FROM CAPTCHA TO AQ-SOCHAMACAP: A MOVE FROM STATIC QUESTION TO DYNAMIC QUESTION

Onwudebelu U.[1], Fasola S.[2], Obi C.N.[3] and Alaba O.B.[4]
[1]Department of Computer Science, Salem University, P.M.B. 1060, Lokoja, Kogi State, Nigeria
[2]Department of Computer Science,University of Ibadan, Ibadan, Oyo State, Nigeria
[3]Department of Computer Science, Federal Polytechnic Mubi, P.M.B. 35, Adamawa State, Nigeria
[4]Politehnica University, Bucharest, Faculty of Control and Computers, 060042, Bucharest Romania

ABSTRACT

This paper proposed AQ-SOCHAMACAP which is a type of CAPTCHA that has to do with mixing alphanumeric characters and other special characters, such that the user will be asked to look at the characters provided and then answer the challenge based on it equivalent question. In addition, rather than the question remaining static it will alternating for each CAPTCHA test such interchanging questions or instructions have as goal to obfuscate an Optical Character Recognition (OCR) software or automated malicious program which spammers have designed to adapt to the static trait of the existing CAPTCHA system questioning.

Keywords: CAPTCHA, HIP, Security, OCR, Turing test

1.0 INTRODUCTION

In 1950 Turing proposed a test for Artificial Intelligent (AI) in which a computer must fool a panel of humans into believing the machine is human and called the test Turing test. While in 1997 Naor discussed what he called Automated Turing Test (ATT) in which computers, rather than humans, must determine whether a user is human or a machine. Although, Coates et al (2001) call Naor's ATT a Reverse Turing Test (RTT), Ahn et al (2004) called it Human Interactive Proof (HIP), which Hopper (2003) describes as a protocol that allows a human to prove something to a computer. Ahn et al proposed a more specific form of HIP called **C**ompletely **A**utomated **P**ublic **T**est to tell **C**omputer and **H**uman **A**part (CAPTCHA).

This technology is now almost a standard security mechanism for defending against undesirable or malicious Internet programs, such as those spreading junk mails and those grabbing thousands of free emails accounts instantly application: Google, Yahoo! Mail, registration.com, Webmasters, Microsoft's MSN and Hotmail. A good CAPTCHA must not be only human friendly but also robust enough to resist computer programs that attackers write to automatically pass CAPTCHA tests (or challenge).

We have come across dozens of proposals for CAPTCHA designs, ranging from counting objects in a picture, segmenting faces, recognizing animations, identifying words in audio, etc. This paper discussed AQ-SOCHAMACAP a sorted character mathematical CAPTCHA that mixes both alphanumerical and special characters (symbols) together in which a user is expected to answer the test according

to the dynamic nature of the question to the corresponding test to become successful in the challenge. AQ-SOCHAMACAP is not just a character recognition scheme it include character separation (that is separating numbers from all the other characters in the image) and providing the right answer based on the type of question asked. Unlike other varieties of CAPTCHA schemes where the user is asked static questions or given unchanging instructions and provided with ready-made answer and expected only to type the characters, nevertheless, in AQ-SOCHAMACAP the user is expected to identify numbers in the mist of characters with interchanging questions or instructions and is granted access to the resource if the right answer is provided to the test. The main aimed of character mixture is to confuse the malicious automated script employed by attackers and also to avoid a situation where the user is provided ready-made answer. Here, the user is expected to task his brain by performing something like addition, multiplication, division, etc with the numbers in the image provided.

2.0 RELATED WORK

CAPTCHAs can take diversity of forms. Reading CAPTCHAs show a cluttered image of a distorted password for users to type; Speech CAPTCHAs play a distorted sound file over cluttered background noise; Quiz CAPTCHAs show a visual or audio puzzle or trivia question that a computer can generate and display, but not solve while Match CAPTCHAs show a set of related images or sounds and ask the user to identify their common theme (Blum et al, 2000). A text-only CAPTCHA shows a reading, quiz, or match CAPTCHA using only plain text (Godfrey, 2001). A Virtual Reality (VR) CAPTCHA shows a three-dimensional (3D) world for the user to navigate (Perrig and Song, 2002). Shape CAPTCHAs show complex shapes for the user to identify (Malik, 2002).

ARTiFACIAL is another form of CAPTCHA, which works as follows: Per each user request, it automatically synthesizes an image with a distorted face embedded in a cluttered background. The user is asked to first find the face and then click on 6 points (4 eye corners and 2 mouth corners) on the face. If the user can correctly identify these points, we can conclude the user is a human; otherwise, the user is a machine (Rui and Liu, 2003). A spatial CAPTCHA's text image is rendered from a three-dimensional model (OCR Research, 2004). A natural CAPTCHA uses media files that record the real world rather than synthesizing them from scratch (Lopresti, 2005). An implicit CAPTCHA blends so well into the flow of a Web site that users may not even know it is testing them (Baird and Bentley, 2005). Assira, a CAPTCHA that asks users to identify cats out of a set of 12 photographs of both cat and dogs. Assira's image database is provided by a novel, mutually beneficial partnership with Petfinder.com (Elson et al, 2007). The differences between cats and dogs are immediately obvious to humans. In many cases, species look similar, with only subtle cues to distinguish them. This makes it a hard vision problem. In order to check Internet masquerading Longe et al (2009) proposed a multiple CAPTCHA response system. Onwudebelu et al (2010) highlighted the discomfort faced by users in the process of using the CAPTCHA challenge. Thus, they made recommend-dations that will help CAPTCHA developers and sites owner to develop user friendly CAPTCHA. However, in all these various CAPTCHAs the same question is asked. This attitude allows attackers to use bot that knows the static question, thus making it easier for the automated script to answer the CAPTCHA.

3.0 PROPOSED TECHNIQUE

In most CAPTCHA presentation the characters are made of alphanumeric

characters only and sometimes thin and thick arcs that intersect characters while others include non-intersecting arcs of different thicknesses, arcs in the background color, random meshes, background textures etc. (Figure 3.1-3.7). Not surprisingly, these thin and thick arcs that intersect are also hard for users, since some characters become unclear to the users such as 1, 7, J, and P can become L, T, Y and R respectively when an arc is passed through them. Therefore, AQ-SOCHAMACAP has to do with mixing alphanumeric characters and other special characters, such that the user will be asked to look at the characters provided and solve the problem based on the type of question demanded. The question can take any form such as multiplication, division, subtraction, addition, etc. or any of the other form listed below.

3.1 Examples of Alphanumeric Character-Based CAPTCHA

Below are examples of CAPTCHAs that consist of alphanumeric characters that have been adopted by several companies to protect various services on the web. CAPTCHAs are deliberately vulnerable to OCR attacks. From an OCR-ing perspective the following are good: overlap, multiple colors, multiple fonts, image with too small rotation and background does not add too much extra protection. However, excessive obfuscation will make the CAPTCHA difficult for the users to answers (Figure 3.4). These distortions are fairly good but an OCR program could still just take a screenshot of your page and solve the CAPTCHA or an attacker may just relay the CAPTCHA to a user who is making use of the attacker's site (most often it is a porn site) to solve the challenge.

Mailblocks: While signing up for free email service with mailblocks (www. mailblocks.com), one will find HIP challenges of the type:  shown in Figure 1.

Figure 1: Mailblocks HIP sample

MSN: While signing up for free e-mail with MSN Hotmail (www. hotmail.com), one will find HIP challenges of the type shown in Figure 2.

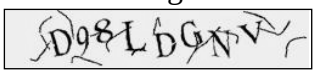

Figure 2: MSN HIP samples

Register.com: While requesting a whois lookup for a domain at www.register.com, one will find HIP challenges of the type shown in Figure 3.

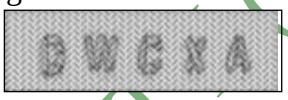

Figure 3: Register.com HIP sample

EZ-Gimpy (CMU): While signing up for free e-mail service with Yahoo! (www.yahoo.com), one received HIP challenges of the type shown in Figure 4.

Figure 4: EZ-Gimpy (CMU) HIP sample

Yahoo!: In August 2004, Yahoo! introduced their second generation HIP as can be seen in Figure 5.

Figure 5: Yahoo! HIP sample

Ticketmaster: While looking for concert tickets at www.ticketmaster.com, one will receive HIP challenges of the type shown in Figure 6.

Figure 6: Ticketmaster HIP sample

Google/Gmail: While signing up for free e-mail with Gmail at www.google.com, one will receive HIP challenges of the type presented in Figure 7.

Figure 7: Google HIP samples

Each form of CAPTCHA can have multiple implementations, each with its own advantages and disadvantages. Mori and Malik (2002) demonstrated an image filtering and dictionary attack with 94% success against EZGimpy and 33% success against Gimpy.

3.2 Proposed Test: AQ-SOCHAMACAP

As mentioned in Section 3.1 AQ-SOCHAMACAP has to do with mixing alpha-numeric characters and other special characters, such that the user will be asked to look at the characters provided and solved it based on corresponding question, say, sum (or multiple) the numbers by identifying numbers among the sorted character as well as performing any other task that may be required by the dynamic question. AQ-SOCHAMACAP is not just a character recognition scheme it include character separation. The 57 standard characters which include: 10 Numerals: 0 through 9; 26 Letters: A through Z; 1 Information Separator: Vertical Line; 17 Symbols: Ampersand, Apostrophe, Asterisk, Colon, Comma, Hyphen, Period, Dollar Sign, Equals, Left Parenthesis, Percent, Plus, Question Mark, Quotation Mark, Right Parenthesis, Semicolon, Slant; 3 Abstract Symbols: Chair, Fork, and Hook can be mixed in various proportion.

In AQ-SOCHAMACAP, the user is not provided with clichéd answer where he is expected to simply type in the characters provided as is common in other CAPTCHA scheme, rather he is expected to identify numbers among the characters provided and performed the task requested by the question associated with that particular CAPTCHA. For example, if the sum of all the numbers is asked, and if the user is unable to identify all the numbers among the characters and sum them correctly, he is assumed to be an automated script. But if he identifies the numbers and adds them rightly then he is considered to be a human being. It should be noted, in this particular case, the user is not expected to type any characters be it special characters or alphanumeric character.

Among visual challenges, character identification is the most obvious favorite because

(i) OCR is a well studied field and the state of the art is well known.
(ii) Characters were designed by humans for humans and humans have been trained at the task since childhood.
(iii) Each character has a corresponding key on the keyboard.
(iv) The task is easily understood by users without much instruction, and
(v) Character-based HIPs can be generated quickly (300 8-character HIPs per second on a 3GHz, Chellapilla et al, 2005).

Therefore, the special characters will not be an added burden to the users since he is not expected to type these characters rather to identify alphanumeric characters and execute the job requested by the corresponding question. AQ-SOCHAMA-CAP is user friendly since the user will appreciate some of these special characters as in the case of example three below where the special character is a symbol of a smiling faces. In addition, since numbers are used by people regardless of nationalities, cultural differences or educational background, all recognize numbers.

3.2.1 Dynamic Questions or Instructions

Every site uses the same questions for different visual verification of a bitmapped image - CAPTCHA. This has made most spammers to focus their attacks on the CAPTCHA without bothering much on the question knowing full well that it is the same unchanging question. Therefore there is a need for this to change drastically to tighten security. We propose a design in which the question or instruction will also be dynamic rather than being static. Below are examples of various static instructions and questions that are used in diverse sites:

- "Please type 1234 here",

- "In 656486473, what number comes before 3?"
- "What's the result of twenty two plus nineteen [8]?"
- "Enter the word <image> …",
- "Complete this CAPTCHA test before posting [9]",
- "Word verification<image>"
- Type the text you see below …
- First copy the string above (or below) to the text field below: …
- Security code? From image above: …
- ETC

Below are examples of AQ-SOCHAMA-CAP:

1. +EU4K7NL =
2. 7*@5# () ~ =
3. ☺9✡8☺&¥ =
4. €2÷☹1C·6* =
5. %4$4@5+3 =

Let us take example one for detailed analysis. The following question can be posed. All the questions below are asked with reference to example one above, that is,

+EU4K7NL =

(a) Please enter all the numbers.
ANSWER: 47

(b) Insert the last number.
ANSWER: 7

(c) Insert the first number.
ANSWER: 4

(d) Please sum all the numbers.
ANSWER: 11

(e) Please multiple all the numbers.
ANSWER: 28

(f) Please insert the last two letters
ANSWER: NL

Since users are living in a dynamic world they would like to see this dynamism being reflected or accommodated in the CAPTCHA system especially with regard to the questioning portion which has so far remain static to the advantage of the spammers and their malicious automated scripts.

4.0 CONCLUSION

In this paper, we have shown how AQ-SOCHAMACAP differs from other CAPTCHAs designs we have come across ranging from counting objects in a picture, segmenting faces, recognizing animations, identifying words in audio, differentiating between cats and dogs etc. The major contribution of this work is the move from static question to dynamic question for different AQ-CHAMACAP and the introduction of special characters in the CAPTCHA system. AQ-SOCHAMACAP is less bothersome to the user since users are just expected to identify the characters in the image provided and say for example, sum them up. The design of AQ-SOCHAMA-CAP may be made more robust by including and increasing segmentation.

5.0 REFERENCES

Ahn L. Von, Blum M., Hopper N.J. and Langford J. (2003). CAPTCHA: Using hard AI Problems for Security. Retrieved October 10, 2005 from http://www.captcha.net.

Ahn L. Von, Blum M. and Langford J. (2004). Telling Computers and Humans Apart Automatically. Communications of the ACM, 47(2), 57-60.

Baird H.S. and Bentley J.L. (2005). Implicit CAPTCHAs, Proceedings, IS&T/ SPIE Document Recognition & Retrieval XII Conference. San Jose, CA. January 16-20, 2005.

Chellapilla K., Larson K., Simard P. and Czerwinski M. (2005). Designing Human Friendly Human Interaction Proofs (HIPs). CHI 2005

Coates A.L., Baird H.S., Fateman R.J. (2001). Pessimal Print: A Reverse Turing Test. Proceeding of IAPR 6th Intl. Conference on Document Analysis and Recognition. Seattle, WA. September 10-13, 2001, 1154-1158.

Elson J., Douceur R.J. and Saul J. (2007). Asirra: A CAPTCHA that Exploit Interest-Aligned Manuel Image Categorization. CCS'07.

Godfrey P.B. (2001). Text-Based CAPT-CHA Algorithms. Proceedings of the First HIP Conference, 2002. December 15, 2001.

http://www.atelierphp5.com/un-captcha-accessible.html

http://www.spamtrackers.eu/wiki

Longe O.B., Robert A.B.C. and Onwu-debelu U. (2009). Multiple CAPTCHA Response System: An Enhanced Authentication Scheme for Checking Internet Masquerading. In Proceeding of the 2nd International Conference on Adaptive Science and Technology. (ICAST'09) pp: 244-249. http://www.edictech.com/ ICAST 09/ICAST2009Program.pdf

Lopresti D. (2005). Leveraging the CAPT-CHA Problem. Proceedings of the Second HIP Conference, 2005.

Malik J. (2002). Visual Shape Recog-nition and CAPTCHAs. Proceedings of the First HIP Conference, 2002.

Mori G. and Malik J. (2003). Recog-nizing Objects in Adversarial Clutter: Breaking a Visual CAPT-CHA. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, June 2003. Retrieved October 10, 2005 from http://www.cs.sfu.ca/~mori/research.

Onwudebelu U., Fasola S., Obi N.C. and Alaba O.B. (2010). CAPTCHA Malaise: Users Suffer Consequences of the Anti-Spam Technology while the Spammers Adapt. In Proceeding of the 1st International Conference and Workshop on Software Engine-ering and Intelligent Systems." (SEIS'10) pp: 113-125.

Perrig A. and Song D. (2002). New Directions for User Authentication: Reflex Instead of Reflection. In Proceedings of the First HIP Conference, 2002.

Rui Y. and Liu Z. (2003). Excuse Me, But Are You Human?