International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 418 – 421

E-CAPTCHA: A Two Way Graphical Password based Hard AI Problem

Sudarshan Soni[1] , Dr. Padma Bonde[2]
Shri Shankaracharya Technical Campus,
Bhilai
[1]*soni.sudd@gmail.com*
[2]*bondepadma@gmail.com*

***Abstract*—** CAPTCHA is a Turing test that people can succeed, however current PC program could not succeed. The primary motivation behind CAPTCHA is to restrict automated scripts that are posted spam content. To upgrade the security another system Enhanced-CAPTCHA(E-CAPTCHA) is going to develop which includes some new elements specifically the Novel security based Grid-Box method where high security can accomplished by including 2 level of accessing.

***Keywords*—** *CAPTCHA, Graphical Password Authentication, Hard AI Problem, Attack.*

*****

I. INTRODUCTION

Presently, security is the most basic variable an information security program for approval. The text based and Graphical passwords [1] used as a piece of the verification method, yet the best alternative for text based secret key is a graphical password. The graphical secret key can diminish the heaviness of human memory as human identity to recollect representation and picture better. Graphical passwords are feeble against shoulder surfing and spyware ambushes, mystery key, enrollment and sign in process needs more storage space. So the best differentiating alternative to graphical arrangement is CAPTCHA (Completely Automated Public Turing-test to separate Computers and Humans One from the other).

CAPTCHA is a sort of test response is delivered by a human not by a PC. It is a program that makes and grade tests that are human plausible, yet current PC projects could not comprehend it. Another security primitive specifically, a novel gathering of graphical watchword systems manufactures CAPTCHA development that was [2] referred to as a CAPTCHA as graphical Passwords(CaRP). [2] was snap based graphical passwords, in which a demand of snaps on a images used to get a mystery word. Separating other snap based graphical passwords, pictures used as a piece of CaRP was CAPTCHA challenges and another CaRP picture is made for each login. The application where CAPTCHA as a graphical mystery word include:

- CAPTCHA as graphical password can be used as a piece of various web applications especially in the e-backing application, where customers expected to understand the differing CAPTCHA at each login.
- By using the CAPTCHA as Graphical Password the collection of spam messages can reduce. Here the email specialist uses the CAPTCHA as a graphical secret key to sign into the email-id, so the spam bots could not access since they could not able to recognize the CAPTCHA.

Some system had utilized as a part of Password based innovation exist to improve the security primitives. One of the primitive used Graphical Password based Technique described below:

Graphical Password based Technique:

Graphical password methods had created to conquer the limitation of content based passwords. Graphical passwords comprise of perceiving the pictures or once in a while to perceive the picture and tap the specific focuses or zone on the picture instead of writing the characters like text based password. Along these lines, the problems that emerge from the text based passwords had diminished. Graphical Password based techniques are discussed below:

- Recognition based Plan

In Recognition based plan, user need to pick the particular number of pictures from collection of irregular pictures for validation purpose, and for approving the customer needs to recognize (see) those photos in a same demand. There are three arranges under this structure:

[3] proposed a graphical check framework depends on upon to the hash discernment system. In their system, the customer was made a request to pick a particular number from pictures from a game plan of arbitrary pictures made by a

program. The client required to recognize the preselected pictures with a particular true objective to be validated.

[4] used a graphical password plot work with the surfing shoulder issue. In the essential methodology, the system will exhibit different passes-objects. A customer needs to see pass-protests and snap inside the outside edge formed by all the pass-objects for confirmation.

Pass face was Real User Corporation developed these techniques. The idea behind this was to the accompanying: The client asked to pick four pictures from human confronting as their future password security. In verification arrange, the client sees a network of nine confronts, comprising of one face past picked by the client and eight decoy faces. The client recognizes and clicks anyplace on the known face. This strategy repeated for a few rounds.

- Recall based Plan

A recall based arrangement required a customer to repeat something that he made or picked before amid the enrollment stage. Three techniques were:

In Draw-A-Secret (DAS) Scheme the customer need to draw an essential picture on 2D network. The bearings of a network was included by the photograph are secured in the demand of the drawing. For the approval, the customer will be encouraged to re-draw the photograph. In case the drawing touches a comparative arrangement, then the customer is confirmed.

In Signature Scheme approval was driven by having the customer drawing their sign using the mouse.

In Pass-point Scheme the customer was tap on wherever on a pictures to make a secret key. A resistance around each picked pixel was ascertained. Remembering the true objective to be approved, the client must click inside the tolerances in the sequence [5].

- Cued Review based Plan

In a Cued Review based Plan Pass Points [5] was a click based signaled review plot where a customer requires clicking a sequence of focuses to wherever on a photo to make a secret key. At the time of verification customer require to re-clicking a comparative arrangement. Cued Click Points (CCP) [6] resembled Pass Points however uses one picture for each snap, with the accompanying picture picked by a deterministic limit. Persuasive Cued Click Points (PCCP) extend CCP where customer needs to pick a point inside a randomly situated viewport. Graphical password has a couple of obstacles. one of that was Password registration and sign in process take too long and furthermore Required more storage space than content based passwords.

II. RELATED WORK IN CAPTCHA

Complete Automated Public Turing Test to distinguish Computers and Human One from the other [6] (CAPTCHA) finds the distinction in people and computer scripts in taking care of the hard AI issues. It is a test to check client is Human and not a computer device.

CAPTCHA has two sorts: Text CAPTCHA, which is acknowledgment of non-character objects and Image Recognition CAPTCHA depend on acknowledgment of Images.

Text CAPTCHA: PayPal and Microsoft CAPTCHA are both depended on background noise and arbitrary character strings to restrict the automated attacks. The CAPTCHA utilized by Google, Yahoo! all offer comparable properties, for example, an absence of background noise of distortion for a character or word pictures and outrageous swarming for a nearby character. Random CAPTCHA pictures had caught humanly dependably by site as pixel, marginal probabilities and site by site covariance. EZ-Gimpy utilizations word pictures which utilize character distortion and clutter. Individual print utilizes a low quality picture by degrading parameters to thicken, group, piece and add noise to character pictures.

Image Recognition CAPTCHA: CAPTCHA comprise of combination of pictures [7]. The client needs to recognize the pictures given to him to taking care of the given puzzle issue. Client needs to choose the pictures as the password characters. Image recognition has a few limitations: such as Image recognition some of the time extremely hard to read. Image recognition CAPTCHA not compatible with clients with incapacities. Image recognition is time-consuming to decipher, And It is significantly upgrade Artificial Intelligence.

III. REVIEW WORK

The related works from first existence to current primitives of CAPTCHA security are shown below:

[8] had discussed both CAPTCHA and password in a user authentication protocol, as a *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks. Discussed in [9] two distortion estimation techniques that solved EZ-Gimpy and 4-letter Gimpy-r CAPTCHAs through object recognition with a high degree of success. Using this technique user can achieved a success rate of 99%. In the case of Gimpy-r a success rate of 78% was achieved by deploying a direct distortion estimation algorithm that was able to correctly identify the four lettered Gimpy-r CAPTCHA.

[10] had done a thorough study of visual CAPTCHAs which are available at captchaservice.org. It is a website that provides services for CAPTCHA generation publically which had sophisticated distortions and were meant to be resistant to OCR attacks. Presented in [11], a character segmentation technique to attack a number of text CAPTCHAs, including those designed and deployed by Yahoo, Microsoft and Google. Specifically they have targeted the Microsoft CAPTCHA which had been deployed since 2002 at a number of their own internet services including Windows Live, MSN

and Hotmail. They implemented the attack in Java on an ordinary desktop computer (with a 1.86 GHz Intel Core 2 CPU and 2 GB RAM). CAPTCHA proposed in [12] based on Image Orientation; The presentation of a new CAPTCHA which is based on identifying an image's upright orientation. This task requires analysis of the often complex contents of an image, a task which human usually perform well and machines generally do not.

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords [13].

A typical scheme is Pass faces [14] wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted.

[15] proposed a novel anti-bot mechanism called Necklace CAPTCHA for securing online social networks(OSNs) against the Social Bots. Social bots that exactly acts as the social behaviors such as auto-Likes, auto-photos/videos sharing, auto-sending friend requests, or auto-joining to strange groups. The effects of these dangerous bots is to perform those malicious activities reflects a big vulnerability in the authentication system of OSNs.

[16] had designed to prevent the system and machine from automatically identify, the code image has a lot of interference, such as inference lines, noise, distorted, twisted, and so forth. Technical and Background of validation code recognition is mainly based on image processing and pattern recognition techniques. That is prior to preprocess the image before the code image recognition, wherein the image pre-processing technology includes binaryzation, a gray-scale image, denoising, character segmentation, tilt correction, and normalization,etc; [17] had discussed about features of various CAPTCHA, methodology used on that CAPTCHA and Its limitations. In [17] the various CAPTCHA discussed are mainly text CAPTCHA, image based CAPTCHA and graphical password based CAPTCHA.

The CAPTCHA had following few limitations:

1. The Text CAPTCHA takes more time to succeed it CAPTCHA test.
2. Text CAPTCHA become easily breakable from the bot.
3. Image CAPTCHA holds limited contents in the in any single image easily breakable.
4. Some CAPTCHA becomes difficult even for human user due to its complex accessing requirements.

IV. E-CAPTCHA TECHNIQUE

A new security primitive of novel family based hard AI technique developed, namely graphical password systems built on top of CAPTCHA technology, which is called as E-CAPTCHA. This Research provides Security by two different Security Approaches namely Motion Pattern CAPTCHA Security and CAPTCHA Grid-Box method.

Motion pattern CAPTCHA:

In Motion Pattern CAPTCHA, The user needs to draw the specific pattern presented by the AI model. By drawing Motion Pattern CAPTCHA user can succeed CAPTCHA test.

The user has to draw the specific shape provided by the system. The model can generate many types of motions pattern randomly one at a time. User has to pass the test to successfully bypass the security system.

CAPTCHA Grid-Box Technique:

In Grid-Box, the system shows some graphical contents to the user. This technique works in 2 level for E-CAPTCHA. In level 1 namely Animal-Grid-Box, The user has to select the relevant image asked by the system from Given Grid-Box. The images presented will arranges in the grid form. One grids holds one image. There are multiple grid present. After selecting the required image from Animal-Grid-Box, the system presents another grid of level 2 namely Number-Grid-Box, which is having number into it. The user need to enter the count of left over grids after selection from Animal-Grid-Box.

V. RESULT AND DISCUSSION

In E-CAPTCHA mechanism motion Pattern CAPTCHA takes very less time as compared to other existing mechanism. To compare the time here is a table in which, the time need to access CAPTCHA are shown below:

Table: Comparing Response Time of various Text CAPTCHA with E-CAPTCHA

Sr. No.	CAPTCHA Name	Response time (sec)	E-CAPTCHA Name	Response time(sec)
1.	Number	4	Star	4
2.	Simple Text	6	Cross	3
3.	Alphanumeric	6	Arrow	4
4.	Mixed	7	Circle	4

The average time taken by various Text Based CAPTCHA =5.75 sec. Similarly the average time taken by motion pattern

CAPTCHA =3.75 sec. Time reduced to access motion pattern CAPTCHA is =5.75-3.75= 2 sec. This result shows that motion pattern CAPTCHA's response time is less that other text based CAPTCHA.

Also Grid-box-method takes reasonable amount of time but ensures security in the web. Proposed Grid-Box-method ensures a very new concept, the similar concept based approaches does not exist in any previous paper so comparison with any previous methodology could not be possible. But it is best approach to enhance the CAPTCHA security options. In Grid-Box two security level consists confuse the automated script or bot in selecting of image and also in counting of images from grids.

VI. Conclussion

In early days, an increasing number of public web services have made an attempt to prevent from exploitation by bots and automated scripts, by need of a user to solve a Turing-test issue commonly known as a CAPTCHA (Completely Automatic Public Turing test to tell Computers and Human Apart) before using the service. The E-CAPTCHAs, drawing pattern CAPTCHA takes very less time as compared to other existing mechanism. While Grid-Box technique takes reasonable amount of time but ensures security in the web. Both E-CAPTCHA mechanism, which can be compared with respect to time and security with other models give better results as compare to all existing techniques.

References

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no.4, 2012, New York NY USA.

[2] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, " Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" , IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014.

[3] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000,.

[4] Sobrado, L and Birget, J. "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, Duluth MN USA, jul 2005,pp. 102–127.

[6] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007,

[7] P. C. van Oorschot and J. Thorpe, "On predictive models and user drawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008.

[8] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 18-22 Nov. 2002, Washington DC USA, pp. 161–170.

[9] Moy G., Jones N., Harkless C., Potter R.,"Distortion estimation techniques in solving visual CAPTCHAs", IEEE CVPR, pp. II-23-II-28, Vol. 2l, 2004

[10] Ahmad Salah El Ahmad, Jeff Yan,"Breaking Visual CAPTCHAs with Naïve Patter Recognition Algorithms", IEEE Computer Security Applications Conference, Dec 2007, Miami Beach FL USA ,pp. 279- 291,.

[11] Jeff Yan, Ahmad Salah El Ahmad,"A low-cost attack on a Microsoft captcha", Proceeding of the 15th ACM Conference on Computer and communications security, October, 2008,Tacoma WA USA, pp. 543-554.

[12] Rich Gossweiler, Maryam Kamvar and Shumeet Baluja, "What's Up CAPTCHA? A CAPTCHA Based on Image Orientation", ACM 2009,20-24 April 2009, New York NY USA, pp. 841-850.

[13] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4,4 Aug. 2012, New York NY USA.

[14] 2012, Feb. *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[15] Mohamed Torky, Ali Meligy, Hani Ibrahim, "Securing Online Social Networks against Bad bots based on a Necklace CAPTCHA Approach." 2016, IEEE 12th ICENCO,Giza Egypt, pp. 158-163.

[16] Gaihuan An, Wanjun Yu, "CAPTCHA Recognition Algorithm Based on the Relative Shape Context and Point Pattern Matching" 2017, 9th International Conference on Measuring Technology and Mechatronics Automation, 14-15 jan 2017, Changshu Hunan China, pp 168-172.

[17] Sudarshan Soni, Padma Bonde,"CAPTCHA: A Security Review" jun 2017, International Journal of Computer Applications, New York USA.