

Survey Paper on Genetically Optimized Face Image CAPTCHA

Juhi Shah¹, D. N. Rewadkar²

¹RMD Sinhgad School of Engineering, Warje, Pune - 411058, India

²RMD Sinhgad School of Engineering, Head of the Computer Department, Warje, Pune - 411058, India

Abstract: *The increasing use of smart phones, tablets, and other mobile devices poses a significant challenge in providing effective online security. CAPTCHAs, tests for distinguishing human and computer users, have traditionally been popular; however, they face particular difficulties in a modern mobile environment because most of them rely on keyboard input and have language dependencies. This paper proposes a novel image-based CAPTCHA that combines the touch-based input methods favored by mobile devices with genetically optimized face detection tests to provide a solution that is simple for humans to solve, ready for worldwide use, and provides a high level of security by being resilient to automated computer attacks. In extensive testing involving over 2600 users and 40 000 CAPTCHA tests, CAPTCHA demonstrates a very high human success rate while ensuring a 0% attack rate using three well-known face detection algorithms.*

Keywords: Mobile security, web security, CAPTCHA, face detection

1. Introduction

Due to recent developments in technology, users are rapidly adopting smart phones, tablets, and other non-traditional smart computing devices in lieu of desktop and laptop computers. Traditional input devices such as keyboards and mice are being replaced by more interactive touch screen technology. With advanced mobile devices, users can easily access Internet services such as online shopping and e-banking. These large-scale applications require improved interfaces (including security systems) designed to easily serve the growing mobile market [1].

Presently, a number of techniques provide device-level security to protect users in case of loss or theft of their mobile device. Solutions based on typing such as passwords and PIN codes dominate, but newer mobile-friendly techniques such as picture puzzles [2], tracing patterns [3], and biometrics features including touch pattern analysis [4], fingerprints [5], and facial images [6] are gaining popularity and acceptance. While many online service providers have completely redesigned their website portals or maintain special mobile versions of their websites, relatively little progress has been made with similar redesigns of application-layer security tools [7] to protect the online resources which mobile users access.



Figure 1: Example of a CAPTCHA image with correct selections, the human faces, circled

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is one major example of a security tool that is not yet mobile user-friendly. CAPTCHAs are designed to prevent automated attacks by requiring users to perform tasks that are relatively easy for humans but challenging for computers (automated algorithms) [8]. They have become ubiquitous in situations where websites want to prevent e-mail, instant messaging, and text message spam. CAPTCHAs provide an additional layer of security and are frequently paired with account login systems to prevent brute force password attacks [9].

Existing CAPTCHA implementations generally belong to one of three categories:

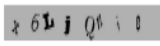

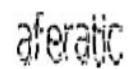

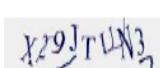
- (1) Text based
- (2) Image-based,
- (3) Video and Audio-based.

Some popular examples of each are shown in Table 1 and most existing CAPTCHAs are text-based. The user is presented with visually distorted text and asked to type it in correctly to prove he or she is a human and not a computer algorithm masquerading as a person. Many mobile devices lack a physical keyboard, which makes text-based input cumbersome and error-prone [10]. Further, most text based CAPTCHAs are (English) language-dependent and not suitable for multilingual worldwide usage. This paper mitigates the shortcomings of existing approaches and proposes a new CAPTCHA, termed as CAPTCHA, which leverages touch screen technology in mobile devices to make CAPTCHAs user-friendly and intuitive. CAPTCHA presents users with a composite image containing several visually distorted human faces along with other objects and non-real faces embedded in a complex background pattern. To prove that a user is human, users must solve the CAPTCHA by correctly selecting only the real human faces without choosing any other objects or non-real face images. If this is successfully done, the user is considered to be human and granted access to the secured resource. Fig. 1 shows an

example of how a CAPTCHA test can be correctly solved. In most cases, solving an instance only requires two or three taps from the user, making it extremely quick to complete and mobile device-friendly.

Key Contributions of this Research Includes:

- Design of an interactive non-keyboard-based (touch screen-compatible) image CAPTCHA to facilitate easy use on mobile devices.
- Generation of computationally-challenging face detection CAPTCHA tests to provide enhanced security.
- Utilization of genetic learning algorithms to optimize CAPTCHA parameters for better human performance and drastically lower the attack success rates of computer algorithms.
- Development of large-scale human and automated testing processes to evaluate performance of the proposed image-based face detection CAPTCHA.

CAPTCHA	Modality	Mode of Operation	Human Accuracy	Attack Accuracy	Sample
AltaVista [11], [12]	Text: 8 random characters	Each character is rendered in a different font, ransom-note style. Different rotations and distortions are applied to each letter.	-	Reduced page accesses by "over 95%"	
EZ-GIMPY [11], [13]	Text: 1 English word	Word is randomly distorted by adding white lines and deformations.	-	92%	
ScatterType [14], [15], [16]	Text: English word-like non-dictionary string of 6-8 characters	Characters are segmented into many pieces then systematically scattered.	Up to 95%	-	
BaffleText [17]	Text: Pronounceable English non-word of 5-8 characters	Text overlaid with random geometric shapes, difference masking applied.	89%	25%	
MSN [18], [19]	Text: 8 random characters	Characters are distorted and rotated, then arcs added to visually connect characters.	-	over 90%	

Handwritten [20]	Text: Full name of a city	Uses images of handwritten city names taken from U.S. mail.	100%	4-9%	
reCAPTCHA [21], [22], [23]	Text: 2 English words	Scanned words that failed OCR presented side-by-side. Some additional distortions may be applied.	-	30%	
ESP-PIX [24]	Images: 4 images	User selects category to describe images from predefined list.	-	High random guess rate	
Asirra [25], [26]	Images: 12 images of cats and dogs	User identifies cats or dogs.	High	82.7%	
Scene Tagging [27]	Images: Small number of images on background image	User answers questions relating to number of images, placement, or relationship to each other.	96.6%	2.6%	
MosaHIP [28]	Images: Collage of many images	User drags descriptor labels on top of images they represent.	98%	4.1%	
IMAGINATION [29], [30]	Images: Collage of images	User clicks on center of one image then categorizes that image.	70%	4.95%	
Digg Audio [31]	Audio: Audio recording of random letters and numbers	User enters information from audio.	-	71%	
Video [32], [33]	Video: Flash video	User types three words describing video.	90%	13%	

Table 1: Summary of selected existing CAPTCHAs

2. Literature Survey

Image-based face detection CAPTCHA for improved Security

They demonstrate an implementation of novel image-based face detection CAPTCHA to add an additional layer of security in web-based services. Existing CAPTCHAs are vulnerable to computer attacks. Text-based CAPTCHAs are vulnerable to advanced OCR technologies. Image-based CAPTCHAs use a small subset of images and are susceptible to random guessing. When the images or videos are selected

from a large database, the users are presented with limited options making it susceptible to random guessing or machine learning techniques. Speech recognition software is used to exploit audio-based CAPTCHAs. Minimizing the vulnerabilities to prevent computers from solving the CAPTCHAs also makes it challenging for humans, often requiring multiple attempts to successfully solve the CAPTCHA.

They proposed an algorithm to generate an image-based CAPTCHA that uses the concept of face detection. The proposed algorithm embeds multiple human faces and non-

human faces in a background image to create image CAPTCHAs. The background image contains randomly generated overlapping blocks of different shapes and contrast levels. The faces were selected from the CMU face database and were subjected to known distortions. By varying different parameters, the intensity of distortion is controlled to produce low, medium, and high levels of distortion. All these processing make it very challenging for face detection algorithm to accurately select all human faces embedded in the CAPTCHA image, while humans generally are able to identify the embedded human faces with relative ease. The design objective Image-based face detection CAPTCHA for improved security [28] is to generate CAPTCHA images such that the computers attack rates are minimized while human accuracy to solve the same CAPTCHA is considerably increased. The use of image quality metrics to study the characteristics of images and design optimal images is briefly presented Here.

An extensive experimental study demonstrates these important features of the image-based face detection CAPTCHA. In addition, key factors that need to be considered in designing image-based face CAPTCHAs are described in detail. The proliferation of new generation mobile devices increasingly uses Internet-based applications and it is imperative they be made secure and resilient to attacks. These devices generally do not have a convenient keyboard and therefore the proposed image-based face detection CAPTCHA is ideally suited for clicking to solve the CAPTCHA rather than typing. Since there is no text involved, this CAPTCHA is language-independent and can be widely used by a large audience.

CAPTCHA Based on Human Cognitive Factor

Here, illustrates a new design for CAPTCHA system based on human cognition. This model demonstrates the ability of human to find the answer that other bots and external programs fail to interpret and evaluate. The conducted survey explains the usability of this new form of CAPTCHA and provides valuable feedback to design the overall system and types of question pattern. This framework can easily be extended to specific website to include question of any particular area of interest.

3. Conclusion

The unique touch screen technology of mobile devices can be leveraged to create an additional layer of security that is both effective and user friendly. The proposed genetically optimized CAPTCHA works efficiently on both touch screens used by tablets and smart phones and on traditional computers, achieving a high 88% human accuracy rate during evaluation. It does so without compromising performance, offering an effective 0% automated attack rate. This combination of low attack rates, high human accuracy rates, and convenient mobile device usage provides major improvements over existing desktop centric security CAPTCHAs in widespread use today.

References

- [1] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Comput. Security*, vol. 28, nos. 3_4, pp. 130_137, 2009.
- [2] J.-C. Birget, D. Hong, and N. Memon, "Graphical passwords based on robust discretization," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 395_399, Sep. 2006.
- [3] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, "On the need for different security methods on mobile phones," in *Proc. 13th Int. Conf. Human Comput. Interaction with Mobile Devices and Services*, 2011, pp. 465_473.
- [4] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 136_148, Jan. 2013.
- [5] H. Lee, S.-H. Lee, T. Kim, and H. Bahn, "Secure user identification for consumer electronics devices," *IEEE Trans. Consum. Electron*, vol. 54, no. 4, pp. 1798_1802, Nov. 2008.
- [6] D.-J. Kim, K.-W. Chung and K.-S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," *IEEE Trans. Consum. Electron*, vol. 56, no. 4, pp. 2678_2685, Nov. 2010.
- [7] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel, "Semantically rich application-centric security in android," in *Proc. ACSAC*, Honolulu, Hawaii, Dec. 2009, pp. 340_349.
- [8] S. Shirali-Shahreza, "Bibliography of works done on CAPTCHA," in *Proc. 3rd Int. Conf. Intell. Syst. Knowl. Eng.*, vol. 1. Xiamen, China, 2008, pp. 205_210.
- [9] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. 9th ACM Conf. Comput. Commun. Security*, 2002, pp. 161_170