Volume 7, No. 5, May 2016
Journal of Global Research in Computer Science
RESEARCH PAPER
ISSN-2229-371X
http://rroij.com/global-research-in-computer-science.php

Enhancing Security Against Hard AI Problems in User Authentication Using Captcha as Graphical Passwords

Murugavalli S[1], Jainulabudeen SAK[2]*, Senthil Kumar G[2], Anuradha D[2]
[1]HOD/Professor, Department of CSE, Panimalar Engineering College, Chennai, India
[2]Assistant Professor, Department of CSE, Panimalar Engineering College, Chennai, India
jainulabudeen_sak@yahoo.com

Abstract:
Information and computer security are supported by the passwords, as passwords play a vital role in authentication process. The traditional authentication method uses text- based passwords, which is also called as alphanumeric passwords, is not reliable in data security, and to overcome these drawbacks, graphical password scheme is introduced as an alternative to text-based passwords. But graphical password scheme is vulnerable to shoulder surfing attacks, spyware attacks. To overcome this vulnerability of graphical passwords, an emerging technique CAPTCHA, as a challenge response test is generated to distinguish humans from bots in authentication. To ensure security on hard AI problems, CAPTCHA as graphical Password (CaRP) scheme is introduced as an alternative method to textual CAPTCHA's. As CaRP scheme has scope of refinements in cyber security a two-way authentication method is proposed in one of the CaRP techniques of Recognition-based scheme.

Keywords- Textual CAPTCHAs, Authentication, Shoulder surfing attacks, Cyber security, CaRP

INTRODUCTION

Information Security is an important factor in security systems nowadays. The security of the systems is provided by the user authentication. Authentication is the process of verifying the identity of a particular person to ensure security in any security systems. The most famous method is password authentication. A user gaining access into any security system should be validated by an authentication followed in that system. This secure authentication primitive is now almost used in all online transactions (such as accessing email accounts, entering a secure vault and so on). When that sensitive information is accessed under unauthorized user, the entire security of the system will collapse and become unreliable. Hence for this secure authentication purpose conventionally we made use of the textual passwords which is also called as alphanumeric passwords. These alphanumerical password [1] can be personal names of family members, phone number, pet name etc., and vulnerable to various attacks like password guessing, dictionary attacks, spyware attacks etc., and hence found that the textual passwords are inefficient to resistant some security and usability problems. This short come in alphanumerical passwords led to the development of graphical password schemes [2]. The graphical password scheme uses images as password to remember easily than text.

The images and password space used in the graphical password technique is large enough, and thus can offer resistance to all possible attacks of text-based password. In such way graphical passwords are tricky to guess and uncomplicated to remember. But also there are some drawbacks of graphical passwords [3], such as password registration and log-in process require much more storage space than text based passwords, exposed to shoulder surfing attacks. So after graphical password an emerging security technique CAPTCHA (Completely Automated Public Turing-test to tell Computers and Humans Apart) was developed as a challenge- response test to identify the interruptions of bots during user authentication. This technique is found difficult for bots and easier for human discernment and followed in some foremost web sites of Microsoft, Google, Yahoo etc., have their own CATCHAs for addressing malicious programs.

The most widely used CAPTCHAs are the textual CAPTCHA, displayed as a distorted textual image along with noise for visually impaired ones. These textual CAPTCHAs were found to be inefficient towards online dictionary attacks and several other attacks, CAPTCHA as graphical password (CaRP) [4] technique is introduced in this paper to ensure security on hard Artificial Intelligence (AI) problems; a two-way authentication technique is used in one of the CaRP techniques of Recognition-based method [5]. The rest of this paper will deal with the related work in the field of CAPTCHAs and security [3], a more detailed description of our proposed work [6], the methods and algorithms to be used [7], conclusion and future developments [8].

RELATED WORK-AN OVERVIEW OF TEXTUAL CAPTCHA

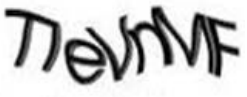
CAPTCHA [9] is a technique first used by computer scientists at Carnegie Mellon University in 2000 to resist against some malicious programs. A CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") is a challenge-response turing test used for computing, to determine whether the user is human or bot. Textual CAPTCHAs [10] as shown in Figure 1 are designed as distorted text images and sometimes with noise addition which are identified by humans easily. The authentication of the user is validated only after the distorted image on the screen is entered.

Text-based CAPTCHAs are the most widely used for security reasons in web application to tend for authentication process like registration, query processing, login validation etc., as shown in Figure 1 but there are some common weaknesses in handling textual CAPTCHAs. The Number of characters and digits used in this technique follow a same font patterns, and hence they are identified easily through OCR or Optical Character Recognition Technique (Figure 1).

Figure 1: Textual CAPTCHA [2].

When the noise is added to the text based CAPTCHA it creates a problem in recognition [11] during login, as the characters in that image have different shapes as depicted in Table 1. This problem is more prevalent in Text based CAPTCHA. In addition to the above mentioned disadvantages, users suffer from blurred vision and wave motion in distinguishing those characters in textual CAPTCHAs (Table 1).

Table 1: Confusing Text- based CAPTCHAs.

S.no	Text Captchas	Remarks
1.		Here the alphabets "c" and "l" maybe misinterpreted as "d"
2.		The first two alphabets "T" and "I" maybe misinterpreted as "T" and "l"

Graphical Password

The concept of graphical passwords was first described by Greg Blonder [Blonder. G, Graphical Passwords, Patent 5559961 at 1996 in United States] [12]. The idea of this is to allow a user to click on the set of images displayed on the screen rather than text- based passwords [13]. To gain access in the system, the user has to click on the same images sequentially again which they have chosen already in the registration. As this is easier for human memory rather than text-based it provides a way of user-friendly passwords (Table 2).

Table 2: Graphical Password Scheme.

Method Used	Merits	Demerits
Novel Authentication Scheme	Better Protection against Denial of Service Attacks	Increases the costs of Online Dictionary Attack
Cued Recall Technique	Complex Real World images can be used	Only Individual Click Points are considered
Draw-A- Secret (DAS) and STORY	It overcomes a drawback of Recall-Based systems	Hotspot was still a serious Security Problem
CORTCHA Technique	CORTCHA Technique is Scalable	It modifies images to generate challenge and images appear unpleasantly
Blowfish Algorithm, Window Clustering Algorithm and Dictionary Generation Algorithm	Preventing Dictionary Attacks [25] and E-Mail Spam [26]	Supports Mobile User Verification Only

There are numerous graphical password schemes [6,7] which can be classified into three categories according to the recording and entering passwords are recognition, recall, and cued recall. Some of the graphical passwords schemes are listed below depicted in Table 2 along with their merits and demerits.

APPENDING GRAPHICAL PASSWORDS WITH TEXTUAL CAPTCHAS

CaRP : CAPTCHA as Graphical Password Algorithm

In CaRP, for every login attempt a new image as shown in Figure 2 is generated for the same user. CaRP, which uses the alphabet is from visual objects (e.g., alphanumerical characters, similar figures) to generate a CaRP image, is an major challenge in Captcha **Source: Internet (Textual CAPTCHA) A major difference between CaRP images and Captcha images [14] is that all the visual objects in the string should appear in a CaRP image allows a user to input any password but not inevitably in a Captcha representation. Many Captcha schemes can be converted to CaRP schemes by following the above. CaRP Schemes is classified into two categories are Recognition-Based (Act of recognizing or condition of being recognized) [5,11] and Recognition-Recall [15]. Among these we discuss about Recognition-based CaRP [16] technique here (Figures 2 and 3).

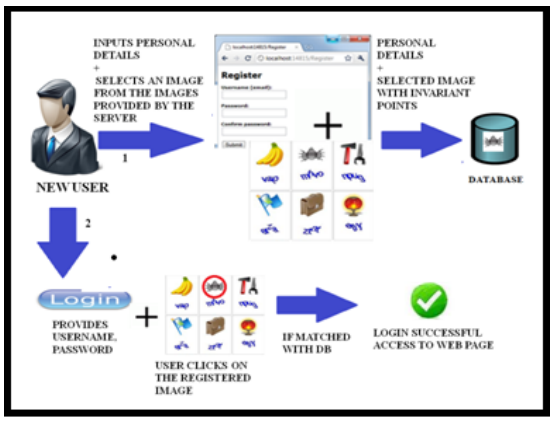


Figure 2: Appending textual CAPTCHA with graphical password.

Figure 3: Image with textual CAPTCHAs **

Recognition-Based CaRP

In this scheme, a password is a progression of optical stuff in the speckled alphabets. The traditional recognition-based graphical passwords, detection-based CaRP seems to have access to an infinite number of different visual objects on the screen. The 3 techniques under this scheme are discussed below.

ClickText

A recognition-based CaRP scheme is similar as text Captcha, with whose alphabets consists of characters are without any visually confusing characters. The ClickText [17] image has mostly 33 characters based on the servers. These characters are randomly arranged on 2D space for user access (Figure 4).

Figure 4: A ClickText Image [1].

Here the password preferred for authentication is a sequence of characters e.g. =“# 9CBYCU”. It is same as text password with difference in their spatial arrangements. The ClickText image generated by the Captcha engine is authenticated by the server according to user-clicked points on the ClickText image as shown in Figure 4 by authentication user.

The idea behind the ClickText image [18,19] is different from normal text Captcha. In text Captcha user has to type the characters from left to right sequentially and in ClickText user has to click the characters in password. In the above example user has to click the characters in the order as „#“, „9“, „C“, „B“, „Y“, „C“, and „U“. If this orders for given password example is followed by user, then user is an authorized user.

ClickAnimal

It is also a recognition-based CaRP scheme, based on Captcha Zoo images [20] Here an alphabet consists of similar animal figures e.g. dog, horse, pig, donkey etc., for every animal 3D model [21] is used for image representation. In accordance with the Captcha generation process, Images for authentication purpose is generated eg. ClickAnimal images as shown in Figure 5 are generated for authentication process. The 2D models are generated from the 3D animal image with minor variations in views, colours, textures, and lightning effects and if entail distortions are also included. These resulting 2D animals are placed on the cluttered background for authentication. In the 2D model of ClickAnimal image [22], a possibility of overlapping of animals may occur, but without any change in their core parts. This will lead a difficult identification for bots and easier for humans during login as shown in Figure 2. Here the password is a sequence of animal names such as password = “Dog, Cat, Turtle, Fox” etc. The ClickAnimal has a less significant alphabet and so the password legroom obligatory is also less as compared to ClickText as number of analogous animals is less than the number of available characters.

AnimalGrid: A Two-way Authentication Technique

To resist the human guessing attacks like shoulder surfing [23], spyware attacks [24] etc.,the password space required for CaRP scheme should be sufficiently larger than other schemes. So here in AnimalGrid CaRP scheme the password space is increased by combining click animal with the grids depending on the size of the selected animal. AnimalGrid as shown in Figure 5 is a amalgamation of ClickAnimal and CAS (Click-A-Secret) (Figure 5).

Figure 5: A ClickAnimal Image [1].

In CAS, a user clicks the grid cells of the corresponding animal in a password. In this AnimalGrid, ClickAnimal image is displayed first for two-way authentication technique [25]. After an animal is selected from a given images, an n*n grid equalizing their size will appear for user identification. As shown in Figure 3, when the red turkey in the left image was selected a 6*6 grid equalizing an animal is generated.

In this scheme password is a sequence of selected animals interleaving with grid cells [26]. Here password must begin with animal name. Eg. pwd=“Cat, Fox, Grid (3), Dog, Grid (2), Grid (1)”.Where Grid (3) means the grid-cell indexed as 3 and grid cells after an animal name means the grid is determined by the bounding rectangle of that animal as shown in Figure 6. Here the correct animal should be clicked for the correct follow up grid. If wrong animal is clicked, the follow up grid is also made wrong and entire registration will collapse. Figure 6 gives more concentration on enhancing security, here the user will get more secured options for their substantiation the illustration is given as aCaRP as key in it can be used in new user registration and login attempts. Captcha covers the gap between the User and System in finding certain AI problems. It can be visualized via text or Image recognition.

In Cued Click Points (CCP) [10], for every login attempts subsequent click point grids are retrieved to determine the tolerance of the original point. With CCP, we use f (username, currentImage, current Tolerance Square) this function to determine next image that distinctively maps each forbearness four-sided figure to a next-image (Figure 7).

1	35	34	3	32	6
30	8	28	27	11	7
24	23	15	16	14	19
13	17	21	22	20	18
12	26	9	10	29	25
31	2	4	33	5	36

Figure 6: 6 x 6 Grid Cells determined by colour bounding rectangle.

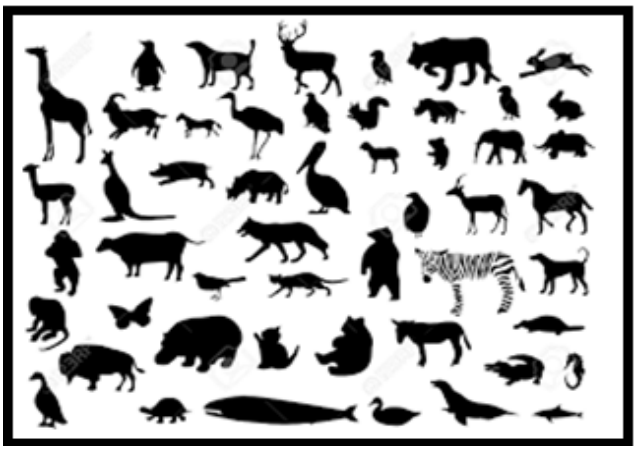


Figure 7: ClickAnimal Image.

As its limitation in duplicate image during multiple tolerance points a two-way authentication, which helps in identifying an error immediately after the click point is used as an enhanced security in Recognition-based CaRP scheme.

EXPERIMENTAL RESULTS

Login Attempts for user attempts leads to 25% failure that Tests when a bigger interval cared-for have a lot of failed makes an attempt. Some participants contributed considerably more failing makes an attempt than others. At the tip of tests, in a total of 50 participants 100% participants remembered their passwords, 97.5% remembered their passwords of each ClickText and Click Animal, and 83% remembered their Normal AlphaNumerical passwords. One of the users forgot the AnimalGrid parole at the one hour test, and another one forgot the ClickText parole at the one-week check depicted in Figure 8. For Text, three participants forgot their passwords at the one-week check, and a more forgot at the three week test. ClickAnimal scored the most effective in memo ability whereas Text scored the worst. This could be part attributable to the very fact that hotspots were allowed for PassPoints passwords, which Text passwords had a far larger alphabet than each ClickText and AnimalGrid. Graphical passwords schemes are compared based on the ease of usage. CaRP has excellent budding refinements it combines both the Captcha and Graphical Password Scheme (Figure 8).

CONCLUSION AND FUTURE ENHANCEMENTS

In this paper, the various password techniques such as textual password, graphical password, Captcha password and CaRP has been studied. The best alternative for textual password is a graphical password. The graphical password can reduce the burden of human memory as humans tend to remember graphics and images better than text. As graphical passwords are vulnerable to shoulder surfing and spyware attacks [27], the best alternative to graphical scheme Captcha technique [28] is used. Captcha can be recognized by humans and not by bots, and with its limitation in providing robust security a CaRP technique, which is the combination of captcha and graphical password is developed. It is relying on hard AI problems [29].

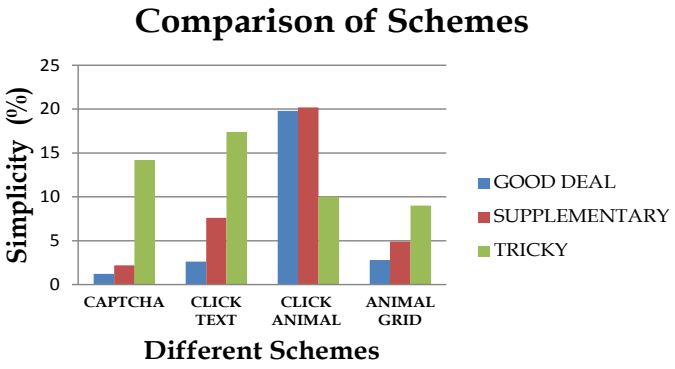


Figure 8: Comparison of Graphical Scheme.

The Recognition-Based CaRP includes ClickText, ClickAnimal and Animal Grid techniques. In all these techniques every time a new image is generated and so all the techniques are resistant to shoulder surfing attack and secure than graphical password techniques. Also for attackers [30] to hack CaRP [31] more incentives are required as compare to Captcha as CaRP does not rely on any specific scheme. At present all the CaRP techniques are more secure as compare to other password techniques [32]. But also CaRP has a scope for refinements. So to increase a security the difficulty level of images can be increased at every login attempt and this level is based on the machine used to login and on the login history of the user. Another scope of improvement here is some CaRP techniques can be made three-way for authentication. E.g. If AnimalGrid and ClickText are combined then it will become three-way authentication technique.

REFERENCES

[1] Reddy A, Goutham, Kim DS and Yoo KY, "Implicit Graphical Password Mutual Authentication using Mirror-Image Encryption", ACM Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems (RACS), pp. 218-223, 2014.

[2] Thorpe J, Al-Badawi M, MacRae B and Salehi-Abari A, "The Presentation Effect on Graphical Passwords", ACM Proceedings of the SIGHI Conference on Human Factor in Computing Systems, pp. 2947-2950, 2014.

[3] Anshuman S and Aniket AM, "Graphical User Authentication Techniques", International Journal of Advanced Research, Vol. 3, pp. 1101-1107, 2015.

[4] Davis M, Divya R, Paul V and Sankaranarayanan PN, "CAPCHA as Graphical Password", International Journal of Computer Science and Information Technologies

(IJCSIT), Vol. 6, No. 1, pp. 148-151, 2015.

[5] Haque A and Imam B, "A New Graphical Password: Combination of Recall & Recognition Based Approach", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol. 8, No. 2, pp. 320-324, 2014.

[6] Jermyn, Mayer A, Monrose F, Reiter M, and Rubin A, "The design and analysis of graphical passwords," in Proc, 8th USENIX Security Symp, pp. 1–15, 1999.

[7] Tao H and Adams C, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw Security, vol. 7, No. 2, pp. 273–292, 2008.

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

[9] Chiasson S, van Oorschot PC, and Biddle R, "Graphical password authentication using cued click points," in Proc, ESORICS, pp. 359–374, 2007.

[10] Rashmi BJ and Maheshwarappa B, "Improved Security Using Captcha as Graphical Password", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 5, pp. 352-354, 2015.

[11] Ugochukwu EKK and Jusoh Y, "A Review on the Graphical User Authentication Algorithm: Recognition-Based and Recall-Based", International Journal of Information Processing and Management, Vol. 4, No. 3, pp.238-252, 2013.

[12] Biddle R, Chiasson S and van Oorschot PC, "Graphical passwords: Learning from the first twelve years," ACM Computation. Surveys, vol. 44, no. 4, 2012.

[13] Pinkas B and Sander T, "Securing passwords against dictionary attacks," in Proc. ACM CCS, pp. 161-170, 2002.

[14] Sahay D, Merchant M, Sheikh S, Shukla R and Suryavanshi S, "Enhanced Security in Online Database System Using Visual Cryptography and Water Marking", International Journal of Computer Science and Information Technology Research, Vol. 3, pp. 297-302, 2015.

[15] Kale ND and Nalgirkar MM, "An Ample-Range Survey on Recall-Based Graphical Password Authentication Based on Multi-Line Grid and Attack Patterns", International Journal of Science and Modern Engineering (IJISME) Vol. 1, pp.32-36, 2013.

[16] Towhidi F and Masrom M, "A Survey on Recognition-Based Graphical User Authentication Algorithms" International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, pp.119-127, 2009.

[17] Oorschot PCV, Salehi-Abari A, and Thorpe J, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans, Inf Forensics Security, vol. 5, no. 3, pp. 393–405.

[18] Oorschot PCV and Thorpe J, "Exploiting predictability in clickbased graphical passwords," J. Comput Security, Vol. 19, No. 4, pp. 669–702, 2011.

[19] Kim S, Cao X, Zhang H and Tan D, "Enabling Concurrent Dual Views on Common LCD Screens", in Proceedings ACM Annual Conference Human Factors Computation System. pp. 2175-2184, 2012.

[20] Alsaleh M, Mannan M, and Oorschot PCV, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput, vol. 9, no. 1, pp. 128–141, 2012.

[21] Oorschot PCV and Thorpe J, "On predictive models and user drawn graphical passwords," ACM Trans Inf Syst Security, vol. 10, No. 4, pp. 1–33, 2008.

[22] Golofit K, "Click passwords under investigation," in Proc ESORICS, pp. 343–358, 2007.

[23] Wang L, Chang X, Ren Z, Gao H, Liu X, and Aickelin U, "Against spyware using CAPTCHA in graphical password scheme," in Proc, IEEE International Conference Advancement in Information Networking, pp. 1–9, 2010.

[24] Dirik E, Memon N, and Birget JC, "Modeling user choice in the passpoints graphical password scheme," in Proc Symp Usable Privacy Security, pp. 20–28, 2007.

[25] Nayan Gawande, "Merging CAPTCHA and Graphical Password on NP Hard Problems in AI: New Security Enhancing Tecnhique", International Journal of Science and Research (IJSR) Vol. 3, pp. 980-983, 2014.

[26] HP Tipping, Point DVLabs, Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs Vienna, Austria, 2010.

[27] Li S, Shah SAH, Khan MAU, Khayam SA, Sadeghi AR, and Schmitz R, "Breaking e-banking CAPTCHAs," in Proc, ACSAC, pp. 1–10, 2010.

[28] Ahn LV, Blum M, Hopper NJ, and Langford J, "CAPTCHA: Using hard AI problems for security," in Proc Eurocrypt, pp. 294–311, 2003.

[29] Thorpe J and Oorschot PCV, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc USENIX Security, pp. 103–118, 2007.

[30] Wolverton T, Hackers Attack eBay Accounts, 2002.

[31] Oorschot PCV and Stubblebine S, "On countering online dictionary attacks with login histories and humans-in-the-loop," ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.

[32] Zhu BB, Yan J, Bao G, Yang M and Xu N "Captcha as Graphical Password – A New Security Primitive Based on Hard AI Problems", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 6, pp. 891-904, 2014.

