



Authenticating a webpage using CAPTCHA image

R. Kanimozhi, Dr. D. Jagadeesan

Student, Assistant Professor

Dept. of Computer Science and Engineering,

Adhiparasakthi College of Engineering, Kalavai, Vellore Dist. Tamil Nadu, India

Abstract: Nowadays peoples are facing many problems while using the internet for data transaction and communications. If any transactions through the online using a particular website, they are unable to know whether the particular website is original or fake. Hence, an identification problem is major challenges if using the internet even though using secure protocols (https) or some icon in the address bar. Instead original website they using fake website make the transactions, the hacker hacking the user information and damage the resources. It is merely thought people in their further transactions, communications, etc. Hence need for a new technique to identify website is original. In this paper, we propose the new technique for identifying originality using steganography. This technique is to provide more security to the website such that even though they do transactions, viewing, etc. Using this technique, this can be provided with highly secure manner.

Keywords: Image, Steganography, CAPTCHA, Security.

I. INTRODUCTION

Security in website: Security is one of the major issues faced by the website or document which is provided on the internet. To provide quality of service (QoS) in the internet they have some basic security, such as, getting password from the user. For any transactions they acquire pin numbers etc. Even though they provide a security level provided to a website or document it can be replicated by hackers. Normally a user enters into the website they are tempted to download by different views of cookies. So well known person can easily understand the means of https or some protocols. Using this technique a normal person can just verify the website or documents with the unique image.

A. *Steganography:*

Steganography is the techniques were the different types of file can be hidden in the existing type of files. Steganography method based on the spatial domain for encoding extra information in an image by making small modifications to its pixels i.e. least Significant bit (LSB) embedding [1]. Steganography technique is used in three methods as follows,

- Text based steganography: Hiding a text file in the existing file.



Figure 1. Example for Text based steganography

- Image based steganography: Hiding the image behind the existing file.



Figure 2. Example for Image based steganography

- Video based steganography: Hiding the video file behind the existing file.

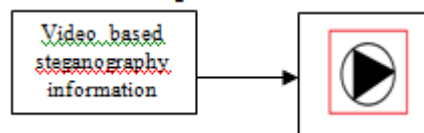


Figure 3. Example for Video based steganography

Advantages of steganography : In use of steganography were the existing file is hidden with some type of file such that it can be compressed to minimize the size of the file.

B. *CAPTCHA image:*

CAPTCHA stands for Completely Automated Turing Test to tell Computers and Human Apart. It is provided to differentiate between the humans and other remote digital entry through some software's etc. Using this we can provide security for viewing, communication, transactions etc. Thus the users can proceed further it is not needed to type the image content rather user can verify with the corresponding image as shown below [2].

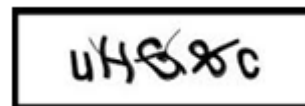


Figure 4. Example for CAPTCHA image

C. *Barcode:*

Barcode is the technique of machine readable form in which the machine can be able to find the code. In which this paper contains a barcode which is in the form of encrypted form such that if any person try them they obtain only the encrypted data [3].



Figure 5. Example for BARCODE image

II. RELATED WORKS

A. Angel Freda, et al. has to solve the problem of phishing textual keyword validation along with visual cryptography is used to increase more security “Blowfish Algorithm” can be used to divide the original image captcha into many blocks and rearrangement can be done. Then “Splitting and Rotating Algorithm” can be used to rotate the rearranged blocks [4].

Sarita Yardi, et al. has lineup works by presenting a user with photographs and asking the user to identify subjects in the photo whom a user with the appropriate identity or group membership should know [5].

T.S.Ravikiran, et al. has proposed hybrid user authentication approach combining CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) and graphical passwords to provide increased security [6].

Monica chew, et al. has proposed CAPTCHA image is also used in three basis as naming images, distinguishing images, identifying anomalous images out of a set [7].

The various other techniques used as security are, Fingerprint segmentation for secure Internet verification purposes is investigated. The novel application of computational geometry algorithms in the fingerprint segmentation stage showed that the extracted feature (characteristic polygon) may be used as a secure and accurate method for fingerprint-based verification over the Internet. On the other hand the proposed method promisingly allows very small false acceptance and false rejection rates, as it is based on specific segmentation [8].

To improve the performance of iris recognition based on stationary images using NI Lab VIEW. Region of interest segmentation and localization of iris using c any edge detection is performed [9].

For example Aadhaar card authentication uses thumb, IRIS in case of verification provided in the India.

III. PROBLEM IDENTIFICATION

In order to provide more security to users a website can be implemented with CAPTCHA image such that the website has their individual CAPTCHA image is hid with the barcode it can be in the encrypted form. So users can identify the website or document whether it is fake or original by using the CAPTCHA image if the hackers try to create the webpage of the same CAPTCHA image it makes them unable as they are registered and reports an error message if they do so. CAPTCHA image is hid with barcode which is in encrypted form and further it can be converted to hash code with the reproduced image cannot have their same hash code. Advantages for using the captcha image in a webpage or document:

- Users can identify the original webpage or documents.
- It makes difficult for creating the same captcha image.
- More secure is provided.

IV. PROPOSED WORK

A. Algorithm 1:

Steps for generating a captcha image for webpage:

Step 1 : Start the session.

Step 2 : Select the string for image i.e. “c” such that c is not in the “k” where “k” is the already registered CAPTCHA image text.

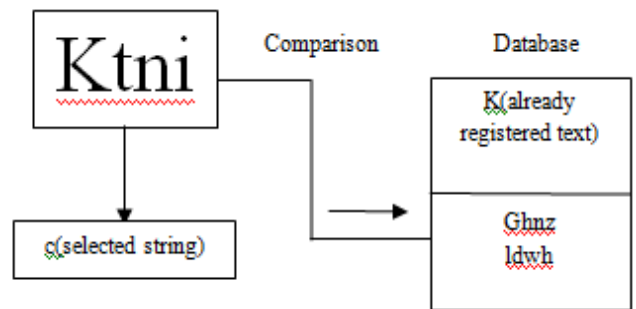


Figure 6. Comparison with database

Step 3 : If the selected string “c” is not in database then fix the text in the 120x120 pixels which contain the bytes as 14400bytes else reject the text.



Figure 7. Unmatched string

Step 4 : Then add the string “c” into the concerned register center.

Step 5 : If the hacker tries to create the same CAPTCHA image in the webpage, then report the error message as “Unable to create the webpage of usage of same CAPTCHA image”.

B. Flowchart :

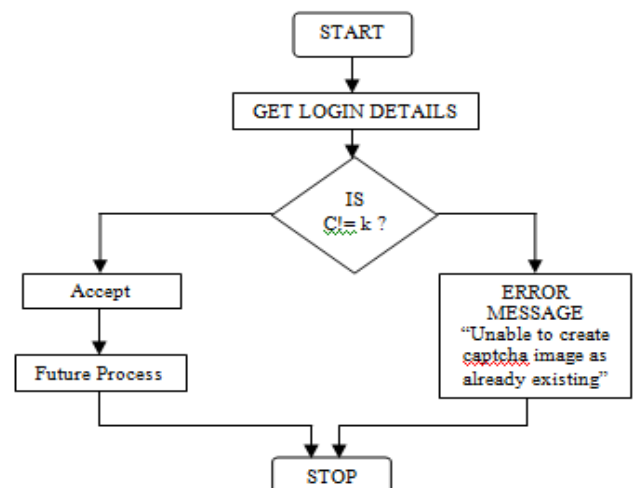


Figure 8. Flowchart for checking CAPTCHA image

C. Architecture for generating a barcode value:

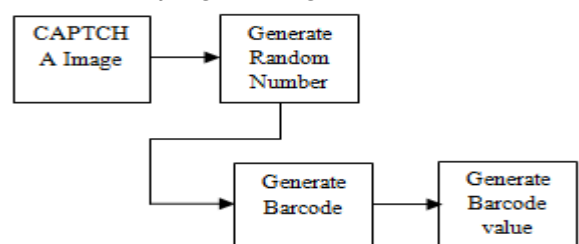


Figure 9. Architecture for generating a barcode value

D. Algorithm 2:

Steps for generating a barcode value:

Srep 1 :Convert the 120x120 pixel CAPTCHA image into the randomly generated number (hidden).

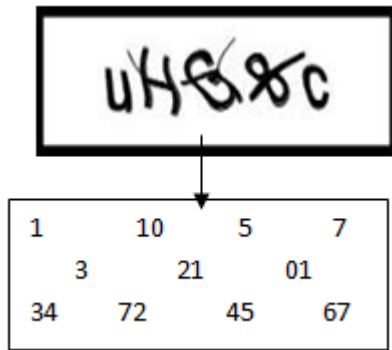


Figure 10. Generating a random number

Srep 2 :Using the random number, then convert into the barcode as hided.

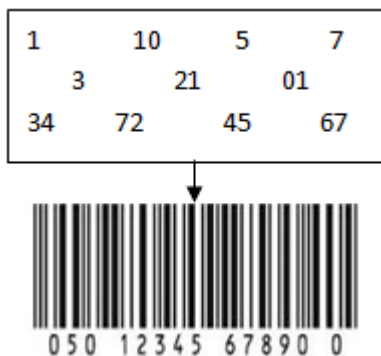


Figure 11. Generating a barcode

Srep 3 :Barcode value can be further converted into encrypted form such that the value of each number can be assigned by our own binary number of 7 bits (hided).



Figure 12 Generating a barcode value

V. RESULTS AND DISCUSSION

Using the existing concepts were the security provided to any type of transactions, viewing etc. where the security

level is maintained at the rate of highly official such that well sophisticated users understand it but this paper reveals a security logic in the form of CAPTCHA image such that more authentication, confidentiality is provided with the image.

Consider the percentage of security is of at 60-68% (approximately) existing were the new concept provides with 70-75% security it is authenticating a user personal details etc.

VI. CONCLUSIONS

Using this technique where the usage of CAPTCHA image provides more secure information in the webpage such that the user can be given authorization to the further transactions etc. In this paper were steganography is used which merely provides with more confidentiality with their respective webpage server.

VII. REFERENCES

- [1] A.E. Mustafa, A.M.F. ElGammal, M.E. ElAlmi and Ahmed. B.D (2011), "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit", Research Journal Specific education, Issue 21, pp.753-767.
- [2] "Captcha image", <http://www.somebits.com>
- [3] "Barcode image", <http://www.themobilists.com>
- [4] A. Angel Freda, M. Sindhuja and K. Sujitha (2013), "Image captcha based authentication using visual cryptography", IJREAT International Journal of Research in Engineering & Advanced Technology, Vol. 1, Issue 2, pp. 1-6.
- [5] Sarita Yardi, Nick Feamster and Amy Buckman (2008), "Photo based authentication using social networks", WOSN'08, Seattle, Washington, USA, pp. 55-59.
- [6] T.S.Ravikiran and Y.Rama Krishna (2012), "Combining CAPTCHA and fraphical passwords for user authentication", International Journal of Research in IT & Management, Vol. 2, pp.29-35.
- [7] Monica chew, J.D. Tygar and U.C. Berkeley (2004), "Image recognition CAPTCHA", In processing of the 7th International Security Conference, Springer, pp.268-279.
- [8] M.Poulos, E.Magkos, V.Chrissikopoulos and N.Alexandris, "Secure Fingerprint Verification Based On Image Processing Segmentation Using Computational Geometry Algorithms", <http://users.ionio.gr/~mpoulos/papers/Fingerprint%20verification.pdf>
- [9] Sheeba Jeya Sophia.S and Veluchamy.S (2013), "Security system based on IRIS recognition", Research Journal of Engineering Science, Vol.2, No. 3, pp. 16-21.