An Investigation Into a New Image Based CAPTCHA

Tianbo Chen
Dept. Electrical and Computer Engineering
Carnegie Mellon University
tianboc@andrew.cmu.edu

Safa Bacanli and Huy Truong
Dept. of Computer Science
University of Central Florida
sbacanli@cs.ucf.edu, estima94@gmail.com

Dr. Cliff Zou and Dr. Damla Turgut
Dept. of Computer Science
University of Central Florida
{czou, turgut}@cs.ucf.edu

ABSTRACT

A CAPTCHA (Completely Automated Turing Test to Tell computers and Humans Apart) is an important tool used to secure online services and resources. Some important functions of CAPTCHAs are [1]:

- Protecting website registration from bots
- Preventing dictionary attacks on passwords
- Stopping search engine bots from scouring websites wishing to remain unindexed

Due to advances in optical character recognition and segmentation techniques, text based CAPTCHAs are becoming easy to crack. In order to create a difficult test for robots to pass, image classification CAPTCHAs are becoming more widely used.

In this work, we examine the strengths and weaknesses of a new image classification CAPTCHA scheme.

CAPTCHA MODEL

Our CAPTCHA will present users with five images and ask the user one of three questions:

- Please order the following objects from fastest to slowest based on max speed
- Please order the following objects from largest to smallest
- Please order the following persons based on their living era- youngest first

Please order the following objects from fastest to slowest based on max speed

The goal is for the users to understand what is represented in each image and sort the pictures according to the question (size, speed or age). This CAPTCHA's strengths lie in the following properties:

- Users must understand what is represented in each picture
- Users must know the relative relationships between the objects
- The image database is constantly updated with new images to create a functionally infinite set of images

A working prototype of this CAPTCHA can be found at http://cns.eecs.ucf.edu/projects/ocaptcha/

RESULTS

Looking at an implementation of this CAPTCHA, we find that there is still a potential for an automated attack against this CAPTCHA scheme. Here are the key weaknesses of this CAPTCHA:

- The images are pulled from Google's image search by querying from a specific list of keywords. For example, "dog" could be a keyword. These keywords are manually created so there are only a finite number of them.
- Google's Vision API has shown high success in objection recognition in images. This is true even with common image distortion effects.

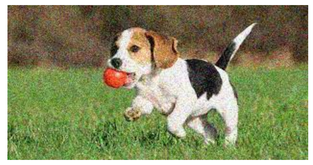
The following are some of our image testing results with Google's Vision API. We tested roughly 400 images with each distortion. The success rate indicates how many images were correctly identified.

Distortion	Success Rate
None	92%
Salt and Pepper	78%
Rotation	79%
Random RGB Value	93%
Gaussian Noise	89%

Salt and Pepper

Rotation

Random RGB



Gaussian Noise

More complicated image altering effects were also tested against Google's Vision API with no success.

Given these weaknesses, an automated attack could be set up as such:

- After iterating through multiple submissions of the CAPTCHA, reconstruct the list of keywords.
- Hardcode the relationships between the keywords for each question type.
- Use a powerful vision API to label the images based on the list of keywords and then sort them based on the hardcoded relationships.

RELATED WORKS

- In 2007, an image recognition CAPTCHA known as ASIRRA was created which had users discriminate 12 images of dogs and cats [2].
- However in 2008, a paper using machine learning techniques was shown to be able to crack the ASIRRA with an acceptable success rate [3].
- In 2010, another image classification CAPTCHA used a technique known as scene tagging. In this In this form of captcha, an image is shown with 4 objects placed on a background. The user will be asked to pick out the object that is not like the others. This work shares similar features to our CAPTCHA in that it requires users to understand the objects and their relative relationships. This CAPTCHA is also more secure against computer vision attacks [4].

CONCLUSION

We presented a different type of image classification captcha. Its novelty lies in its functionally infinite image database as well as its use of object properties which are not immediately known by a machine (size, speed, age). When a machine correctly identifies an image, it still must determine the relative relationships of the present objects.

Unfortunately, a combination of the limited keywords bank and the strong advances in machine learning and computer vision allow our CAPTCHA to be susceptible to automated attacks. We have shown that Google's Vision API - which is currently one of the best vision tools available - can be used to automate an attack against our CAPTCHA

REFERENCES

- [1] C. M. University. (2010) Captcha: Telling humans and computers apart automatically. [Online]. Available: http://www.captcha.net
- [2] J. H. Jeremy Elson, John R. Douceur, "Asirra: A captcha that exploits interest-aligned manual image categorization," ACM conference on Computer and communications security, pp. 366–374, 2007.
- [3] P. Golle, "Machine learning attacks against the asirra captcha," ACM conference on Computer and communications security, pp. 535–542, 2008.
- [4] C. C. Z. Peter Matthews, Andrew Mantel, "Scene tagging: Image-based captcha using image composition and object relationships," ACM Symposium on Information, Computer and Communications Security , pp. 345–350,2010.

ACKNOWLEDGEMENTS

The support for this work was provided by the National Science Foundation REU program under Award No. 1560302. Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.