ISSN:0975-9646

CAPTCHAs based on the Principle- Hard to Separate Text from Background

Niket Kumar Choudhary[#1], Rahul Patil[#2]

[#]*1-2 Department of Computer Engineering, Pimpri-Chinchwad College of Engineering,*
1-2 Savitribai Phule Pune University, India.

Abstract—CAPTCHAs have become a very popular security mechanism used to prevent automated abuse of online services intended for humans. Different flavors of CAPTCHA can be seen on Internet. However, a wide variety of CAPTCHAs have been successfully attacked by automated programs. This has made CAPTCHA design an interesting area for research. Among various flavors of CAPTCHA text based are most preferable because of its low implementation cost but this category of CAPTCHA can be attacked with very high success rate. To provide stronger and user-friendly text based CAPTCHA, in this paper, we propose three text based CAPTCHA designs- BarCAPTCHA, TransparentCAPTCHA and ThreadCAPTCHA based on the design principle "hard to separate text from background". The underlying security assumption is that if an automated program cannot locate text in CAPTCHA then it cannot do further processing to identify the characters of it.

Keywords— CAPTCHA, security, automated abuse, online service, text based, design principle.

I. INTRODUCTION

CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) are the challenges given by the online service providers to its users to distinguish bots and humans. The concept of CAPTCHA was originally developed by [1] as hard Artificial Intelligence problem that can be used for security purposes. Since then CAPTCHAs have become an integral part of the Internet and used as a standard by online service providers to prevent automated abuse of their services intended for humans. An example of this could be preventing a bot from signing up many email accounts and sending Spam mails every minute [2].

CAPTCHAs are developed with the intent that they get easily cracked by a human and not by a bot. They should be very user friendly. They should also be easy to maintain. CAPTCHA schemes can belong to one of these categories- text based, image based, animation based, audio based and natural language based. Among these, text based CAPTCHAs are most easy to implement and maintain [3] which has made it most popular compared to others. For other kinds of CAPTCHA there is a need of a database which can store the challenge in the form of image or audio and its solution. But a text based CAPTCHA can be generated and processed at run time. There is no requirement of a database. In a text based CAPTCHA usually a sequence of characters is presented on an image. This sequence of characters can be generated using random functions available in almost all web designing languages. The image then may contain noise or the sequence of characters may be distorted to deter automated attacks. However, many of these CAPTCHAs are cracked with high successful rates using machine learning, computer vision, pattern recognition or other techniques [2, 4, 5, 6]. Other than these, Optical Character Recognition (OCR) program is also improving and becoming very effective in recognizing texts within an image. Before proposing new CAPTCHA designs, few CAPTHCHAs developed in past and their cracking techniques are studied. Section 2 presents some popular CAPTCHA schemes designed in past along with their automatic cracking approaches. In section 3, three proposed CAPTCHA designs are presented. Finally section 4 contains the conclusion.

II. LITERATURE SURVEY

Many 2D text based CAPTCHAs, proposed in past by various research communities, are vulnerable to attacks. These vulnerabilities are due to number of flaws in their design schemes which are described in this section.[7] successfully broke the popular Gimpy and EZ-Gimpy CAPTCHA (earlier used by Yahoo), developed at Carnegie Mellon University, 33% and 92% of the time respectively. To develop the cracking technique they used an image database of characters written with different fonts and also the knowledge that the word in the CAPTCHA is one of the words taken from dictionary. They then proceeded with generating some candidate words and selecting the word with highest matching score. They also described a holistic approach of recognizing the word in the CAPTCHA instead of trying to find individual characters of the word. This attack was also successful in breaking two other CAPTCHAs- PessimalPrint[8] and BaffleText [9]. [10] described how machine learning algorithms are effective in breaking different kinds of text based CAPTCHA. Their aim was to develop an algorithm which could work on any

randomly generated set of characters. The generated word need not be a word of dictionary. They tried to find segments or individual characters present in the text of the CAPTCHA. This led to a new principle of designing more secured CAPTCHAs- "segment resistant" [11]. Based on this principle new CAPTCHAs were developed in Microsoft research team and deployed on number of their online services but [4] showed that this CAPTCHA is also vulnerable to a low-cost attack. They did not negate the principle of segment resistant but said that after knowing the number of characters used in the CAPTCHA it is easy to segment them after some pre-processing. [2, 12, 13] showed that characters can be easily judged based on pixel count of their formation. [14] broke EZ-Gimpy and Gimpy-r by developing an estimation technique of distortion. Their first step of separating the text from its background gave birth to the new principle- "hard to separate text from background" [12]. The three CAPTCHA schemes proposed in this paper also follows this principle. Looking at the recent work, the most popular- reCAPTCHA, designed by Google, is broken down using holistic approach of recognizing shape contexts of the sequence of characters [15] and a method using heuristic character segmentation and recognition [16]. To overcome the limitations of 2D text CAPTCHAs 3D CAPTCHAs came into picture in recent years. In 3D CAPTCHA the assumption is that a computer program cannot identify 3D content but it is an inherent part of human visual system. This assumption is successfully falsified by [17] who showed that 3D CAPTCHA also contains some patterns which can be easily identified and cracked. Not only text based CAPTCHAs but other categories also have not been proven too strong. [18] demonstrated attacks against a number of image based CAPTCHAs. [19] described the crack for MathCAPTCHA. [20, 21] showed successful attack on audio based CAPTCHA. In addition, techniques for breaking animation based CAPTCHAs in [22].

III. PROPOSED DESIGN

Considering the steps of various cracking techniques applied so far on CAPTCHAs three designs of text based CAPTCHAs have been proposed in this paper- BarCAPTCHA, TransparentCAPTCHA and ThreadCAPTCHA. The CAPTCHAs are designed following the principle "hard to separate text from background".

In BarCAPTCHA lot of small bars are used to represent the text as well as to put noise in the background. The bars in the background are used to make bots difficult to distinguish which bars represent text and which represent noise. An example of BarCAPTCHA is shown in figure 1.

In the second design i.e. TransparentCAPTCHA text is written with a transparent font over an image. It is difficult for a program to find the pixels used to represent the text and the pixels used to represent other objects in the image. The image contains lot of pixels with non-uniform color distribution. Among these, few pixels represent text. This is a difficult task to identify the pixels representing text in the image programmatically. An example of TransparentCAPTCHA is shown in figure 2.

The third design, ThreadCAPTCHA contains the text which appears like it is written using a long thread in free form style. The thread not only used to write the text but also used to create noise in the image. Inside the image the thread at some location gives the impression of the text. An example of ThreadCAPTCHA is shown in figure 3.

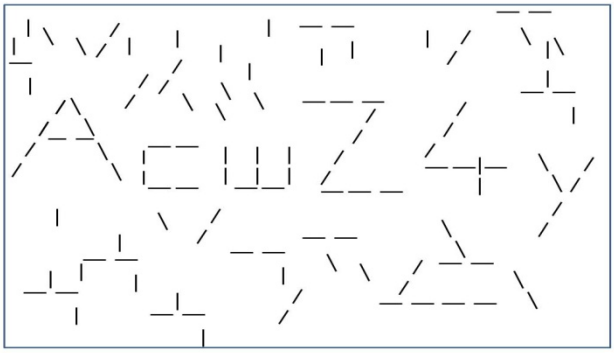

Fig. 1 An example of BarCAPTCHA

Fig. 2 An example of TransparentCAPTCHA

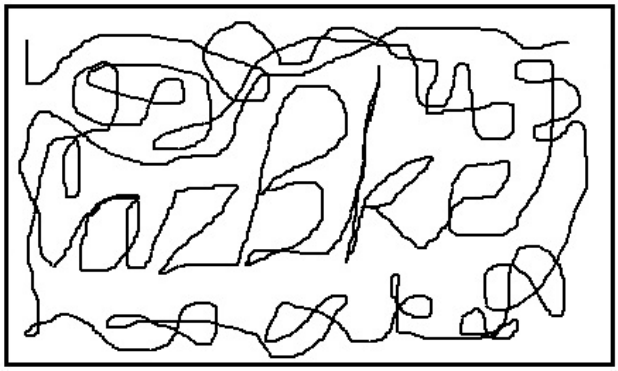

Fig. 3 An example of ThreadCAPTCHA

IV. CONCLUSION

In summary, three designs of text based CAPTCHA are proposed in this paper namely BarCAPTCHA, TransparentCAPTCHA and ThreadCAPTCHA. These three CAPTCHA designs follow the principle "hard to separate text from background". The CAPTCHAs are designed considering the techniques and concepts involved in cracking various existing CAPTCHAs. The proposed designs of CAPTCHA are thus too strong to get cracked and at the same time very user friendly.

REFERENCES

[1] L. von Ahn, M. Blum, N. J. Hopper and J. Langford, "CAPTCHA: using hard AI problems for security", *Springer*, vol. 2656, pp. 294-311, 2003.

[2] J. Yan and A. S. E. Ahmad. "Breaking visual CAPTCHAs with naive pattern recognition algorithms", "*IEEE Computer Society"*, pp. 279-91, 2007.

[3] K. Chellapilla, K. Larson, P. Y. Simard and M. Czerwinski, "Designing human friendly human interaction proofs (HIPs)", *ACM*, pp. 711-720, 2005b.

[4] J. Yan and A. S. E. Ahmad, "A low-cost attack on a Microsoft CAPTCHA", *ACM conference on computer and communications security,ACM*, pp. 543-554, 2008.

[5] A. S. E. Ahmad, J. Yan and W. Y. Ng, "CAPTCHA design: color, usability, and security", *IEEE Internet Computing, pp.* 44-51, 2012.

[6] Y. Nakaguro, M. N. Dailey, S. Marukatat and S. S. Makhanov, "Defeating line-noise CAPTCHAs with multiple quadratic snakes", *Computers & Security, Elsevier, pp.* 91-110, 2013.

[7] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: breaking a visual CAPTCHA", *IEEE Computer Society*, pp. 134-144, 2003.

[8] H. S. Baird, A. L. Coates and R. J. Fateman, "PessimalPrint: a reverse turing test", *IJDAR*, pp. 158-163, 2003.

[9] M. Chew and H. S. Baird, "BaffleText: a human interactive proof", *SPIE proceedings*, vol. 5010, pp. 305-16, 2003.

[10] K. Chellapilla, K. Larson, P. Y. Simard and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs (HIPs)", *Springer*, vol. 3517, pp. 1-26, 2005a.

[11] A. S. E. Ahmad, J. Yan and L. Marshall, "The robustness of a new CAPTCHA", *ACM*, pp. 36-41, 2010.

[12] J. Yan and A. S. E. Ahmad, "CAPTCHA security: a case study", *IEEE Security & Privacy*, pp. 22-28, 2009.

[13] J. Yan and A. S. E. Ahmad, "CAPTCHA robustness: a security engineering perspective". Computer, pp. 54-60, 2011.

[14] G. Moy, N. Jones, C. Harkless and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs", *IEEE Computer Society*, pp. 23-28, 2004.

[15] P. Baecher, N. Buscher, M. Fischlin and B. Milde, "Breaking reCAPTCHA: a holistic approach via shape recognition", *Future challenges in security and privacy for academia and industry, IFIP advances in information and communication technology*, vol. 354, pp. 56-67, 2011.

[16] C. Cruz-Perez, O. Starostenko, F. Uceda-Ponga, V. A. Aquino and L. Reyes-Cabrera, "Breaking reCAPTCHAs with unpredictable collapse: heuristic character segmentation and recognition", *Springer*, vol. 7329, pp. 155-165, 2012.

[17] V. D. Nguyen, Y. W. Chow and W. Susilo, "On the security of text-based 3D CAPTCHAs", *Computers and Security, Elsevier*, pp. 84-99, 2014.

[18] B. B. Zhu, J. Yan, Q. Li, C. Yang, J. Liu, N. Xu, M. Yi and K. Cai, "Attacks and design of image recognition CAPTCHAs", *ACM conference on computer and communications security, ACM*, pp. 187-200, 2010.

[19] C. J. Hernandez-Castro and A. Ribagorda, "Pitfalls in CAPTCHA design and implementation: the math CAPTCHA, a case study", *Computers & Security, Elsevier*, pp. 141-57, 2010.

[20] J. Tam, J. Simsa, S. Hyde and L. von Ahn, "Breaking audio CAPTCHAs", *NIPS, MIT Press*, pp. 1625-1632, 2008.

[21] E. Bursztein, R. Beauxis, H. Paskov, D. Perito, C. Fabry and J.C. Mitchell, "The failure of noise-based non-continuous audio captchas", *IEEE Computer Society*, pp. 19-31, 2011a.

[22] Y. Xu, G. Reynaga, S. Chiasson, J. M. Frahm, F. Monrose and P. Van Oorschot, "Security and usability challenges of moving-object CAPTCHAs: decoding codewords in motion", *Proceedings of the 21st USENIX conference on security symposium. Security'12. Berkeley, CA, USA: USENIX Association*, p. 4, 2012.