CAPTCHA as Graphical Password: A Novel Approach to Enhance the Security in WWW

Parul Jadon, Darpan Anand, Jayash Sharma

Department of Computer Science Engineering, Hindustan Institute of Technology and Management, Agra, (U.P.) India

***Abstract*—This research aims to study the existing password scheme and to design and develop a new improved graphical password scheme. A novel protection primitive is presented in view of strong AI problems namely a new family of graphical password scheme built up on top of captcha technology, which we call Captcha as graphical password (CaRP). CaRP is both a captcha and graphical password scheme. CaRP addresses number of security issues altogether for example, online guessing attacks, relay attacks and if combined with dual-view technologies shoulder-surfing attacks. CaRP likewise offers a novel way to deal with address the notable image hotspot problem in well-known graphical password systems for example, Pass Points.**

***Keywords*— CaRP; Captcha; Graphical password; Securities**

I. INTRODUCTION

Presently a days, validation is the central procedure to ensure data security and the most widely recognized and simplest strategy is password authentication [1]. Conventional alphanumeric passwords are series of letters and digits, which are simple and natural to all clients. Nonetheless, there are a few inborn imperfections and lacks in alphanumeric passwords, which effectively advance into security issues. Today clients have numerous passwords for PCs, informal communities, E-mail and so on. They may choose to utilize one secret word for all frameworks to diminish the memory load, which decreases security [2, 3]. Alphanumeric passwords are defenseless against shoulder surfing attack, spyware attack and social engineering attack and so on. Propelled by the guarantee of enhanced secret word ease of use and security, the idea of graphical passwords was proposed in 1996 [4].The primary objective of graphical passwords is to utilize pictures or shapes to supplant content, since various intellectual and mental reviews exhibited that individuals perform far superior when recollecting pictures than words. Our own reports or passwords are hacked by the third individual normally called programmers. There are distinctive courses for giving security. Here what we presented is one of the techniques for the security reason. Another insurance primitive is demonstrated in light of hard AI inconveniences, to be specific, another group of graphical password scheme based on top of Captcha innovation, which is known as Captcha and Graphical Password (CaRP). The vigor of CAPTCHA is found in its quality in opposing programmed antagonistic assaults, and it has numerous applications for down to earth security, including free email services, online polls, and search engine bots, forestalling dictionary attacks, worms and spam [4]. Combination of CAPTCHA as well as graphical password initiative a new type of security feature which is known as CaRP. In CaRP, another picture is produced for each login endeavor notwithstanding for a similar client. CaRP utilizes a letter set of visual items (e.g., alphanumerical characters, comparable creatures) to produce a CaRP picture, which is additionally a Captcha challenge.

II. RELATED WORK

A. Graphical Password

The term graphical password was initially presented by Greg Blonder in 1996. Graphical password is the password where client set his/her password as image or picture. Graphical password word plans have been proposed as a conceivable contrasting option to alphanumeric schemes, inspired mostly by the way that people can recollect image effortlessly than content; mental reviews backings such presumption. They can be classified into three categories as per the errand required in remembering and entering passwords: recognition, recall, and cued recall [5].

a. Recognition based

A recognition-based scheme requires distinguishing among decoys the objects belonging to a password portfolio. An unmistakable scheme is: Pass faces where a client picks a component of appearances or faces from a database in giving ascent a password. Amid affirmation, a board of applicant countenances is appeared for the client to choose the face setting off to her capacity. This procedure is iterated different assaults, each round with a different board. An effective login calls for right choice in each round. The band of images in a panel remains the same between logins, yet their positions are permuted [6]. Déjà vu plot the Dhamjia et al. proposed Déjà vu, where clients or users will choose a specific number of art image from a set of pictures generated by a system in the registration phase. Amid confirmation, the system shows a testing set blends with password and some decoy image. The use must recognize the password pictures [7]. Story is like pass faces yet the pictures in the portfolio are requested, and a client must distinguish her portfolio images in the correct request [8].

b. Recall based

At the time of authentication a use is made a request to imitate or choose something which he create or chose amid the registration step. Draw-A Secret [9] (DAS) was the starting recall based system proposed. A client draws her password on a 2D grid [10].The system encodes the order of grid cells along the drawing course as a client drawn password.

c. Cued recall based

This is also known as click based technique. In this method user gives a picture / images or set of images and user need to choose click point on that images as the password. User will effectively validate by entering correct click point and request of that point [7.] Pass Points is a generally contemplated click-based signaled cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks a similar arrangement amid authentication [11]. Cued Click Points (CCP) is like Pass Points yet utilizes one image for every click, with the next image chose by a deterministic function [12].

B. Captcha

Captcha is a program that can produce and grade tests that: (A) most people can pass, however (B) current PC programs can't pass. Such a program can be utilized to separate people from PCs [6]. There are two sorts of visual CAPTCHA: Text CAPTCHA and Image Recognition CAPTCHA (IRC). Text captcha is recognition of character. It contain trouble to comprehend character. What's more, image captcha depends on recognition of non-character object [13].

III. CAPTCHA AS GRAPHICAL PASSWORD

Bib B. Zhu, Jeff Yan,et. al. [14] proposed CaRP scheme. In CaRP i.e. CAPTCHA as graphical Passwords, CAPTCHA and graphical password is joined and utilized as a solitary element for confirmation. CaRP is click based graphical secret word or password system, where an arrangement of click on pictures/image is utilized to characterize a password and for each login endeavor another CaRP image is created. CaRP image generate, which ends up being a CAPTCHA challenge for the user. Nowaday's captcha and a graphical password together can be connected on touch screen mobiles because writing passwords is hectic, particularly for secure utilizations of Internet, for example, e-banks for login sessions.

CaRP can be classified into (1) Recognition based and (2) Recognition-Recall.

IV. RECOGNITION BASED CARP

In this system, uncounted number of visual Recognition-based for this sort of CaRP, a password is an arrangement of visual questions in the letters in order Per perspective of conventional recognition based graphical passwords, recognition-based CaRP appears to have admittance to a limitless number of various visual objects. There are three recognition-based CaRP scheme:

A. Click Text

Click Text is a recognition-based CaRP scheme worked with respect to top of text Captcha. It utilizes text CAPTCHA as its underlying principle. Alphabet in order set of Click Text contains alphanumeric characters. Its alphabet comprises characters without visually-confusing characters. For example, Letter "O" and digit "0" may bring about disarray in CaRP images, and in this manner one character ought to be avoided from the letter set. A Click Text password is a sequence of characters in the alphabet e.g., ρ ="DE@F2SK78", which is like a content password.

A Click Text image is unique in relation to regular CAPTCHA as here every one of the characters of letter set are to be incorporated into the picture as appeared in Fig.1.

Fig. 1 Click Text image with 33 characters [15]

B. Click Animal

Captcha Zoo is a Captcha scheme which utilizes 3D models of dog and horse to produce 2D animals with various texture, color, lightings and poses, and arranges them on a jumbled background. A user click all the horses in a challenge to pass the text. Fig.2 demonstrates a specimen click image challenge with 10 animals wherein every one of the horses are surrounded be red circle. Click Animal is a recognition-based CaRP scheme built on top of Captcha Zoo, with an alphabet of similar animals such as dog, horse, pig, etc. Its password is a sequence of animal names such as ρ = "Turkey, Cat, Horse, Dog," For each animal, one or more 3D models are built [14].

Fig. 2 Click Animal image with Horse Circled red [16]

C. Animal Grid

It is a combination of Click A Secret (CAS) and Click Animal. In this framework, firstly Click Animal image is shown, after the animal is chosen, an image of n*n grid shows up.

Fig. 3 Click Animal images (left) and 6x6 grid (right) [17]

V. RECOGNITION BASED CARP

In this system, sequence of some invariants points of objects is the password. Points are the invariant points of object that has a fixed relative value in different fonts. User must identify the object image and then use identified objects as a cue to locate a password within a tolerance area. Recognition recall CaRP techniques are Text Points and Text Point4CR [18].

A. Text Points

Characters contain invariant points. Fig.4 demonstrates some invariant points of letter "A", which offers a solid cue to remember and find its invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of inner invariant point of characters is chosen to form a set of clickable points for Text Points.

Fig.4 Some invariant points (crosses) of "A" [15]

B. TextPoint4CR

Text Points can be changed to fit challenge-response authentication. This adjustment is called Text Points for Challenge-Response or TextPoints4CR. Not at all like Text Points wherein the authentication server stores a salt and a password hash value for each account, has the server in Text Points 4 CR stored the password for each account. Another distinction is that each character seems just once in a TextPoints4CR image but may appear multiple times in a Text Points image. This is because both server and customer (client) in TextPoints4CR ought to produce a similar grouping of sequence of discretized grid-cells independently.

VI. AUTHENTICATION PROCESS IN CARP

CaRP schemes having additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). CaRP schemes in user authentication is as follows:

I. Enter ID and send it to Authentication server AS.
II. AS Stores a salt and hash value H (P, S) for each ID.P is the user password and it is stored.
III. Upon receiving login request, AS generates a CARP image. It records location of characters or animals in image and the image is sent to the user.
IV. User Clicks the Password.
V. Co-ordinates of points are recorded are sent to AS.
VI. AS maps these Co-ordinates & recovers clickable points of object P, that user clicked.
VII. Then AS retrieves salt s of account &calculate its hash value with salt using algorithm like SHA-1.
VIII. IT compares result with hash value stored for the a/c.
IX. Authentication is successful if and only if the two hash value matched [19].

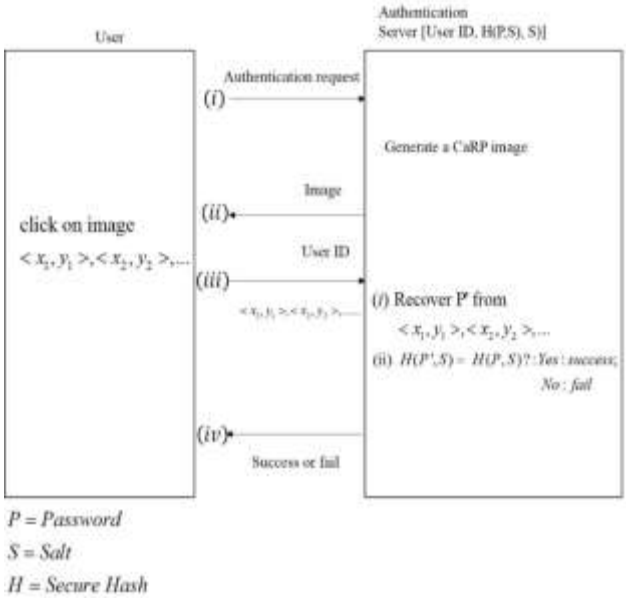

Fig. 5 Flowchart of basic CaRP authentication [14]

VII. SECURITY ANALYSIS

A. Automatic Online Guessing Attacks

In automatic online guessing attacks, the experimentation procedure is executed consequently though dictionaries can be built physically.

B. Human Guessing Attacks

In human guessing attacks, humans are used to enter passwords in the trial and error process. Humans are much slower than computers in mounting guessing attacks.

C. Relay Attacks

Relay attacks might be executed in a few ways. Captcha challenges can be transferred to a high-volume Website

hacked or controlled by enemies to have human surfers solved the challenges keeping in mind the end goal to keep surfing the Website, or relayed to sweatshops where people are hired to solve Captcha challenges for small payments.

D. Shoulder-Surfing Attacks

Shoulder-surfing attacks are a threat when graphical passwords are entered in a public place, for example, bank ATM machines. CaRP is not vigorous to shoulder-surfing attacks without anyone else. Be that as it may, joined with the accompanying dual- view technology, CaRP can thwart shoulder-surfing attacks.

E. Dictionary Attack

In this attack, an attacker tries to figure the password from a list of words, dictionary. Dictionary will be the gathering of all high probability passwords based on past determinations.

TABLE I. Attack Comparison in Graphical Password and CaRP [20]

Name of attacks	Graphical Password						Captcha as graphical Password
	Recognition Based			Recall Based	Cued Recall Based		
	Deja Vu	Pass Faces	Story	DAS	Pass Points	CCP	
Shoulder-surfing	Y	Y	Y	N	N	N	N
Online Guessing	Y	Y	Y	N	Y	N	Y
Relay	-	-	-	-	-	-	Y
Human Guessing	-	-	-	-	-	-	N
Online dictionary	N	Y	N	N	N	N	Y

Table 1 summarizes the security of the different graphical password schemes and CaRP we analyzed. 'Y' means Yes, that it is resistant to that form of attack. 'N' means No that the scheme is open to attack.

VIII. PERFORMANCE ANALYSIS

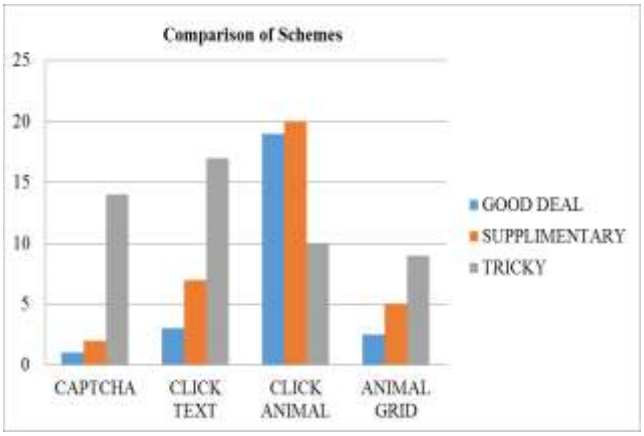

Fig. 6 Comparing different schemes for Ease of Use [14]

Above figure 6 shows the comparison results of different scheme for ease of use as a password system. CaRP system is user friendly, easy to use.

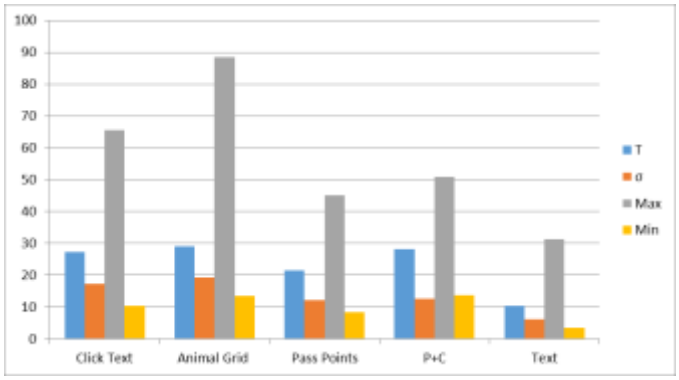

Fig. 7 Login Time for Different Scheme [14]

T : Average σ : Sample Standard Deviation Max Min

IX. CONCLUSION AND FUTURE SCOPE

We have proposed CaRP, another security primitive depending on unsolved hard AI issues. CaRP is both a Captcha and a graphical password scheme. The thought of CaRP presents another group of graphical passwords, which embraces another way to deal with counter online guessing attacks: another CaRP image, which is likewise a Captcha test, is utilized for each login endeavor to make trials of an online guessing attack computationally free of each other. A password of CaRP can be discovered just probabilistically by automatic online guessing attacks including brute-force attacks, a coveted security property that other graphical secret word plans need. Hotspots in CaRP pictures/image can never again be abused to mount automatic online guessing attacks, an inborn powerlessness in numerous graphical password systems. CaRP strengths foes to fall back on altogether less effective and a great deal more exorbitant human-based attacks .Notwithstanding offering security from online guessing attacks, CaRP is additionally impervious to Captcha relay attacks, and, if joined with dual-view technologies, shoulder-surfing attacks. CaRP can likewise help diminish spam email sent from a Web email service. Our convenience investigation of two CaRP scheme we have executed is empowering. For example, more members considered Animal Grid and Click Text easier to use than Pass Points and a combination of text password and Captcha.

REFERENCES

[1] K. Renaud. "Evaluating authentication mechanisms". In L.Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.
[2] G. Blonder. "Graphical passwords". United States Patent, 5,559,961, 1996.
[3] B. Kirkpatrick. "An experimental study of memory". Psychological Review, 1:602-609, 1894.
[4] S. Madigan. "Picture memory". In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[5] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, 44, 4, 2012.
[6] Rashmi B J, Prof. B Maheshwarappa."Improved Security Using Captcha as GraphicalPassword" IJARCCE , 4, 2015.
[7] Shraddha S. Banne , Prof. Kishor N. Shedge."CARP: CAPTCHA as A Graphical Password Based Authentication Scheme"IJARCCE , 5, 2016.
[8] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in Proc. USENIX Security, 1–11, 2004.
[9] T. S. Ravi Kiran , and Y. Rama Krishna."Combining captcha and graphical passwords for user authentication‖" International Journal of Research in IT & Management, 2, 4, 2012.
[10] NayanGawande. **"**Merging CAPTCHA And Graphical Password On NP Hard Problems In AI: New Security Enhancing Technique" IJSR , 3, 2014.
[11] 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, 63, 102–127, 2005.
[12] S. Chiasson, P. C. van Oorschot, and R. Biddle. "Graphical password authentication using cued click points," in Proc., ESORICS, 359–374, 2007.
[13] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA: Using Hard AI Problems for Security." Proceeding 2003.
[14] Bin B.Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu. "Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems." IEEE TRANSACTIONS ON INFORMATION FORENSIS AND SECURITY, 9, 6, 2014.
[15] Gubbala Jahnavi Deepika, DDD Suri Babu, "A noval approach for captcha as graphical password using a new safety primitive based on hard AI problems" , IJCSMC,4,2015.
[16] Murugavalli S, Jainulabudeen SAK, Senthil Kumar G, Anuradha D,"Enhancing Security Against Hard AI Problems in User Authentication UsingCaptcha as Graphical Passwords" Journal of Global Research in Computer Science, 7, 2016.
[17] Mrs. Anuradha. V, Mr.M.Nagesh, Mr.N. Vijaya sunder sagar," A Survey on Graphical Passwords in Providing Security", International Journal of Advanced Engineering and Global Technology, 3, 2015.
[18] ShraddhaS.Banne, Prof. K.N.Shedge,"A Review Graphical password Based Authentication Scheme",International Journal of Science & Research(IJSR), 3 , 2014.
[19] M. M. VamsiPriya, SushmaNallamalli, D. Bhanu Prakash, Ramya Sri "Authentication Using CAPTCHA as Graphical Password", International Journal of Advanced Research in Computer Science and Software Engineering, 5, 2015.
[20] Saranya Ramanan, Bindhu J S ,"A survey on different graphical password authentication techniques", International Journal of Innovative Research in Computer and Communication Engineering", 2, 2014.