Research Article

International Journal of Advanced Computer Research, Vol 6(24)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.624001

Enhancing security against hard AI problems in user authentication using CAPTCHA as graphical passwords

S. Murugavalli[1], S.A.K. Jainulabudeen[2*], G. Senthil Kumar[3] and D. Anuradha[3]
Professor and HOD, Department of CSE, Panimalar Engineering College, Chennai, India[1]
Assistant Professor, Department of CSE, Panimalar Engineering College, Chennai, India[2]
Associate Professor, Department of CSE, Panimalar Engineering College, Chennai, India[3]

Received: 28-February-2016; Revised: 19-May-2016; Accepted: 24-May-2016

Abstract

Information and computer security are supported by the passwords, as passwords play a vital role in the authentication process. The traditional authentication method uses text-based passwords, which is also called alphanumeric passwords, is not reliable in data security, and to overcome these drawbacks, the graphical password scheme is introduced as an alternative to text-based passwords. But the graphical password scheme is vulnerable to shoulder surfing attacks, spyware attacks. To overcome this vulnerability of graphical passwords, an emerging technique that is Completely Automated Public Turing Tests to tell Computers and Humans Apart (CAPTCHA), as a challenge response test is generated to distinguish humans from bots in authentication. To ensure security, an alternative method to textual CAPTCHA is replaced by CAPTCHA as gRaphical Password (CaRP). As CaRP scheme has a scope of refinements in cyber security a two-way authentication method is proposed in one of the CaRP techniques of Recognition-based scheme. The graphical password scheme when compared, confer exceptional nascent outcome when it coalesces both CAPTCHA and graphical passwords.

Keywords

Textual CAPTCHAs, Authentication, Shoulder surfing attacks, Cyber security, CaRP.

1.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 [1]. 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). In the meadow of artificial intelligence, the majority of complicated problems is casually said to be AI-Complete or AI-Hard, this implies the complexity of computing those problems is alike to that of solving the vital artificial intelligence problem (simply means building machines as smart as the populace or burly AI) [2].

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 passwords [3] 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 resist some security and usability problems. This short come in alphanumerical passwords led to the development of graphical password schemes [4]. 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 [5],

*Author for correspondence

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 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 websites 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, CaRP [6] 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 [7]. The rest of this paper will deal with the related work in the field of CAPTCHAs and security [5], a more detailed description of our proposed work [8], the methods and algorithms to be used [9], conclusion and future developments [10].

2.Related work-an overview of textual CAPTCHA

CAPTCHA [11] 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 [12] 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 the 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 follows a same font patterns, and hence they are identified easily through OCR or Optical Character Recognition Technique.

When the noise is added to the text based CAPTCHA it creates a problem in recognition [13] during login, as the characters in that image have different shapes as depicted in *Table 1*.

This problem is more prevalent in a 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.

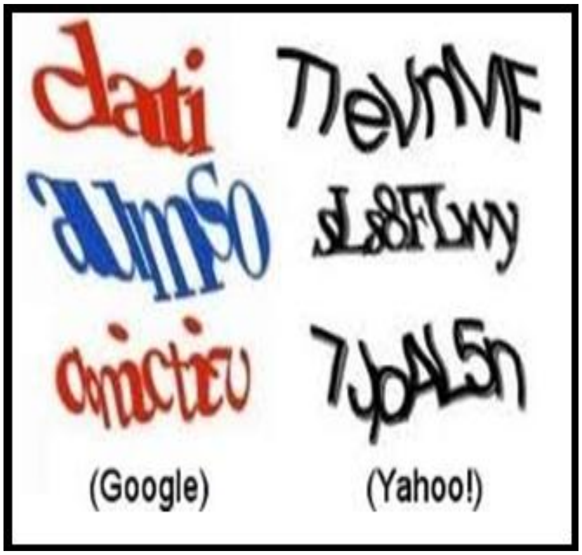
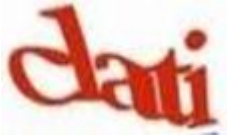
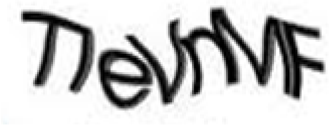


Figure 1 Textual CAPTCHA [2]

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”

2.1Graphical password

The concept of graphical passwords was first described by Greg Blonder [Blonder. G, Graphical Passwords, Patent 5559961 at 1996 in the United States] [14]. 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 [15]. To gain access to 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 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 [15] and E-mail spam [16]	Supports mobile user verification only

There are numerous graphical password schemes [13] [14] which can be classified into three categories according to the recording and entering passwords are recognizing, recall, and cued recall. Some of the graphical password schemes are listed below depicted in *Table 2* along with their merits and demerits.

3.Appending graphical passwords with textual CAPTCHAs

As Graphical passwords [14] finds limitation in both storage space and time than text-based, we have proposed an idea of combining the above two techniques to enhance the security in authentication for any web application as shown in *Figure 2*. We use a technique named CaRP.

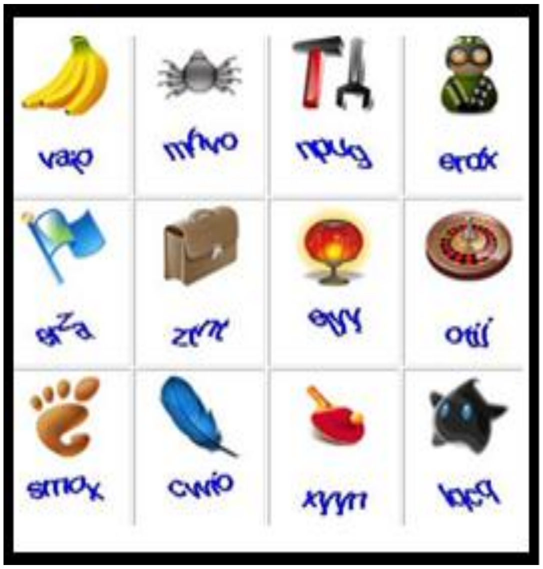


Figure 2 Image with textual CAPTCHAs [1]

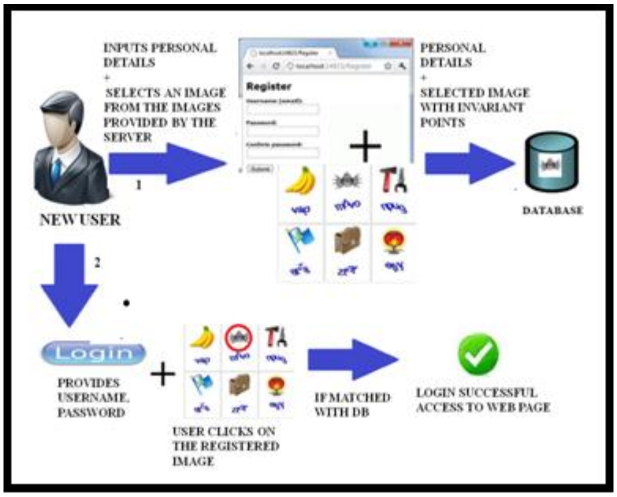

INPUTS PERSONAL DETAILS
+
SELECTS AN IMAGE FROM THE IMAGES PROVIDED BY THE SERVER
1
NEW USER
Register
+
PERSONAL DETAILS
+
SELECTED IMAGE WITH INVARIANT POINTS
DATABASE
2
Login
PROVIDES USERNAME, PASSWORD
+
USER CLICKS ON THE REGISTERED IMAGE
IF MATCHED WITH DB
LOGIN SUCCESSFUL ACCESS TO WEB PAGE

Figure 3 Appending textual CAPTCHA with graphical password

3.1 CaRP : CAPTCHA as graphical password algorithm

In CaRP, for every login attempt a new image as shown in *Figure 3* 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. A major difference between CaRP images and CAPTCHA images [17] 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 are classified into two categories are Recognition-Based (Act of recognizing or condition of being recognized) [18] and Recognition-Recall [19]. Among these we discuss about Recognition-based CaRP [19] technique here.

3.2Recognition-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.

3.2.1ClickText

A recognition-based CaRP scheme is similar as text Captcha, with whose alphabets consist of characters are without any visually confusing characters. The ClickText [20] image has mostly 33 characters based on the servers. These characters are randomly arranged in 2D space for user access.

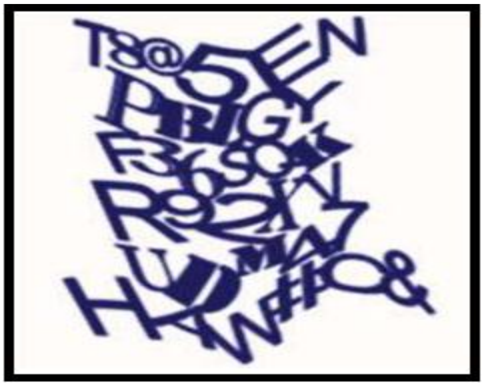


Figure 4 A ClickText image [1]

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 point on the ClickText image as shown in *Figure 4* by authentication user. The idea behind the ClickText image [21] [22] is different from normal text CAPTCHA. In text CAPTCHA user has to type the characters from left to right sequence and in ClickText user has to click the characters in the password. In the above example, a 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 the user is an authorized user.

3.2.2ClickAnimal

It is also a recognition-based CaRP scheme, based on CAPTCHA Zoo images [23] Here an alphabet consists of similar animal figures, e.g. dog, horse, pig, donkey etc., for every animal 3D model [24] is used for image representation. In accordance with the CAPTCHA generation process, Images for authentication purpose is generated, e.g. ClickAnimal images as shown in *Figure 5* are generated in authentication process. The 2D models are generated from the 3D animal image with minor variations in views, colors, 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 [25], 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.

3.2.3Animal grid: A two-way authentication technique

To resist the human guessing attacks like shoulder surfing [26], spyware attacks [27] 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 6* is an amalgamation of ClickAnimal and Click-A-Secret (CAS).

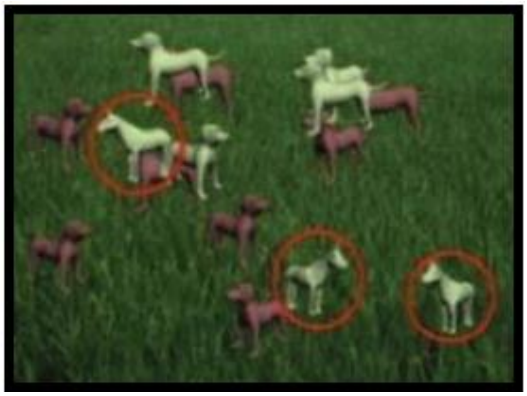


Figure 5 A ClickAnimal image [1]

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 [28]. After an animal is selected from a given image, a 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 [29]. Here password must begin with animal names. E.g., 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 7*. Here the correct animal should be clicked for the correct follow up the grid. If wrong animal is clicked, the follow up the grid is also done 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 a CaRP 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.

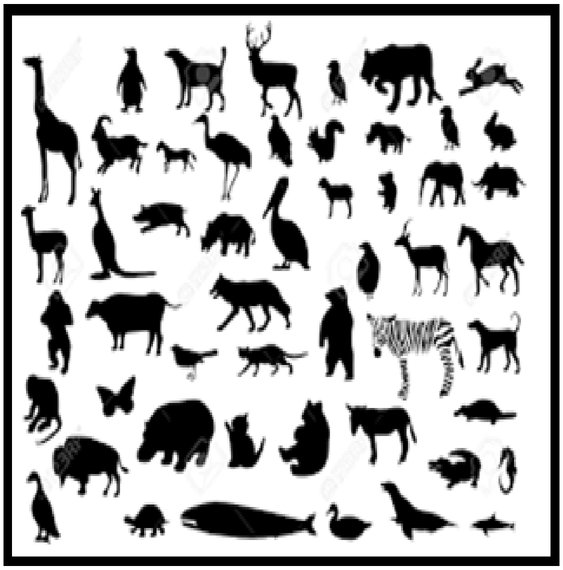
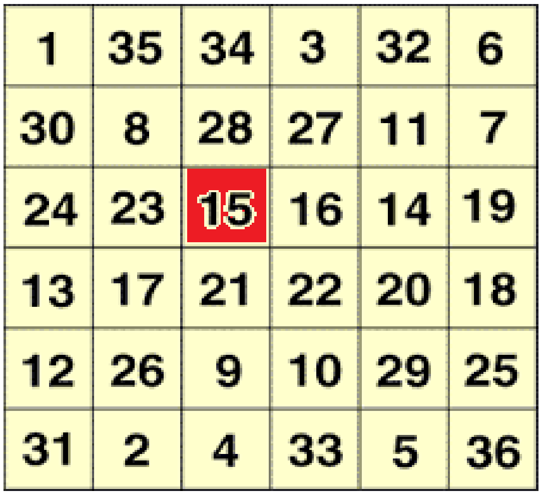


Figure 6 ClickAnimal image [1]

In Cued Click Points (CCP) [30], for every login attempts subsequent click point grids are retrieved to determine the tolerance of the original point. With CCP, we use of (username, currentImage, current Tolerance Square) this function to determine the next image that distinctively maps each forbears four-sided figure to a next-image.



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 7 6 x 6 Grid Cells determined by color bounding rectangle [1]

As its limitation on the 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.

4.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 in 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.

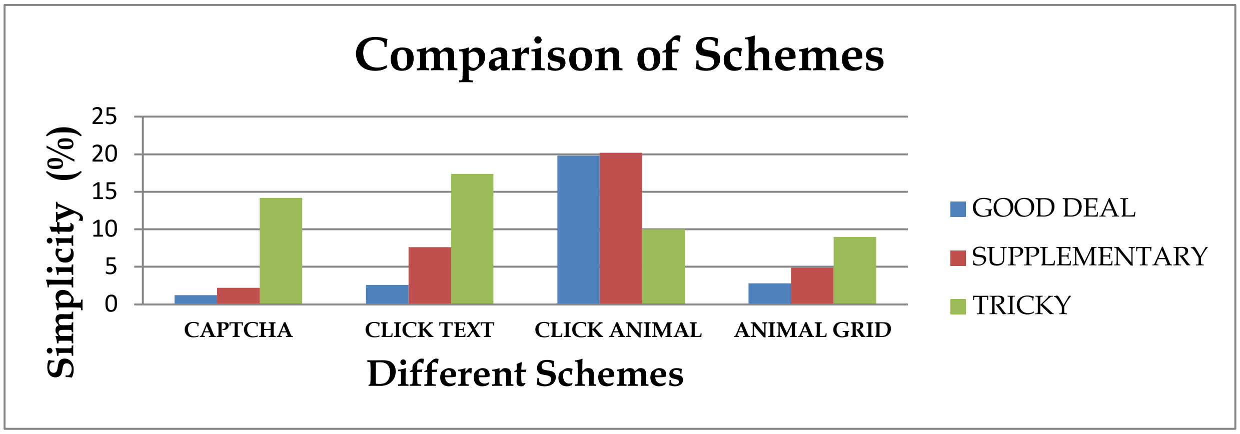


Figure 8 Comparison of graphical scheme

5.Conclusion and future enhancements

In this paper, the various password techniques such as textual password, graphical password, CAPTCHA password and CaRP have been studied. The better 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 [31], the best alternative to the graphical scheme CAPTCHA technique [32] is used. A CAPTCHA can be recognized by humans and not by bots, and with its limitation on providing robust security a CaRP technique, which is the combination of CAPTCHA and graphical password is developed. It is relying on hard AI problems [33]. The Recognition-based CaRP includes ClickText, ClickAnimal and AnimalGrid 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 [33] to hack CaRP [34] more incentives are required as compared 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. 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 of authentication. E.g. If AnimalGrid and ClickText are combined, then it will become a three-way authentication technique.

Acknowledgment

None.

Conflicts of Interest

The authors have no conflicts of interest to declare.

References

[1] Zhu BB, Yan J, Bao G, Yang M, Xu N. Captcha as grRaphical passwords-a new security primitive based on hard AI problems. IEEE Transactions on Information Forensics and Security. 2014; 9(6):891-904.

[2] Yampolskiy RV. AI-complete, AI-hard, or AI-easy: classification of problems in artificial intelligence. 2011.

[3] Goutham RA, Kim DS, Yoo KY. Implicit graphical password mutual authentication using mirror-image encryption. In proceedings of the conference on research in adaptive and convergent systems 2014 (pp. 218-23). ACM.

[4] Thorpe J, Al-Badawi M, MacRae B, Salehi-Abari A. The presentation effect on graphical passwords. In proceedings of the SIGCHI conference on human factors in computing systems 2014 (pp. 2947-50). ACM.

[5] Anshuman S, Aniket AM. Graphical user authentication techniques. International Journal of Advanced Research 2015; 3(11):1101-7.

[6] Davis M, Divya R, Paul V, Sankaranarayanan PN. CAPCHA as graphical password. International Journal of Computer Science and Information Technologies. 2015; 6(1); 148-51.

[7] Haque MA, 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. 2014; 8(2):320-4.

[8] Jermyn I, Mayer AJ, Monrose F, Reiter MK, Rubin AD. The design and analysis of graphical passwords. In Usenix security 1999.

[9] Tao H, Adams C. Pass-Go: A proposal to improve the usability of graphical passwords. International Journal Network Security. 2008; 7(2):273-92.

[10] Wiedenbeck S, Waters J, Birget JC, Brodskiy A, Memon N. Pass points: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies. 2005; 63(1):102-27.

[11] Chiasson S, van Oorschot PC, Biddle R. Graphical password authentication using cued click points. In computer security–ESORICS 2007 (pp. 359-74). Springer Berlin Heidelberg.

[12] Rashmi BJ, Maheshwarappa B. Improved security using captcha as graphical password. International Journal of Advanced Research in Computer and Communication Engineering.2015; 4(5):352-4.

[13] Ugochukwu K, Ekeke E, Jusoh YY. A review on the graphical user authentication algorithm: recognition-based and recall-based. International Journal of Information Processing & Management. 2013; 4(3):238-52.

[14] Biddle R, Chiasson S, Van Oorschot PC. Graphical passwords: learning from the first twelve years. ACM Computing Surveys (CSUR). 2012; 44(4):19.

[15] Pinkas B, Sander T. Securing passwords against dictionary attacks. In proceedings of the ACM conference on computer and communications security 2002 (pp.161-70). ACM.

[16] Van Oorschot PC, Stubblebine S. On countering online dictionary attacks with login histories and humans-in-the-loop. ACM Transactions on Information and System Security. 2006; 9(3):235-58.

[17] Sahay D, Merchant M, Sheikh S, Shukla R, Suryavanshi S. Enhanced security in online database system using visual cryptography and water marking. International Journal of Computer Science and Information Technology Research. 2015; 3(4): 297-302.

[18] Kale ND, 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. 2013; 1(5):32-6.

[19] Towhidi F, Masrom M. A survey on recognition based graphical user authentication algorithms. International Journal of Computer Science and Information Security. 2009; 6(2):119-27.

[20] Van Oorschot PC, Salehi-Abari A, Thorpe J. Purely automated attacks on passpoints-style graphical passwords. IEEE Transactions on Information Forensics and Security. 2010; 5(3):393-405.

[21] Van Oorschot PC, Thorpe J. Exploiting predictability in click-based graphical passwords. Journal of Computer Security. 2011; 19(4):669-702.

[22] Kim S, Cao X, Zhang H, Tan D. Enabling concurrent dual views on common LCD screens. In proceedings of the SIGCHI conference on human factors in computing systems 2012 (pp. 2175-84). ACM.

[23] Alsaleh M, Mannan M, Van Oorschot PC. Revisiting defenses against large-scale online password guessing attacks. IEEE Transactions on Dependable and Secure Computing. 2012; 9(1):128-41.

[24] Van Oorschot PC, Thorpe J. On predictive models and user-drawn graphical passwords. ACM Transactions on Information and System Security (TISSEC). 2008; 10(4):5.

[25] Gołofit K. Click passwords under investigation. In computer security–ESORICS 2007 (pp. 343-58). Springer Berlin Heidelberg.

[26] The Science Behind Passfaces. http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf. Accessed 23 December 2015.

[27] Wang L, Chang X, Ren Z, Gao H, Liu X, Aickelin U. Against spyware using CAPTCHA in graphical password scheme. In IEEE international conference on advanced information networking and applications (AINA) 2010 (pp.760-7). IEEE.

[28] Dirik AE, Memon N, Birget JC. Modeling user choice in the pass points graphical password scheme. In proceedings of the 3rd symposium on usable privacy and security 2007 (pp. 20-8). ACM.

[29] Gawande N. Merging CAPTCHA and graphical password on NP hard problems in AI: new security enhancing Tecnhique. International Journal of Science and Research. 2014; 3(12); 980-3.

[30] Thorpe J, Van Oorschot PC. Human-Seeded attacks and exploiting hot-spots in graphical passwords. In USENIX security symposium 2007 (pp.103-18).

[31] T Wolverton. Hackers Attack eBay Accounts. http://www.zdnet.co.uk/news/networking/2002/03/26/hackers-attack-ebay-accounts-2107350/. Accessed 23 December 2015.

[32] DVLabs HT. Vienna, Austria. Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs. http://dvlabs.tippingpoint.com/toprisks2010/ Accessed 23 December 2015.

[33] Li S, Shah S, Khan M, Khayam SA, Sadeghi AR, Schmitz R. Breaking e-banking CAPTCHAs. In proceedings of the annual computer security applications conference 2010 (pp. 171-80). ACM.

[34] Von Ahn L, Blum M, Hopper NJ, Langford J. CAPTCHA: using hard AI problems for security. In advances in cryptology-EUROCRYPT 2003 (pp. 294-311). Springer Berlin Heidelberg.

S A K Jainulabudeen was born in Chennai on 03rd April, 1989. He received B.E degree in Computer Science and Engineering from Anna University, Chennai in 2010 and M. Tech in Computer Science and Engineering from B.S. Abdur Rahman University in 2013. He is currently working as Assistant Professor in Panimalar Engineering College, Chennai. His research interest is in the areas of Image processing, Cloud Computing.

Email: jainulabudeen_sak@yahoo.com