ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems

Satlawar Rajani
M.Tech Student,
Department of CSE,
AMR Institute of Technology,
Mavala, T.S, India.

Mrs.B.Manasa
Associate Professor
Department of CSE,
AMR Institute of Technology,
Mavala, T.S, India.

Abstract

This method has been shown to have significant drawbacks. For example, user tends to pick passwords that can be easily guessed. The most common computer authentication method is to use lphanumerical usernames and passwords. On the other hand, if a password is hard to guess, then it is often hard to remember. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and captcha. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present a new security primitive based on hard AI problems, graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme .We discuss the strengths and limitations of each method and point out the future research directions in this area. And also major design and implementation issues are clearly explained. The main advantage of this method is it is difficult to hack.

Keywords—Graphical password , password, CaRP, Captcha, dictionary attack, password guessing attack, security primitive.

INTRODUCTION

In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks.

Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.Defense against online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons: It causes denial-of-service attacks (which were exploited to lock highest bidders out in final minutes of eBay auctions and incurs expensive helpdesk costs for account reactivation.Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been under-exploredCaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk . Defense against online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:1) It causes denial-of-service attacks (which were exploited to lock highest bidders out in final minutes of eBay auctions and incurs expensive helpdesk costs for account reactivation.2) It is vulnerable to global password attacks whereby adversaries intend to break into any

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

account rather than a specific one, and thus try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold to avoid triggering account lockout. CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks ifcombined with dual-view technologies. The most common computer authentication method is for a user to submit a user name and text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics have been used.

BACKGROUND WORKS

Authentication is the process to allow users to confirm his or her identity to a Web application. Human factors are often considered the weakest link in a computer security system. Point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. A computer operating systems,mobile phones, ATMs machines, etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online. The password is a very good and strong authentication method still used up to now butbecause of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of conventional password appears like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our application as possible, so a researches come out with advanced password called graphical password where they tried to improve the security andavoid the weakness of conventional password. Graphical password have been proposed as a possible alternative to textbased, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

A large number of graphical password schemes have beenproposed. They can be classified into three categories accordingto 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

A. Passwords of the graphical

In this module, Users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first A *recognition-based* scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces [2] wherein a user selects a portfolio of faces from a database in creating a password. This process is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. Story [20] is similar to Passfaces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Déjà Vu [21] is also similar but uses a large set of computergenerated "random-art" images. Among the three types, recognition is considered the easiest for human memory whereas pure recall is the hardest [1]. Recognition is typically the weakest in resisting guessing attacks. Many proposed recognition-based schemes practically have a password space in the range of 213 to 216 passwords [1]. A study [6] reported that a significant portion of passwords of DAS and Pass-Go [4] were successfully broken with guessing attacks using dictionaries of 231 to 241 entries, as compared to the full password space of 258 entries. Images contain hotspots [7], [8], i.e., spots likely selected in creating passwords. Hotspots were exploited to mount successful guessing attacks on PassPoints [8]–[11]: a significant portion of passwords were broken with dictionaries of 226 to 235 entries, as compared to the full space of 243 passwords.

B. Captica in Authentication

It was introduced in [14] to use both Captcha and password in a user authentication protocol, which we call *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks. The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access. Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. Security of text Captchas has been extensively studied [26]–[30]. The following principle has been established: text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorially hard [30].Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation. Asirra [31] relies on binary object classification: a user is asked to identify all the cats from a panel of 12 images of cats and dogs. Security ofIRCs has also been studied. Asirra was found to be susceptible to machine-learning attacks [24]. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure [25]. Multi-label classification problems are considered much harder than binary classification problems.Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application

C.Thwart Guessing Attacks

In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials. No matter how secure a graphical password scheme is, the password can always be found by a brute force attack. In this paper, we distinguish two types of guessing

attacks: *automatic guessing attacks* apply an automatic trial and error process but *S* can be manually constructed whereas *human guessing attacks* apply a manual trial and error process.

D.Security Of Underlying Captcha

Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

model has been established yet. Object segmentation is considered as a computationallyexpensive, combinatorially-hard problem, which modern text Captcha schemes rely on

CAPTCHA AS GRAPHICAL PASSWORDS

A.what is password

The term PASSWORD commonly refers to a secret used for authentication. Passwords are the most commonly used method for identifying users in computer and communication systems.

B. passwords are used for:

Logging into accounts, Retrieving emails, Accessing applications, Networks, Websites, Databases, workstations

C. An Overview OF CaRP:

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an *alphabet* of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes, as described in the next subsection.

D.Captcha to CaRP

any visual Captcha scheme relying on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and most IRCs meet this requirement. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects. In practice, conversion of a specific Captcha scheme to a CaRP scheme typically requires a case by case study, in order to ensure both security and usability. We will present in Sections IV and V several CaRPs built on top of text and image-recognition Captcha schemes.

E.recognition-based carp

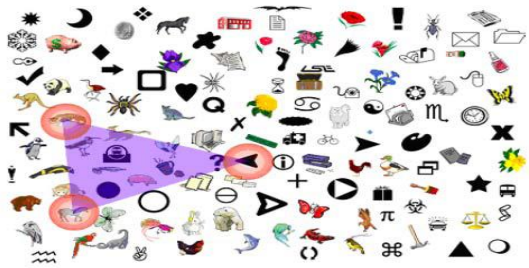
For this type of CaRP, a password is a sequence of visual objects in the alphabet. Per view of traditional recognitionbased graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects. We present two recognition-based CaRP schemes and a variation next.

ClickText image with 33 characters

Captcha Zoo with horses circled red.

A Click Animal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle. System display a number of pass-objects (pre-selected by user) among many other objects, user click inside the convex hull bounded by pass-objects

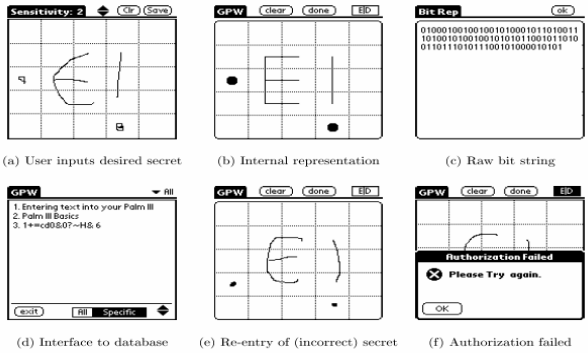
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



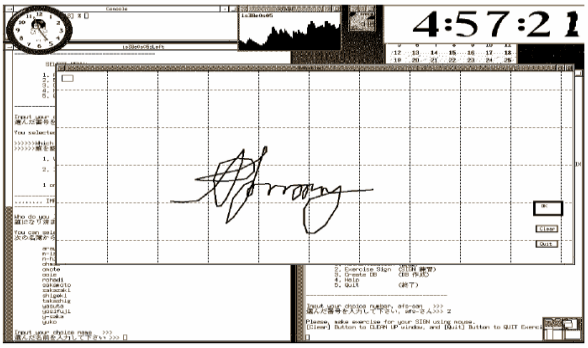
RECOGNITION-RECALL CaRP

Draw-A-Secret (DAS) Scheme

User draws a simple picture on a 2D grid, the coordinates of the grids occupied by the picture are stored in the order of drawing.Redrawing has to touch the same grids in the same sequence in authentication.



Signature scheme Here authentication is conducted by having the user drawing their signature using a mouse



Characters contain invariant points. Fig. 5 shows some invariant points of letter “A”, which offers a strong cue to memorize and locate 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 internal invariant points of characters is selected to form a set of *clickable points* for TextPoints. The internality ensures that a clickable point is unlikely occluded by a neighboring character and that its tolerance region unlikely overlaps with any tolerance region of a neighboring character’s clickable points on the image generated by the underlying Captcha engine. In determining clickable points, the distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images. In addition, variation should also be taken into consideration. For example, if the center of a stroke segment in one character is selected, we should avoid selecting the center of a similar stroke segment in another character.

A. Security of Captcha

This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test. This term is ambiguous because it could also mean a Turing test in which the participants are both attempting to prove they are the computer..This user identification procedure has received many criticisms, especially from disabled people, but also from other people who feel that their everyday work is slowed down by distorted words that are illegible even for users with no disabilities at all. As a framework of graphical passwords, CaRP does not relyon any specific Captcha scheme. If one Captcha scheme gets broken, a new and more robust Captcha scheme may appear and be used to construct a new CaRP scheme. In the remaining security analysis, we assume that it is intractable for computers to recognize any objects in any challenge image generated by the underlying Captcha of CaRP. More accurately, the Captcha is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

assumed to be *chosen-pixel attack (CPA)*-secure defined with the following experiment: an adversary *A* first learns from an arbitrary number of challenge images by querying a groundtruth oracle *O* as follows: *A* selects an arbitrary number of internal object-points and sends to *O*, which responds with the object that each point lies in. Then *A* receives a new challenge image and selects an internal object-point to query *O* again.

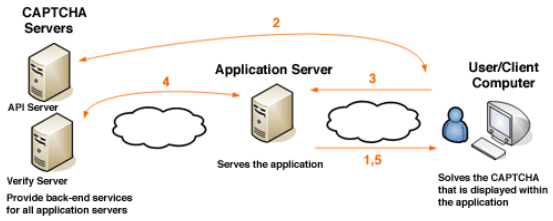
B.Human Guessing Attacks

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. A recent study on text passwords [42] indicates that users tend to choose passwords of 6–8 characters and have a strong dislike of using non-alphanumeric characters, and thatan acceptable benchmark of effective password space is the expected number of optimal guesses per account needed to break 50% of accounts, which is equivalent to 21.6 bits for Yahoo! users. If we assume that ClickText has roughly the same effective password space as text passwords, it requires on average 1000 people to work 1.65 days or one person to work 4.54 years to find a ClickText password

SYSTEM ARCHITECTURE

PTCHAs based on reading text — or other visual-perception tasks — prevent blind or visually impaired users from accessing the protected resource.[7] However, CAPTCHAs do not have to be visual. Any hard artificial intelligence problem, such as speech recognition, can be used as the basis of a CAPTCHA. Some implementations of CAPTCHAs permit users to opt for an audio CAPTCHA.[8] Other implementations do not require users to enter text, instead asking the user to pick images with common themes from a random selection.[9]

For non-sighted users (for example blind users, or the color blind on a color-using test), visual CAPTCHAs present serious problems. Because CAPTCHAs are designed to be unreadable by machines, common assistive technology tools such as screen readers cannot interpret them. Since sites may use CAPTCHAs as part of the initial registration process, or even every login, this challenge can completely block access. In certain jurisdictions, site owners could become target of litigation if they are using CAPTCHAs that discriminate against certain people with disabilities. For example, a CAPTCHA may make a site incompatible with Section 508 in the United States. In other cases, those with sight difficulties can choose to identify a word being read to them.



EMPIRICAL EVALUATIONS

Modern CAPTCHAS like reCAPTCHA no longer rely just on fixed patterns but instead present different variations of characters that are often collapsed together, making segmentation almost impossible. These newest iterations have been much more successful at warding off automated tasks. In 2009, Professor Anand Gupta of Netaji Subhas Institute of Technology led a team of researchers (Ashish Jain, Tushar Pahwa, Aditya Raj) to propose a novel scheme of embedding numbers in text CAPTCHAS (called Sequenced Tagged Captchas).[13] It incorporates two levels of testing that includes identification of displayed characters, and secondly, interpreting the logical ordering based on the embedded numbers. This adds significantly to the difficulty of breaking the CAPTCHA since the numbers signifying the ordering have to be separately identified; yet it can be dynamically generated. VIn October 2013, artificial intelligence company Vicarious claimed that it had developed software that was able to solve modern CAPTCHAs with character recognition rates of up to 90%.[14] Unlike the previous one-off successes that made use of flaws in specific CAPTCHA tests,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Vicarious asserted that its algorithms were powered by a holistic vision system modeled after insights from the human brain. The company also indicated that its AI was not specifically designed to complete CAPTCHA but rather to correctly recognize photographs, videos, and other visual data. However, Luis von Ahn, a pioneer of early CAPTCHA and founder of reCAPTCHA, expressed skepticism, stating: "It's hard for me to be impressed since I see these every few months. In its earliest iterations there was not a systematic methodology for designing or evaluating CAPTCHAs.[6] As a result there were many instances in which CAPTCHAs were of a fixed length and therefore automated tasks could be constructed to successfully make educated guesses about where segmentation should take place. Other early CAPTCHAs contained limited sets of words, which made the test much easier to game. Still others made the mistake of relying too heavily on background confusion in the image. In each case, algorithms were created that were successfully able to complete the task by exploiting these design flaws. These methods proved brittle however, and slight changes to the CAPTCHA were easily able to thwart them.

A. Accessibility

As many CAPTCHAs have the option of audio CAPTCHAs for the visually impaired people, an audio file of the CAPTCHA can be downloaded that reads out the CAPTCHA which can be decoded using a speech to text synthesis software with greater accuracy and the obtained result can be used to serve as the input to the CAPTCHA asked. But noises in the sound file can be obstructive. The Australian Communications Consumer Action Network's CEO Teresa Corbin has stated “CAPTCHAs fundamentally fail to properly recognise people with disability as human”.[17]

B.Computer character recognition

Although CAPTCHAs were originally designed to defeat standard OCR software designed for document scanning, a number of research projects have proven that it is possible to defeat many CAPTCHAs with programs that are specifically tuned for a particular type of CAPTCHA. For CAPTCHAs with distorted letters, the approach typically consists of the following steps:

1. Removal of background clutter, for example with color filters and detection of thin lines.
2. Segmentation, i.e., splitting the image into segments containing a single letter.
3. Identifying the letter for each segment.

Step 1 is typically very easy to do automatically. In 2005, it was also shown that neural network algorithms have a lower error rate than humans in step 3.[21] The only part where humans still outperform computers is step 2. If the background clutter consists of shapes similar to letter shapes, and the letters are connected by this clutter, the segmentation becomes nearly impossible with current software. Hence, an effective CAPTCHA should focus on step 2, the segmentation. Neural networks have been used with great success to defeat CAPTCHAs as they are generally indifferent to both affine and non-linear transformations. As they learn by example rather than through explicit coding, with appropriate tools very limited technical knowledge is required to defeat more complex CAPTCHAs. Detailing a method for defeating one of the most popular CAPTCHAs, EZ-Gimpy, which was tested as being 92% accurate in defeating it.[22] The same method was also shown to defeat the more complex and less-widely deployed Gimpy program 33% of the time. However, the existence of implementations of their algorithm in actual use is indeterminate at this time.PWNtcha has made significant progress in defeating commonly used CAPTCHAs, which has contributed to a general migration towards more sophisticated CAPTCHAs. A number of Microsoft Research papers describe how computer programs and humans cope with varying degrees of distortion

INSECURE IMPLEMENTATION

Howard Yeend has identified two implementation issues with poorly designed CAPTCHA systems Some

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CAPTCHA protection systems can be bypassed without using OCR simply by re-using the session ID of a known CAPTCHA image.CAPTCHAs residing on shared servers also present a problem; a security issue on another virtual host may leave the CAPTCHA issuer's site vulnerable. Sometimes, if part of the software generating the CAPTCHA is client-side (the validation is done on a server but the text that the user is required to identify is rendered on the client side), then users can modify the client to display the unrendered text. Some CAPTCHA systems use MD5 hashes stored client-side, which may leave the CAPTCHA vulnerable to a brute-force attack Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

We present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices.

CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem than it might appear.

Conclusion

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only *probabilistically* by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service.

ACKNOWLEDGMENT

I am **SATLAWAR RAJANI** k and would like to thank the publishers, researchers for making their resources material available. I am greatly thankful to Associate Prof**: MRS.B.MANASA** for their guidance. We also thank the college authorities, PG coordinator and Principal for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

[2] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

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

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

[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, pp. 102–127, Jul. 2005.

[6] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, CAPTCHA: Using hard AI problems for security, in Proc. Eurocrypt, 2003, pp. 294 to 311.

[7] B. B. Zhu *et al.*, "Attacks and design of image recognition CAPTCHAs," in *Proc. ACM CCS*, 2010, pp. 187–200.

[8] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in *Proc. ACM CCS*, 2008, pp. 543–554.

[9] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in *Proc. ACSAC*, 2010, pp. 1–10.

Miss SATLAWAR RAJANI. MTech student, in M.Tech Student, Dept of CSE in **Amr Institute of Technology**, mavala, T.S, India

Mrs.B.MANASA working as a Associate Professor at **Amr Institute of Technology**, mavala, T.S, India, Graduate from JNTUH Hyderabad. She has 2 years of UG/PG Teaching Experience