DOI 10.4010/2016.1286
ISSN 2321 3361 © 2016 IJESC

Research Article Volume 6 Issue No. 5

Secured CAPTCHA Password Verification Using Visual Cryptography

Prof. Ms. Shrilekha Mankhair[1], Aparna Raut[2], Monika Mohimkar[3], Kiran Sukal[4], Anushree Khedekar[5]
Department of Computer Engineering
MESCOE, Pune, India
aparnaraut94@gmail.com[2], monikamohimkar@gmail.com[3], Kiran.sukal@gmail.com[4], anushreekhedekar@gmail.com[5]

Abstract:
With the advent of internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. We are using visual cryptography algorithm for separating privileges. The use of visual cryptography is explored to preserve the privacy of an image CAPTCHA by decomposing the original image CAPTCHA into two shares (known as sheets) that are stored in separate database servers(one with user and one with server such that the original image CAPTCHA can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image CAPTCHA. Once the original image CAPTCHA is revealed to the user it can be used as the password

Keywords: Visual Cryptography, DES, LSB

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanisms should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness .The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image.

Watermarking is a major image processing application used to authenticate user documents by embedding and hiding some authenticated piece of information behind an image, audio or the video le. Video watermarking involves embedding a secret information in the video. For example, copyright symbols or signatures are often used. The traditional watermarking approach tends to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer. Nowadays more efficient and secured approach to perform watermarking is used. It is done by using sub image classification, i.e. selected frames only will contain a fractional number of total bits from the watermark image.Video watermarking is done by block based Scene change detection technique which embeds different parts of a single watermark into different scenes of a video.

-Previous Studies

Considerable number of studies was conducted by researchers on developing new CAPTCHA methods and breaking them. CAPTCHAs were originally developed by AltaVista to avoid the submission of URLs to the search engine[6]. It was a simple CAPTCHA which asks users to type a distorted English word. Carnegie Mellon designed the Gimpy method which selects a word from dictionary and asks users to type what they see as an image after rendering the distorted image containing the text [7]. Yahoo uses the simple version of this method; EZGimpy. EZ-Gimpy's image modification includes background grids, gradients, non-linear deformations, blurring, and pixel noise. Most humans can read three words from the distorted image, while current computer programs can not.

Figure 1. Some CAPTCHA words

which uses the major weaknesses of OCR systems such as the inability to recognize low quality images [8]. It contains only common English words between five and eight characters long.

PessimalPrint used only 70 words which is very low. PessimalPrint's CAPTCHA would break with the probability of 1/70. So, this method does not succeed as expected.

Hotmail is a free email service by the Microsoft Cooperation, and another CAPTCHA method is used [10]. A string of English characters is randomly selected, and after applying some changes, users are asked to type what they see.

II. SYSTEM ARCHITECTURE

System design provides the understanding and procedural details necessary for implementing the system recommended in the system study.

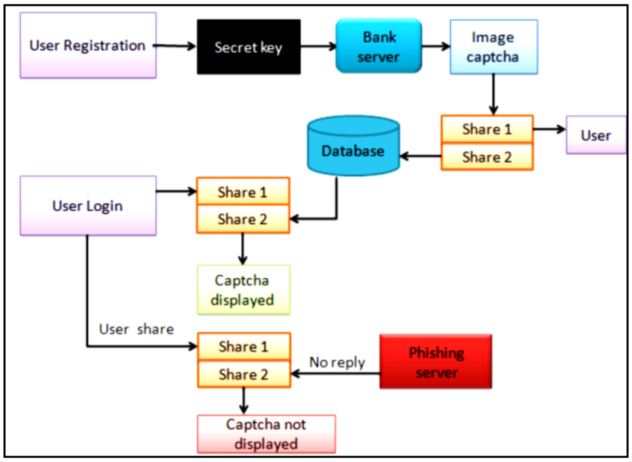


Fig.2.1.System Architecture

III. DESIGN PRINCIPLE

There are a number of important characteristics that a CAPTCHA can exhibit. These include the difficulty to be solved by OCR and any attack programs, readable common distortions, resisting malicious attacks, carrying many bits of information, the capability of coexisting with other CAPTCHAs, and little cognitive computation requirement by the user. The relative importance of these characteristics depends on the CAPTCHA type. The principles behind CAPTCHA are as follows:

- The user is presented with a garbled image on which some text is displayed. This image is generated by the server using random text.
- The user must enter the same letters in the text into a text field that is displayed on the form to protect.
- When the form is submitted, the server checks if the text entered by the user matches the initial generated text. If it does, the transaction continues. Otherwise, an error message is displayed and the user has to enter a new code.
- Exploits observation that humans are still much better than computers at many pattern recognition tasks.

IV. VISUAL CRYPTOGRAPHY

Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

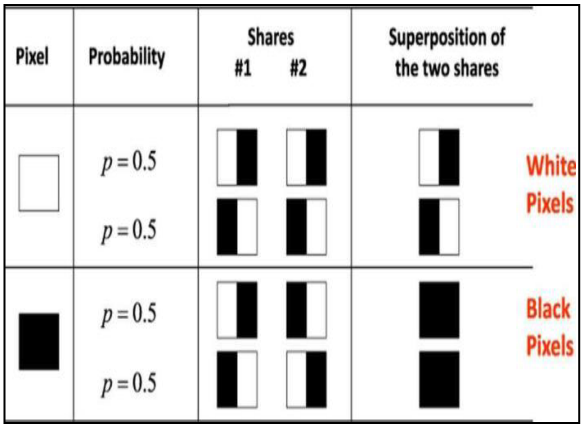
1.(2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2.(2,n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two(or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3.(n,n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4.(k,n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the Threshold,, and n, the number of participants.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.1 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixels.



IV. PROPOSED METHODOLOGY

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

The proposed approach can be divided into two phases:

A. Registration Phase
B. Login Phase
C.Watermarking Phase

A. *Registration Phase*

In the registration phase, a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha[4][5] is generated. The image captcha is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed. Registration process is depicted in Fig.3.

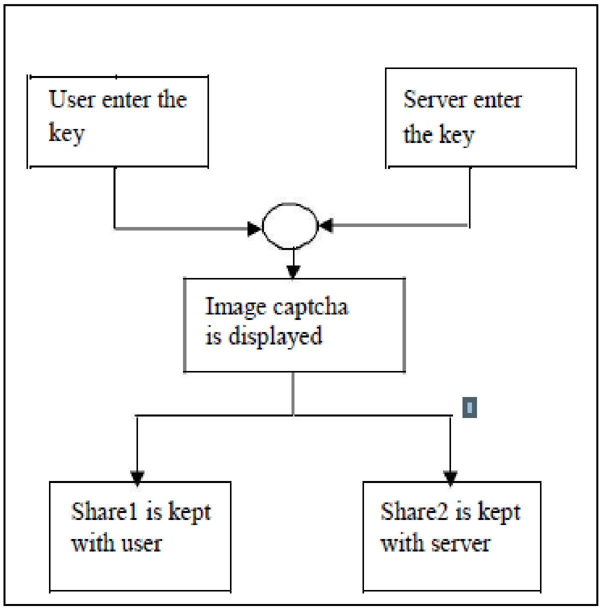


Fig.4.1 When user performs registration process for the website

B. *Login Phase*

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not. This phase is depicted in Fig.4

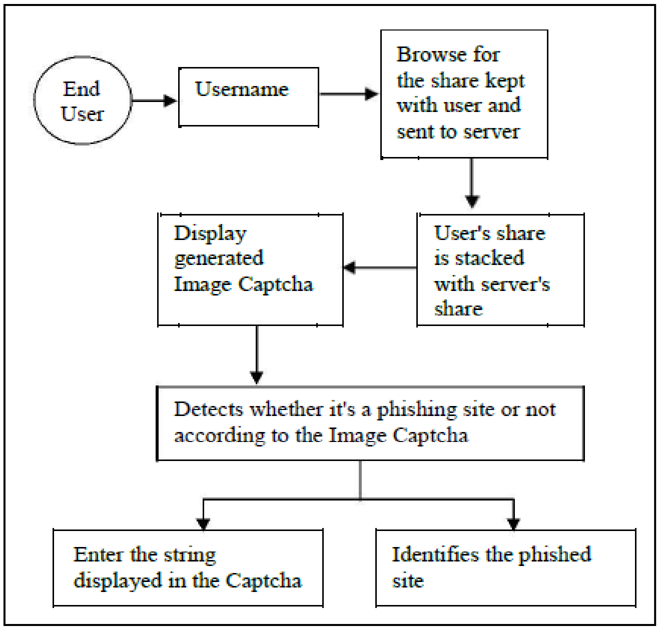

End User
Username
Browse for the share kept with user and sent to server
User's share is stacked with server's share
Display generated Image Captcha
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the Captcha
Identifies the phished site

Fig.4.2 When user attempts to log in into site

C. *Watermarking Phase*

MODULES

I)INPUT MODULE:

ii)ENCRYPTION MODULE :
1. Select Secret File,
2. Select Cover File (video, Audio), 3. Select Save Location,
4. Enter Password ,
5. Select Done

iii) DECRYPTION MODULE:
1. Select Encrypeted File,
2. select Save Location To file,
3. Enter Password,
4. Select Done

Modules Description:

i)Input Module:

The Input Module is designed as such a way that the proposed system must be capable of handling any type of data formats, such as if the user wishes to hide any image format then it must be compatible with all usual image formats such as jpg, gif, bmp, it must be also compatible with video formats such as .avi, .flv, .wmf etc.. And also it must be compatible with various document formats, so that the user can be able to user any formats to hide the secret data.

ii)Encryption Module:

In Encryption module, it consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and where the user can select the secret message. Then the user can select the image or video file through another open file dialog box which is opened when the cover file button is clicked. Where the user can select the cover file and then the Hide button is clicked so that the secret data or message is hidden in cover file using Forbidden Zone Data Hiding Technique.

iii) Decryption Module:
This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted cover file and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

V. IMPLEMENTATION & ANALYSIS

The proposed methodology is implemented . Fig 5.1, Shows the result of creation and stacking of shares.

In the registration phase the most important part is the creation of shares the image captcha where one share is kept with the user and other share can be kept with the server. for login, the user needs to enter a valid username in the given field. then he has to browse his share and process. at the server side the user's share is combined with the share in the server and an image captcha is generated. the user has to enter the text from the image captcha in the required field in order to log in into the website. the entire process is depicted in fig.5.1 as different cases.case1 and case 2 illustrates the creation and stacking of shares of two image captcha's resulting in original captcha. in case3 share1 of first image captcha(case.1) is combined with share2 of second captcha(case.2) resulting in an unrecognizable form of CAPTCHA.

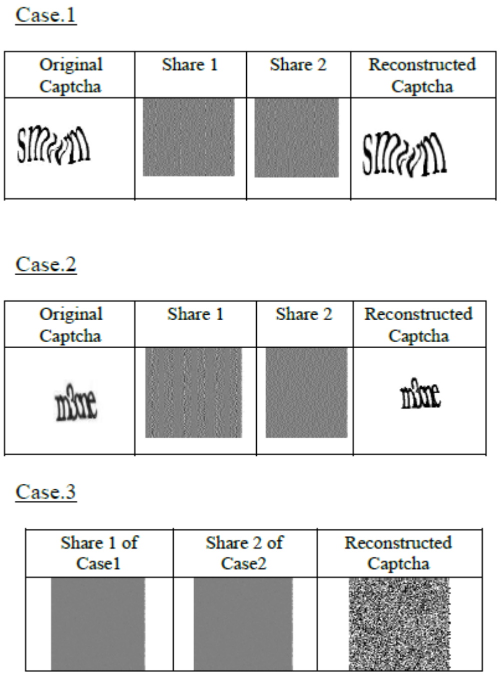


Fig. 5.1 implementation of Proposed methodology

VI.PROJECT SCOPE

Using visual cryptography the user will be able to login securely. Invalid User will not be able to login on the site. Personal and confidential information will be secure. In this, the user will be waiting for a period of time to receive the reconstructed CAPTCHA. If the user does not receive correct CAPTCHA or wrong CAPTCHA then he will not be able to login. After login user will be able to encrypt the data in the video so as to keep the data in secure form.

Conclusion

In this paper we concluded that online attacks has been increased. Here an image based authentication using Visual Cryptography is implemented. After successfully login of the system we can upload encrypted data on the system.

The process of this comprehensive video watermarking scheme, including watermark preprocessing, video preprocessing, watermark embedding, and watermark detection, is described in detail. Various improvement approaches are also presented.

References

[1] Ollmann G., The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[2] M. Naor and A. Shamir, ―Visual cryptography,‖ in Proc. EUROCRYPT,1994, pp. 1–12.

[3] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.

[4] CAPTCHA:Using Hard AI Problems For Security Luis von Ahn1, Manuel Blum1, Nicholas J. Hopper1, and John Langford.

[5] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre.

[6] Moy, G., Jones, N., Harkless, C., Potter, R., "Distortion estimation technique in solving visual CAPTCHAs", *Proc. Of the 2004 IEEE Computer Society Conference on ComputerVision and Pattern Recognition*, CVPR 2004, vol.2, 2004, pp.23-28.

[7] G. Mori, and J. Malik, "Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA", *Proc. Of IEEE CS Society Conf. on Computer Vision and Pattern Recognition*, Madison, 2003, pp. 134-141.

[8] Coates, A.L., Baird, H.S, Fateman, R.J., "PessimalPrint: A Reverse Turing Test", *Proc.of 6th Int. Conf. on Document Analysis and Recognition*, Seattle, WA, USA, 2001, pp.1154 – 1158.

[9] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, .An Innocuous Visual Cryptography Scheme,. in Proceedings of

IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.

[10] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes,. in Journal on Cryptography, vol. 12, 1999, pp. 261-289.

[11] P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with specified Whiteness Levels of Reconstructed Pixels,. Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.

[12] E. R. Verheul and H. C. A. Van Tilborg, .Constructions and Properties of k out of n Visual Secret Sharing Schemes,. Designs, Codes, *Cryptography*, vol. 11, no. 2, 1997, pp. 179-196.

[13] H. Yan, Z. Gan and K. Chen, .A Cheater Detectable Visual Cryptography Scheme,. *Journal of Shanghai Jiaotong University*, vol. 38, no. 1,2004.

.