THE NOVEL IMAGE BASED CAPTCHA FOR SECURITY IN WEB APPLICATIONS

Miss Rachana P G [1], Dr. Shrinivasa Naika C L [2]

[1]Student, [2]Assistant Professor, Computer Science and Engineering, UBDTCE, VTU (India)

ABSTRACT

Internet is being used for various activities by great range of users even through smart phones, tablets and other mobile devices. It is crucial for websites to differentiate human users and computer programs because malicious computer programs are threat for availability and security of websites. The challenge is to stop automated scripts from enforcing DOS attack, while ensuring proper service to genuine users. This paper proposes a novel image based CAPTCHA which overcome the disadvantage of language dependency in text CAPTCHA and it combines touch based input methods favored by mobile devices to solve CAPTCHA which is generated through unique steps. To solve CAPTCHA, user must correctly identify visually distorted human faces embedded in complex background without selecting any non human faces.

Keywords: CAPTCHA, Face detection, Mobile Security, Web Security

I. INTRODUCTION

Security is a major concern on web exposed systems holding valuable data or something that can be compromised.

There are many types of attacks that can be carried out on these systems. A variety of bots, spiders, DOS attacks, domain hijacking, worms and spam pose a serious threat to online systems and can cause major losses. So there is a great need for secondary authentication to reduce automated attacks while posing a minimal hindrance to legitimate users. CAPTCHA is one of the possible ways to classify human users and automated scripts. Completely Automated Public Turing Test to Tell Computers and Humans Apart or CAPTCHA is the standard security technology designed to distinguish between genuine users and automated scripts. The objective of CAPTCHA is to ensure proper service to genuine users while minimizing the attacks by bots. CAPTCHAs are being used for several services including web and financial services, and to provide security against malicious attacks. CAPTCHA focuses on developing tests that are easy for humans to solve and difficult for automated approaches. The challenge is to stop automated scripts from enforcing DoS attack. Existing CAPTCHA algorithms can be broadly grouped into three classes [1]: (1) text based, (2) image-based, and (3) video- and audio-based CAPTCHAs. Text-based CAPTCHAs are the most common and widely used form. These CAPTCHAs require the users to decipher text that has been visually distorted and rendered as an image. A major shortcoming of these early approaches was vulnerability to segmentation, where each character could

be identified in isolation. This greatly simplifies attacks using optical character recognition techniques. One solution was proposed to design the CAPTCHA such that one-to-one mapping between characters and outlines was distorted. As an alternative to text, several CAPTCHA applications utilize image classification or recognition tasks as part of their test and overcome disadvantage of language dependency. Other than text and image CAPTCHAs, video and audio CAPTCHAs have also been proposed. Video-based CAPTCHAs function by posing the tagged videos with descriptive text. To provide access for visually-impaired users, audio CAPTCHAs are used as an alternative to standard visual CAPTCHAs. These work by playing a recording of words or letters which users are then asked to enter.

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 [2]. 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 [3], tracing patterns [4], and biometrics features including touch pattern analysis [5], fingerprints, and facial images 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 tool to protect the online resources which mobile users access. CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is one major example of a security tool.

Key contributions of this research include:

1) Design of an interactive non-keyboard-based (touch screen-compatible) image CAPTCHA to facilitate easy use on mobile devices.

2) Generation of computationally-challenging face detection CAPTCHA tests to provide enhanced security.

In this paper, we propose a Novel Image based CAPTCHA method. In section 2, we analyze the main design idea of this new implementation of CAPTCHA mechanism. In section 3 we give an example of our implementation, and illustrate the flow chart step by step. Section 4 concludes with a research summary.

II. DESIGN

In this paper, we present Novel Image Based CAPTCHA — in which four to six distorted face/non-face images are embedded in a complex background and a user has to correctly mark the center of all the face images within a defined tolerance.

2.1 Algorithm of Design

CAPTCHA generation:

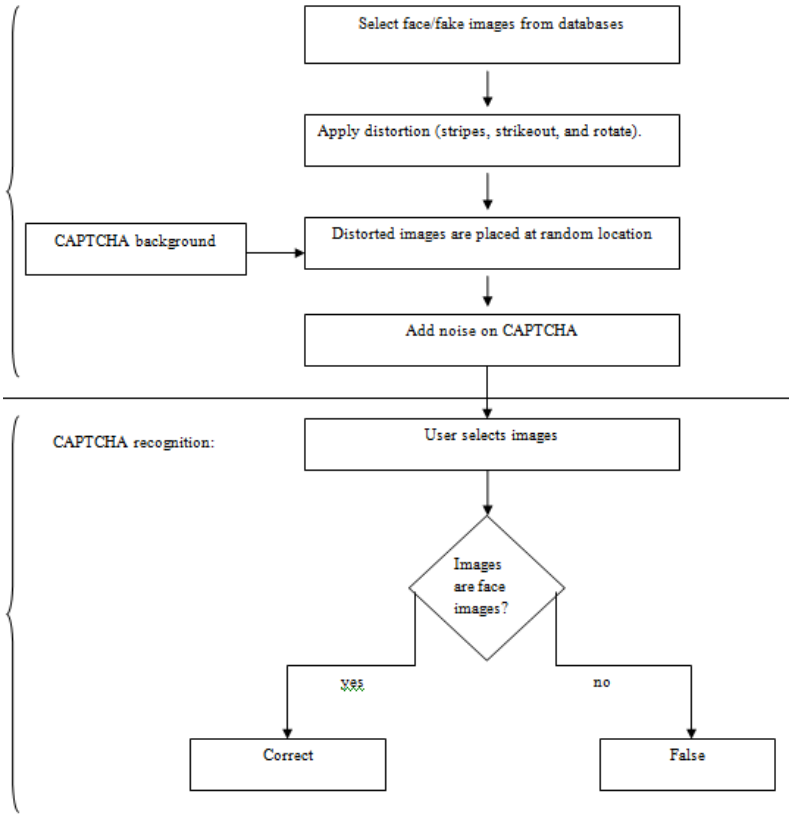

Fig.1 Algorithm of Design

III. THE PROPOSED NOVEL IMAGE BASED CAPTCHA ALGORITHM

The proposed Novel Image Based CAPTCHA algorithm utilizes the limitations of automatic algorithms to create image CAPTCHAs. In other words, the proposed algorithm is based on optimizing sets of parameters on which standard face detection algorithms fail but humans can succeed. The process of using Novel Image Based CAPTCHA is as follows:

- The face CAPTCHA image containing distorted and occluded genuine face images and fake images on a random background is shown to a user.
- The user must select all genuine face images present in the CAPTCHA.
- If all the responses are correct (i.e. approximate center of all genuine faces are marked correctly) then the test is solved otherwise not.

3.1 Generating Novel Image Based CAPTCHA

In the Novel Image Based CAPTCHA design, we choose the following parameters (and related operations):

- The first parameter is the total number of images, both genuine and fake faces, and is represented as n_{total}. Genuine faces are images of real humans collected from different publicly available face databases. Fake faces are images of cartoons and other objects known to generate false positives by automatic face detectors.
- The number of genuine face images in a CAPTCHA, represented as n_{face}, is the second parameter. In a given CAPTCHA, $n_{total} = n_{face} + n_{fake}$. Where n_{face} is the number of fake images. For a given CAPTCHA,

we only need to define n_{fake} and n_{face}. Also, randomly changing these parameters in each (new) CAPTCHA can change the content such that only a genuine human user can respond correctly.

- The third parameter, CAPTCHA background B, is important to make sure that background has randomness to confuse automatic face detection algorithms. B contains parameters such as the number of background shapes to be generated (n_s), the number of dilation operations to be adopted (n_d), and the number of random portions to be placed (n_p).
- Location (x, y) of each constituent image is an important factor. With random location, the segmentation is more difficult than if a static location scheme is used.
- Next, five distortion operations are applied as follows:

➢ Stripes of three to six pixels width are applied on some constituent images (faces and fake faces) in the CAPTCHA. It is not necessary that this operation is applied uniformly on all face or fake face images in a CAPTCHA. An example of this operation is shown in Fig. 2(a).

➢ Rotate operation is used to rotate the constituent face and fake images with θ^0 angle (Fig. 2(b)).

➢ Strikeout operation, as shown in Fig. 2(c), is used to cover key facial features such as eyes and mouth with some transparency.

➢ Blending operation is used to smoothly blend the constituent face and fake images with the background, as shown in Fig. 2(d).

➢ Noise addition. Using the above mentioned parameters and operations, the CAPTCHA image is prepared and then noise is added on the complete CAPTCHA image. The type parameter is used to select the type of noise to be applied (additive, multiplicative or salt & pepper). Collectively, these parameters are referred to as n_s.

(a) and (b) **(c)** **(d)**

Fig.2 Illustrating the Effect of (A) Stripes,(B) Rotation, (C) Strikeout And (D) Blending with The Background and Noise Adding.

3.1.1 Background Generation

Here, we have followed the random color approach, in this approach; the background image is created using random shapes such as circles, squares, and crosses with randomly chosen sizes and colors. These shapes are then pasted on the canvas at random co-ordinates to generate the final background image. This background image is then dilated before being used for CAPTCHA generation.

a. b.

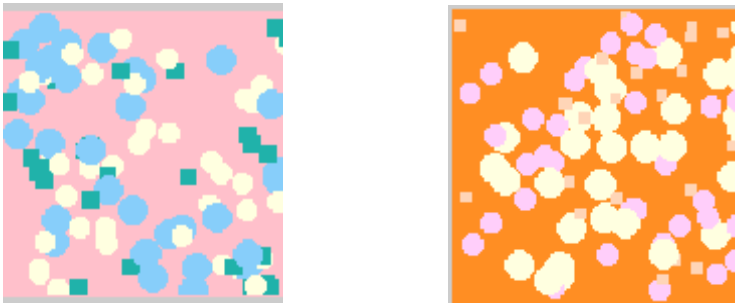

Fig.3. a and b: Background Generation Using Random Color Approach.

To make the background more complex for automated bots to attack or break the CAPTCHA, we are using different types of noises such as Gaussian noise and salt pepper noise. In order to make image selection complex for automated systems we are using different structural elements such as disks, ball and square shapes and we are dilating the shapes to make CAPTCHA solving easier for human and difficult for automated systems.

3.1.2 Novel Image Based CAPTCHA generation

Below are the steps in generating Novel Image Based CAPTCHA:

Step 1: From a set of genuine and false face images, randomly select $n_{face} \geq 2$ (i.e., the number of face images) and

$n_{fake} \geq 1$ (i.e., the number of fake images).

Step 2: Each constituent image (both genuine and fake) is processed using the distortion operations (stripes, strikeouts, and rotate).

Step 3: Each constituent face image is placed at a randomly selected location (x, y) on the CAPTCHA background B.

Step 4: At the end, one of the three noise operations {additive, multiplicative, or salt & pepper}, is applied on the complete CAPTCHA image to generate the final CAPTCHA.

Fig.4 Image Underwent Distortion Operation.

Fig.5 Placing Images in Random Location

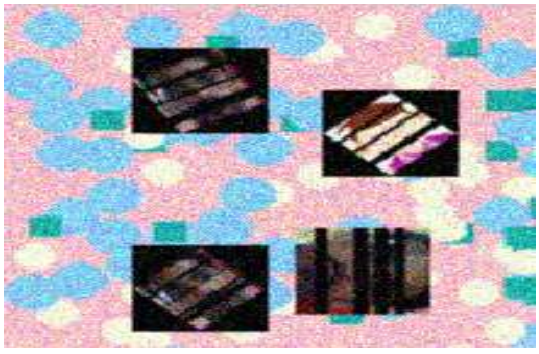

Fig.6 Addition of noise

IV. CONCLUSION

This paper presents the Novel Image Based CAPTCHA algorithm that utilizes the difference between face detection capabilities of humans and automated algorithms. By combining face detection with visual distortions, it is possible to create a test that is simple for human users to solve while effectively eliminating automated attacks. The proposed methodology offers major benefits over traditional text-based CAPTCHAs, most notably language independence. By incorporating the proposed Novel Image Based CAPTCHA into existing online authentication schemes, developers can substantially reduce the likelihood of credentials-based attacks. In requiring users to solve the CAPTCHA in addition to providing a username and password, an additional dimension of complexity can be added that requires human effort. The Novel Image Based CAPTCHA point-and-click-based implementation adds this additional stage with minimum difficulty for users. It can be readily used on mobile devices since it has no language requirements and does not require a keyboard for data entry.

REFERENCES

[1] Gaurav Goswami et al., FaceDCAPTCHA: Face detection based color image CAPTCHA , Future Generation Computer Systems (2012),doi:10.1016/j.future.2012.08.013.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] H. Lee, S.-H. Lee, T. Kim, and H. Bahn, ``Secure user identi_cation for consumer electronics devices," IEEE Trans. Consum. Electron., vol. 54, no. 4, pp. 1798_1802, Nov. 2008.