Secured Captcha Based Authentication Using Visual Cryptography

Ankit Jain[1], Abhishek Gupta[1], Akshay Verma[1], Monica Gautam[1], Deepika Kumar[1, #]
[1]*Dept. of Computer Science, Bharati Vidyapeeth's College of Engineering, Delhi, India*

[#]Corresponding Author, Email: *deepika.kumar@bharatividyapeeth.edu*

***Abstract*— A CAPTCHA, which means, Completely Automated Public Turing test to tell the Computer and Human Apart is a test which allows only humans beings to go through. With the growth in online transactions, attacks are also increasing and desired one among them is phishing. Phishing is the effort to hack confidential information of an individual or a group of individuals. We are focusing on making CAPTCHA based password verification techniques which is made more secure using an encryption technique. Image CAPTCHA privacy is maintained by using an encryption technique i.e. Visual Cryptography. This is done by generating n number of shares (sheets) and then image CAPTCHA is separated into the n number of shares. These individual n-shares are then stored separately, with the user and the server such that the original image CAPTCHA can be revealed only when specified number of shares are available and overlaid one over the other. The server instead of relieving the CAPTCHA to the user asks for a share which is sent to the user via email at the time of registration. By using Visual Cryptography, the reliability of the process is enhanced.**

***Keywords*—Captcha, Visual Cryptography, Security, Phishing, Artificial Intelligence, Captcha Encryption.**

1. INTRODUCTION

Nowadays, most transactions are becoming online and along with it comes attempts to steal personal transaction details. Among these attacks, phishing is considered as a major threat which is increasing every day. Communications mostly appear to be from famous social media websites, auction deals, bank transactions, online payment between two parties often tempts the interest of hackers. Fake SMS or email might contain links to websites that contain malware. The threat of phishing is increasing continuously day by day. In social networking sites the threats are increasing more and more. Hackers commonly use these sites to hack into a target user or a set of users, abstract all their personal information, and then use it for their own personal benefit. Usually a regular person cannot spot the difference between a phishing website and a genuine website and once caught up in the act, his personal credentials get lost to the hacker [1-3]. Thus security in cases of online transaction should not be compromised and should be at its peak. The image processing techniques and encryption technique i.e. visual cryptography is implemented in this method.

Visual Cryptography is a technique of breaking an image into different (n number) sheets, and revealing the original image when a specific (k number) are brought together. Image processing is used to enhance the characteristics of that the input image and provide an output [5].

1.1 Previous Studies

A number of studies have been conducted in the field of CAPTCHA in order to develop new CAPTCHA methods and to break them. CAPTCHA was first used by an AltaVista (a search platform) as a means to block automated uniform resource

locator (URL) submission to their search engine [6]. Carnegie Mellon designed the Gimpy method whose more sophisticated version is used by Yahoo known as EZ-Gimpy. EZ-Gimpy's image modification made CAPTCHA more secure by including pixel noise, nonlinear deformations, background grids, blurring along with gradients [5]. Humans can identify few words but bots cannot. Some CAPTCHA words uses the biggest weakness of an OCR (Optical Character Recognition) system such as they are not capable enough to recognize low quality images. A CAPTCHA contains only five to eight English words which is generated through different processes.

Further PessimalPrint used only 70 words in their captcha and thus the probability to break PessimalPrint's Captcha is 1/70, so this was the reason this method does not do well enough as anticipated [5][7]. Another method used by Hotmail to generate CAPTCHA was selecting a random string of English characters, rearranging them and then user needed to type what they see.

2. System Architecture

System design helps one in understanding and provides the procedural details required for implementing the system in the system study.

This System contains different stages which include registration stage, login stage and generation of CAPTCHA. Each stage is important and without the completion of the prior stages, the system will not move to the next stage. All the different stages proceeded stepwise in a proper manner increases the security.

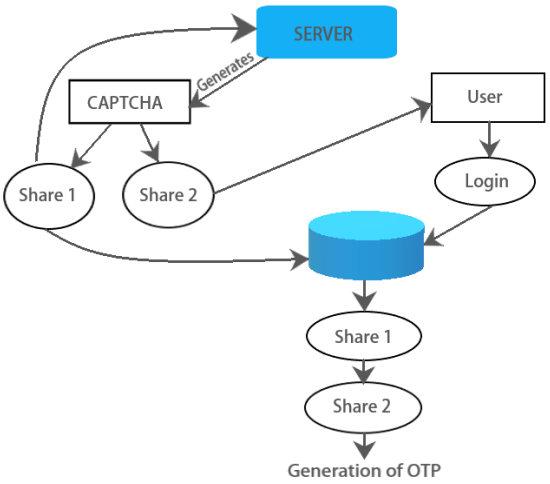

Fig.1: System Architecture

3. Design Principle

Captcha show different type of characteristics which are based on its type such as capability of coexisting with other Captchas [5], non-linear distortion including gradient and blurred background, readable ordinary distortions, resisting malicious attacks and difficulty resolved by Optical Character Recognition system.

Basic principles behind the working of Captcha are as follows:-

- The user receives a distorted image in which some random text is displayed. This text in the image is generated using different algorithms by the server.
- The user is required to enter the same letters shown in the image or the answer to a simple mathematical problem accordingly in the text field.
- When the user submits the text, the server checks whether the text entered by the user in the text field matches the initial generated text by the server. The user will be allowed to continue only if the text entered by the user matches the text generated by the server otherwise an error message is popped and user needs to enter a new and different code [4].
- Observations states that humans are generally much better in pattern recognition than computer bots.

DATABASE

4. VISUAL CRYPTOGRAPHY

Visual Cryptography is an encryption method which allows us to encrypt information like images or videos maintaining the privacy [13]. The original image should only be revealed by stacking together a specified number of shares (sheets) as per the Scheme used [15].

Methods used for Visual Cryptography are as follows:-

A. *Threshold VCS (2,2):* This is one of the beginner techniques in which the image is broken down into two different sheets [13] and in order to obtain the original image back we need both the sheets overlaid over each other. One sheet is stored with the user and the other sheet is stored with the server.

B. *Threshold VCS (2, n):* This includes the breaking down of the image into n number of sheets [13]. These n number of sheets are than stored with the user and the server accordingly. In order to obtain back the original image, 2 specific sheets are required and they have to be overlaid over each other.

C. *Threshold VCS (n, n):* Similar to the VCS (2, n) scheme, in this the image is again broken into n-sheets and the secret image is only revealed when all the n-shares are overlaid over each other [13]. The secret image will not be displayed if even one of the share is missing.

D. *Threshold VCS (k, n):* This is the most used scheme in VSC which includes breaking of a secret image into n number of share, and the original image is shown only when k number (specified) are superimposed over each other [13].Those specified number of k shares are a must else a blur and non-recognizable image CAPTCHA will be displayed.

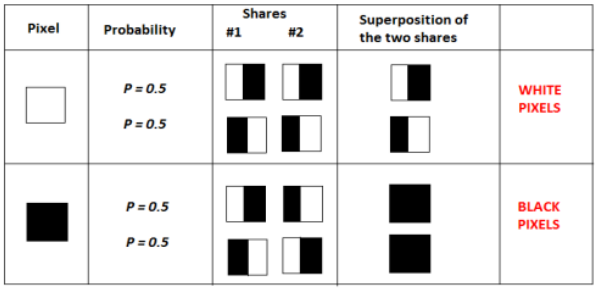

Fig. 2: (2, 2) VCS Scheme using 2 Sub-Pixel construction[11]

In the (2, 2) case, every pixel of the original CAPTCHA image goes through encryption and then it is broken down into two sub shares (sheets) consisting of black and white pixels [13]. The choice of a black pixel and that of a white is totally random based on the algorithm used. A single sheet, may it be white or black cannot provide any clue what the secret image is. We need both the sheets superimposed to disclose the true image.

5. CURRENT METHODOLOGY

In the current scenario, when a user has to access his personal information online or do a transaction, he has to login into his account using his user_id, password and then enter the card details for a transaction. But due to progress in attacking methods, this information can be easily be accessed by an attacker using a bot, phishing sites and other unethical means. To intercept such attacks and loss of personal information CAPTCHAs are generated by the server which the user has to enter in a text field during the time of login. Then the user has to follow the following steps such as type a word, solve an equation or select images accordingly (shown in Fig. 3) as asked [5]. This makes sure that person accessing the

site is not a bot and is the real owner of that specific information.

Fig. 3: Different types of CAPTCHAS

6. Disadvantage Of The Existing System

The disadvantages phased by current existing system are as follows:

1) Authentication: In this, the client and server do not get authenticated properly by the server.
2) This system does not provides enough protection from a bot created using Artificial Intelligence.
3) Security: Customer information might be shared to the merchant if bot enters, and verifies the server [8].
4) This system lacks in higher security features and could be improved to a great extend [8].

7. Implementation

For the purpose of safe login in a more secure and fast way, we are proposing a way to remove the use of CAPTCHA which is very time consuming and irritating at times. We are using visual cryptographic image share, which would be sent to the user at the time of registration via email, and the user would be required to enter that image each time to make a safe login. This increases the security during the time of login and it is sent to the register email id making sure that only the authentic user can access their personal details.

In our proposal, (Fig. 4) using the same procedure of visual cryptography in which when a specified k shares of an image is overlaid the captcha is revealed, we propose that the server rather than generating a CAPTCHA generates a email containing a share derived by the image uploaded by the user. In this, firstly the user gets registered with a trusted server. Once he has registered, during the time of login through the client application, he sends his UID to the server, the server validates it with the server share and once they match [13], [15] the server provides a safe and secured login. If both the shares don't match, login fails and the whole process of login starts from the beginning till the shares match.

This proposed method is divided into two stages:

A. Stage I: Registration Stage

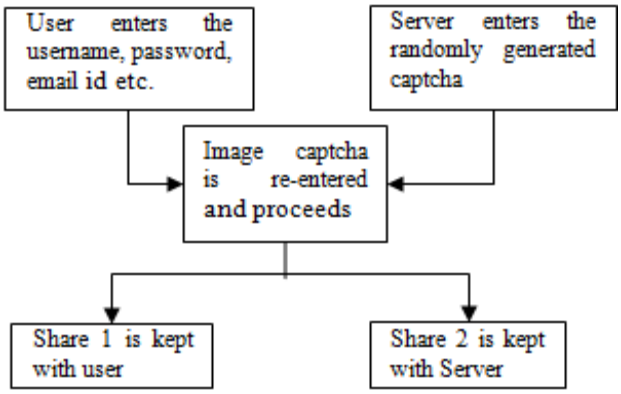

Fig 4: Registration Stage [12]

During this stage the user is requested to enter their user_id, Email id and phone number along with other necessary details. The string in the user_id could be made of alphabets, numbers and special symbols. When the user enter the log-in details, the server generates a random image CAPTCHA. The image captcha is then divided into n number of shares such that shares are split between the user and the server. The shares with the user is sent to the server for the login stage verification [12]. The shares with the server are stored in a confidential database. The whole registration stage is shown in Fig. 4.

B. Stage II: Login Stage

In the login Stage, first user has to enter user_id. Then the half share images which is kept with the user are sent to the server where the user's shares and shares are uploaded by the user during the time of login, is overlaid together to generate the image CAPTCHA. The generated image will be checked by the server and if it matches the original image which was generated during the time of registration [12]. This will complete the login stage. This phase is shown in Fig. 5.

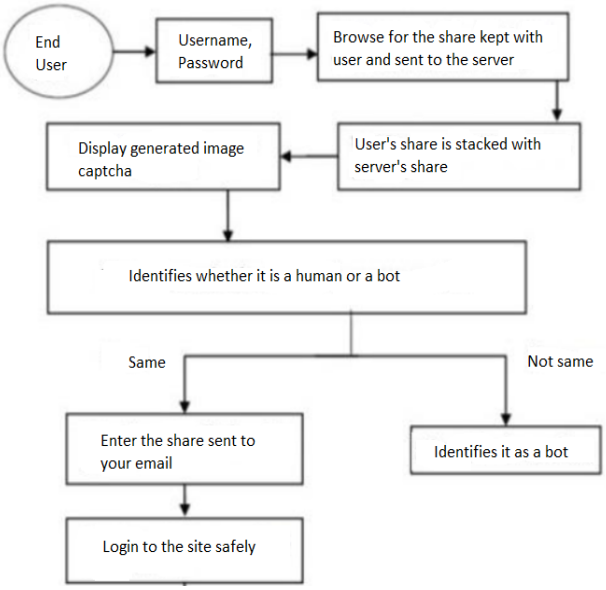

Fig. 5: Login Stage [12]

8. PROJECT SCOPE

Using visual cryptography and Email security, a user will be able to login more securely [15]. This will help to protect personal and confidential information. In this, the user will not go through the painful process of identifying the CAPTCHA or solving some mathematical equation rather the user will just have to upload the image sent to their registered email during registration phase. The process of splitting of the shares of images is totally random and it does not uses the same set of pixels to break the images. Rather it uses six different set of dividing of the shares code to do so randomly. This will help to make sure that the personal details are secured from any outside intrusion and the user is genuine and a bot. Along with it, security increases as the share would be only available to the user and the user would only be able to access the share required.

9. CONCLUSION

Due of the sudden boost to online transactions, certain attacks are becoming regular, increasing the risk of acquiring

personal details being accessed by unauthorized users [15]. With our methodology "Secured Captcha Based Authentication Using Visual Cryptography" we can simply secure online transactions. Our methodology provides better protection since each time a random set of dividing shares is chosen for the current session and visual cryptography is done to authenticate the server side which increases the security. Also the share needs to be uploaded directly during the time of login, and the share required would only be available to the user (via his registered Email). Hence it provides better security altogether.

REFERENCES

[1] Liang H., & Xue Y., "Understanding security behaviors in personal computer usage: A threat avoidance perspective", Association for Information Systems, 11(7), pp. 394–413, 2010.

[2] Nalin Asanka Gamagedara Arachchilage, Steve Love, Security awareness of computer users: A phishing threat avoidance Perspective, Computers in Human Behavior (38), pp. 304–312, 2014Yuancheng Lia et al., "A semi-supervised learning approach for detection of phishing web pages", Optik, (124), pp. 6027–6033, 2013.

[3] Anti-Phishing Working Group (APWG), Phishing activity trends report for the month of June, 2007 http://www.antiphishing.org/

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

[5] Prof Ms. Shrilekha Mankhair, Aparna Raut, Monika Mohimkar, Kiran Sukal, Anushree Khedekar,"Secured Captcha Password Verification Using Visual Cryptography", International Journal of Engineering Science and Computing, May 2016.

[6] A Text-Graphics Character Captcha for Password Authentication, Matthew Dailey Chanathip Namprempre.

[7] 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.

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

[9] Prof N.R.Jain ,Kashid Ujwal , Shaikh Apsara, Patel Nikhil, Divekar Tejashri , "Advance Phishing Detection Using Visual Cryptography And One Time Password", International Journal of Advanced Research in Science, Engineering and Technology, Vol. 3, Issue 4 , April 2016.

[10] 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.

[11] A.Vinodhini and L. Jani Anbarasi, "Visual Cryptography for Authentication Using CAPTCHA", International Journal of Computer and Internet Security.ISSN 0974-2247 Volume 2, Number 1 (2010),

[12] Kajal NanawareȦ, Kirti KanadeȦ, Manisha BhatȦ, Reshma PatilȦ and A.S. DeokarȦ, "Malicious Website Detection using Visual Cryptography and OTP", International Journal of Current Engineering and Technology, October 2014.

[13] Sneha M. Shelke, Prachi A. Joshi, " Prevention of Phishing Threats using Visual Cryptography and One Time Password (OTP)," International Journal of Science and Research (IJSR),Volume 5 Issue 2,Februaray 2016.

[14] A.Ange Freeda1, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography", International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013.

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