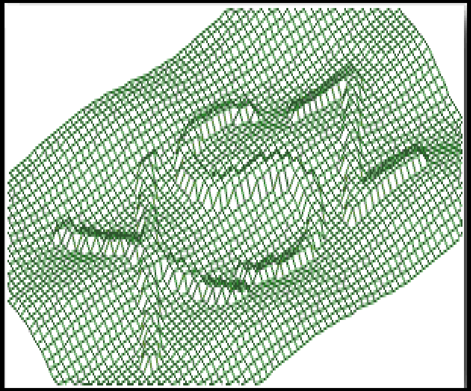
Advancing CAPTCHA Technology

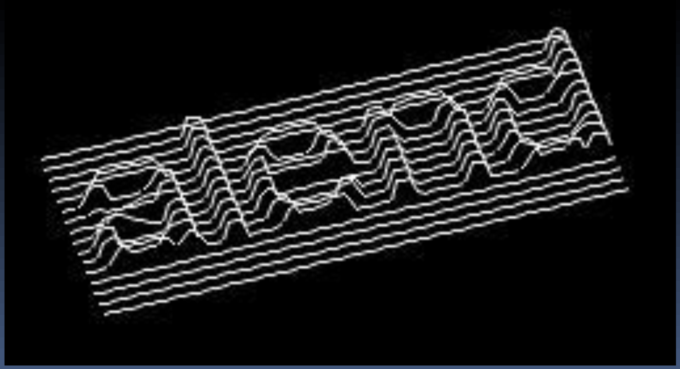
- ESP Game
  - Invented by Luis von Ahn
  - Use wasted human cycles to label all images on the Web
  - Pits 2 players against each other
  - Users cannot communicate with each other
  - Each player is presented with an image and asked to type single words to describe it
  - Once a common word is entered round is over
  - Control images are used to validate answers
  - Description is recorded and image is added to dictionary of control words and pool of images for CAPTCHA challenges
  - Estimated that 5,000 people playing simultaneously could label all of the images on Google in 30 days

Advancing CAPTCHA Technology

- Text-Based 3-D CAPTCHA
  - Harder than 2-D CAPTCHAs for machine learning

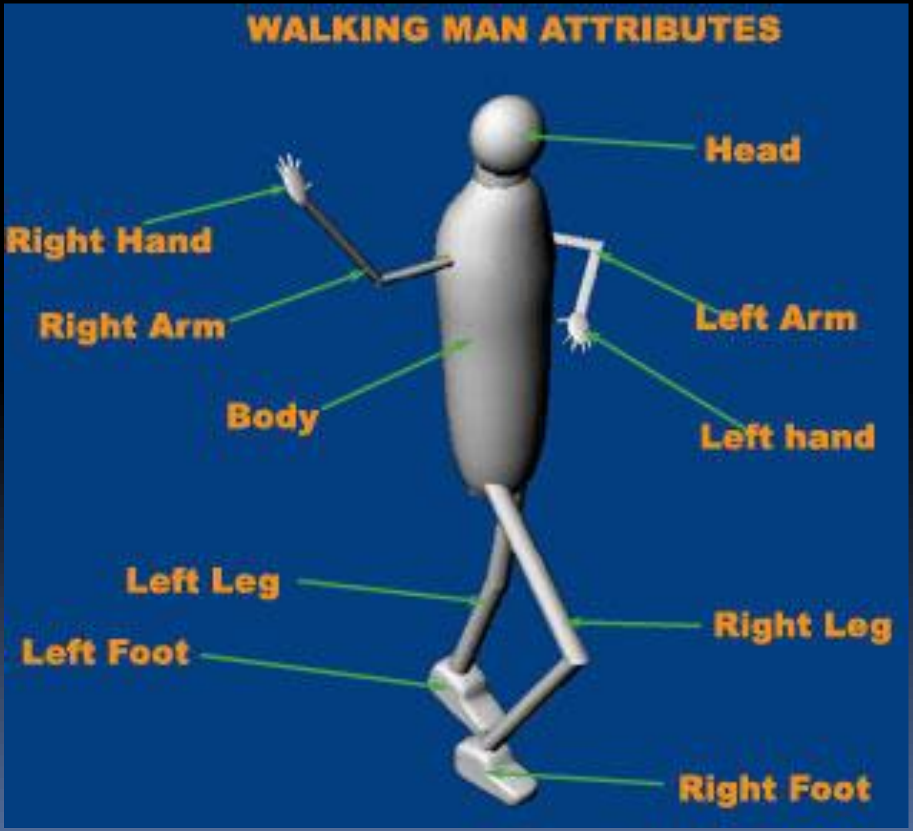


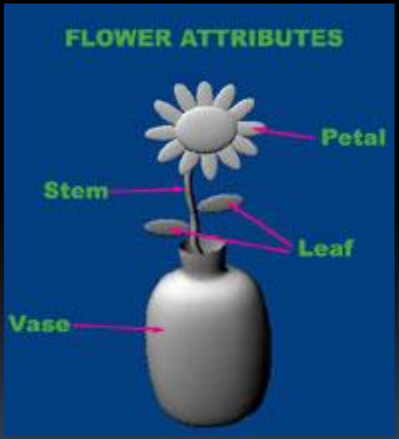




Advancing CAPTCHA Technology

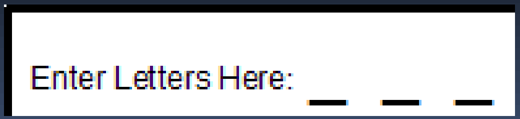
- Image-Based 3-D CAPTCHA
  - Developed by Michael Kaplan
  - Generates a database of 3-D objects and labels all attributes



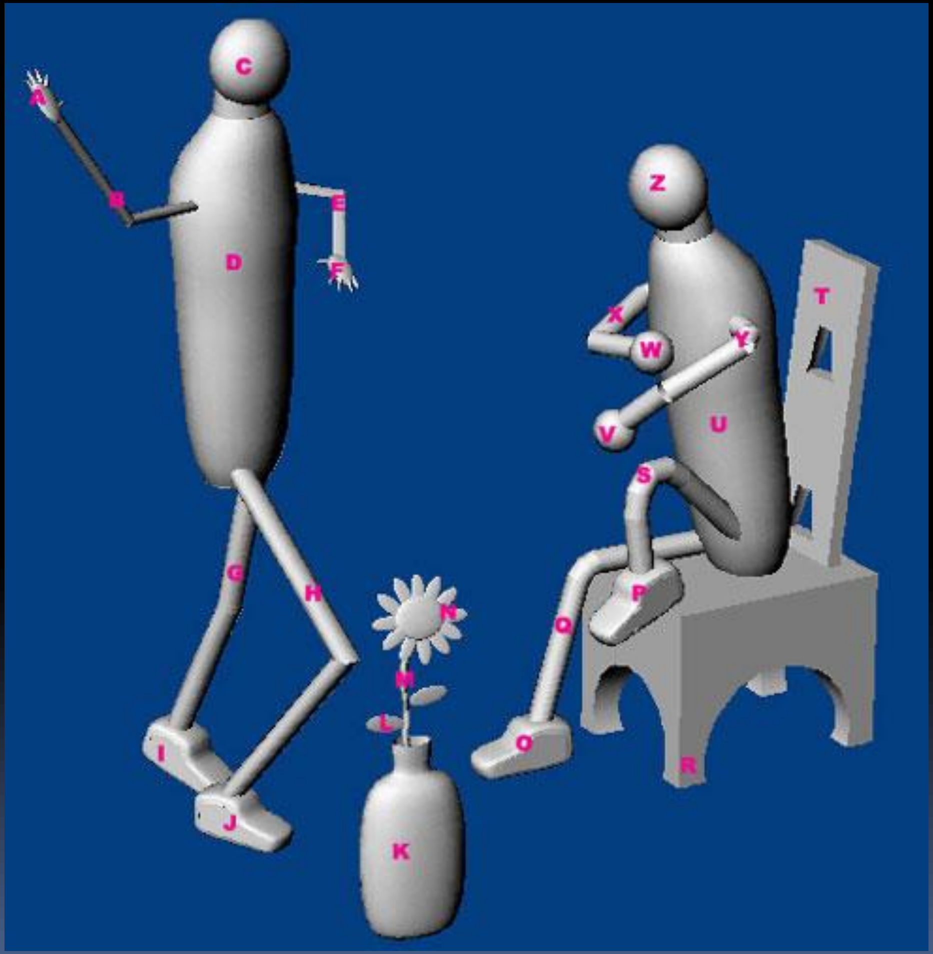


Advancing CAPTCHA Technology

- Image-Based 3-D CAPTCHA (continued)
  - Places objects in scenes and presents them in a challenge
  - User is asked to identify attributes in the picture
  - For example, user may be asked to identity the head of the walking man, the vase, and the back of the chair.



Enter Letters Here: __ __ __



Advancing CAPTCHA Technology

- Image-Based 3-D CAPTCHA (continued)
  - Resistant to brute force attacks:
    - Asking user to identify 3 objects presents 15,600 combinations
    - Increase to 5 and there are 7,893,600 possibilities
    - New challenge presented after *n* incorrect guesses
  - Resistant to machine learning techniques:
    - Attacks are easily detected
    - If a bot solves an image of a flower, then there would be a large number of correct responses identifying the flower and incorrect responses for other objects
    - Flower can be removed from database of objects and replaced with another object
    - Bot must recognize every object in the pool, and every variation of that object

Conclusions

- Effective despite attack attempts
  - CAPTCHA technology is advancing faster than crackers’ ability to break them
    - Many research projects ongoing
    - New private implementations
  - CAPTCHAs hit black hats where it hurts – in the pocketbook
    - Human labor costs increasing – not cost effective
    - Segmentation is expensive – computationally and in human costs
  - Pornography attack not a concern
    - Not enough traffic to inflict any real damage to protected sites

References

- Ahn, Luis von, & Blum, Manuel, & Langford, John. (2004, February). *Telling Humans and Computers Apart Automatically.* Retrieved November 1, 2009 from website: http://www.captcha.net/captcha_cacm.pdf
- Ahn, Luis von, & Maurer, Benjamin, & McMillen, Collin, & Blum, Manuel. (2008, September 8). *reCAPTCHA: Human-Based Character Recognition via Web Security Measures.* Retrieved November 7, 2009 from website: http://www.cs.cmu.edu/~biglou/reCAPTCHA_Science.pdf
- Ahn, Luis von. (2003, November). *CAPTCHA, the ESP Game and Other Stuff.* [PowerPoint slides] Retrieved November 12, 2009 from website: http://www.cs.cmu.edu/~biglou/cycles.ppt
- Atwood, Jeff. (2006, October 25). *CAPTCHA Effectiveness.* Retrieved November 4, 2009, from Coding Horror website: http://www.codinghorror.com/blog/archives/000712.html
- CAPTCHA. In *Wikipedia*. Retrieved November 1, 2009 from website: http://en.wikipedia.org/wiki/Captcha#Computer_character_recognition
- CAPTCHA. (2000 – 2009). *CAPTCHA: Telling Humans and Computers Apart Automatically.* Retrieved November 5, 2009 from website: http://www.captcha.net/
- CAPTCHA. (2000 – 2009). *reCAPTCHA: Digitizing Books One Word at a Time.* Retrieved November 6, 2009 from website: http://recaptcha.net/learnmore.html

References

- Chellapilla, Kumar, & Simard, Patrice Y. *Using Machine Learning to Break Visual Human Interaction Proofs (HIPs).* Retrieved November 10, 2009 from the website: http://research.microsoft.com/en-us/um/people/kumarc/pubs/chellapilla_nips04.pdf
- Chew, Monica, & Baird, Henry S. (2003, January 2). *BaffleText: a Human Interactive Proof.* Retrieved November 5, 2009 from website: http://www.cse.lehigh.edu/~baird/Pubs/baffletext.pdf
- Datta, Ritendra, & Li, Jia, & Wang, James Z. (2005, November). *IMAGINATION: A Robust Image-based CAPTCHA Generation System.* [PowerPoint slides] Retrieved November 14, 2009 from website: http://wang.ist.psu.edu/imagination/imagination.ppt
- Hocever, Sam. *PWNtcha – CAPTCHA Decoder.* Retrieved November 16, 2009 from caca labs website: http://caca.zoy.org/wiki/PWNtcha
- Jung, EJ. (2008, March 11). *CAPTCHA.* Retrieved November 8, 2009 from the website: http://www.cs.uiowa.edu/~ejjung/courses/169/lectures/15CAPTCHA_anot.pdf
- Kaplan, Michael G. *The 3-D CAPTCHA.* Retrieved November 15, 2009 from the website: http://spamfizzle.com/CAPTCHA.aspx
- Louis, Sari. (2006, April). *CAPTCHA (Multi-Media Security).* [PowerPoint slides] Retrieved November 12, 2009 from website: http://www.ee.columbia.edu/~suezou/e6886/isaF.ppt

References

- Mori, Greg, & Malik, Jitendra. (2003). *Breaking a Visual CAPTCHA.* Retrieved November 15, 2009 from the website: http://www.cs.sfu.ca/~mori/research/gimpy/
- Muqattash, Isa. (2003, November). *Breaking CAPTCHA (Multi-Media Security).* [PowerPoint slides] Retrieved November 12, 2009 from website: http://www.ee.columbia.edu/~suezou/e6886/isaF.ppt
- PARC. (2003, April 4). *CAPTCHAs.* Retrieved Novembers 12, 2009 from the website: http://www2.parc.com/istl/projects/captcha/captchas.htm
- PowersShow. (2009, July 4). *Fighting the WebBots.* Retrieved from the website: http://www.powershow.com/view.php?id=P1246211291aemHI&t=Fighting+the+WebBots
- Robinson, Sara. (2002, December 10) Human of Computer? Take This Test. *New York Times.* Retrieved November 27, 2009, from website: http://www.nytimes.com/2002/12/10/science/physical/10COMP.html?pagewanted=1
- Scribd. (2009, March 28). *CAPTCHA - Seminar Report.* Retrieved November 5, 2009 from website: http://www.scribd.com/doc/13743228/CAPTCHA-Seminar-Report

References

- Tam, Jennifer, & Simsa, Jiri, & Hyde, Sean, &Ahn, Luis von. *Breaking Audio CAPTCHAs.* Retrieved November 15, 2009 from the website: http://www.captcha.net/Breaking_Audio_CAPTCHAs.pdf
- Yeend, Howard. *Breaking CAPTCHA Without OCR.* Retrieved Novembers 16, 2009 from the puremango.co.uk website: http://www.puremango.co.uk/2005/11/breaking_captcha_115/