Survey of Text CAPTCHA Techniques and Attacks

Simran Sharma[#1], Nidhi Seth[*2]

[#]M.TECH, [*]Assistant Professor Computer Science & Engineering Department&
JMIT, Radaur / Kurukshetra University, India

***Abstract*— CAPTCHA is a challenge-response test most often placed within web forms to determine whether the user is human. The purpose of CAPTCHA is to block automated scripts that post spam content everywhere they can. This paper presents a survey of Optical Character Recognition applications and further focuses on three important applications of Optical Character Recognition, CAPTCHAS. There is a constant need to improve current CAPTCHAs and to develop new CAPTCHAs in order to safely secure against developing programs which can create thousands of e-mail accounts used for malicious purposes, stuff online polls with ballots, and develop worms and viruses contained in emails.**

***Keywords* — HIP, Challenge Response, CAPTCHAS, OCR, Security.**

I. INTRODUCTION

Many websites use CAPTCHAs or Completely Automated Public Turing tests to tell Computers and Humans Apart in an attempt to block automated interactions with their sites[1]. These efforts may be crucial to the success of these sites in various ways. For example, Gmail improves its service by blocking access to automated spammers, eBay improves its marketplace by blocking bots from flooding the site with scams, and Facebook limits creation of fraudulent profiles used to spam honest users or cheat at games. The most widely used CAPTCHA schemes use combinations of distorted characters and obfuscation techniques that humans can recognize but that may be difficult for automated scripts

The term "CAPTCHA" was first described by von Ahn[2]., describing a test that can differentiate humans from computers.Text CAPTCHAs are almost exclusively used in real applications. In a text CAPTCHA, characters are deliberately distorted and connected to prevent recognition by bots. Most of the proposed or deployed text CAPTCHA's have been broken. It is possible to enhance the security of an existing text CAPTCHA by systematically adding noise and distortion, and arranging characters more tightly. These measures, however, would also make the characters harder for humans to recognize, resulting in a higher error.

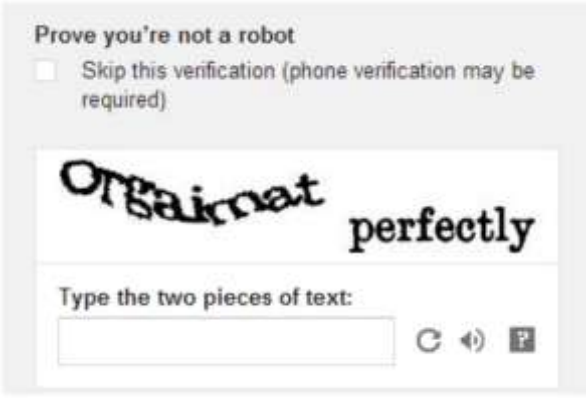

Figure 1 text-based CAPTCHA used by Gmail account creation process. A user must enter each displayed character correctly in-order to proceed. The volume icon indicates that a user may elect for an audio-based CAPTCHA test.[2]

Captchas are sometimes called "reverse Turing tests": because they are intended to allow a computer to determine if a remote client is human or not. In spite of their importance, their extremely widespread use, and a growing number of research studies there is currently no systematic methodology for designing or evaluating captchas. In fact, as we substantiate by thorough study, many popular websites still rely on schemes that are vulnerable to automated attacks.

Analysis of the resulting data reveals that CAPTCHAS are often difficult for humans, with audio captchas being particularly problematic. Demographic trends indicating, for example, that non-native speakers of English are slower in general and less accurate on English-centric captcha schemes. There is a limit to the distortion and noise that humans can tolerate in a challenge of a text CAPTCHA. Usability is always an important issue in designing a CAPTCHA. With advances of segmentation and Optical Character Recognition (OCR) technologies, the capability gap between humans and bots in recognizing distorted and connected characters becomes increasingly smaller. This trend would likely render text CAPTCHAs eventually ineffective.

Finding alternative approaches in designing CAPTCHAs to replace text CAPTCHAs has become increasingly important. A major effort has been directed to developing CAPTCHAs based on image or object recognition. Images are rich in information, intuitive to humans, and of a large variation. More importantly Images seem to be a better medium than characters for designing CAPTCHAs. To archive human knowledge and to make information more accessible to the world, multiple projects are currently digitizing physical books that were written before the computer age. The book pages are being photographically scanned, and then, to make

them searchable, transformed into text using "Optical Character Recognition" (OCR)

II. APPLICATIONS OF CAPTCHAs

CAPTCHAs have several applications for practical security, including

A. *Preventing Comment Spam in Blogs*
Most bloggers are familiar with programs that submit bogus comments, usually for the purpose of raising search engine ranks of some website (e.g., "buy penny stocks here"). This is called comment spam. By using a CAPTCHA, only humans can enter comments on a blog. There is no need to make users sign up before they enter a comment, and no legitimate comments are ever lost!

B. *Protecting Website Registration*
Several companies (Yahoo!, Microsoft, etc.) offer free email services. Up until a few years ago, most of these services suffered from a specific type of attack: "bots" that would sign up for thousands of email accounts every minute. The solution to this problem was to use CAPTCHAs to ensure that only humans obtain free accounts. In general, free services should be protected with a CAPTCHA in order to prevent abuse by automated programs

C. *Online Polls*
With most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Mellon found a way to stuff the ballots using programs that voted for CMU thousands of times. CMU's score started growing rapidly. The next day, students at MIT wrote their own program and the poll became a contest between voting "bots." MIT finished with 21,156 votes, Carnegie Mellon with 21,032 and every other school with less than 1,000. Can the result of any online poll be trusted? Not unless the poll ensures that only humans can vote.

D. *Preventing Dictionary Attacks*
CAPTCHAs can also be used to prevent dictionary attacks in password systems. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins.

E. *Search Engine Bots*
It is sometimes desirable to keep web pages unindexed to prevent others from finding them easily. There is an html tag to prevent search engine bots from reading web pages. The tag, however, doesn't guarantee that bots won't read a web page; it only serves to say "no bots, please." Search engine bots, since they usually belong to large companies, respect web pages that don't want to allow them in. However, in order to truly guarantee that bots won't enter a web site, CAPTCHAs are needed.

F. *Worms and Spam*
CAPTCHAs also offer a plausible solution against email worms and spam: "I will only accept an email if I know there is a human behind the other computer." A few companies are already marketing this idea.

III. ATTACKS ON TEXT BASED CAPTCHA

A history of how CAPTCHA has been adopted over the years is instructive. Larger sites adopted CAPTCHA because their resources were easy to abuse for the purposes of sending spam or conducting anonymous, illegal activity.As a result CAPTCHAsare widely used than before, which becomes the common part of current website login system. However, the CAPTCHA implementation is tricky and risky without deliberate design. With some specialized methods, the CAPTCHA scheme in its website can be easily cracked[3].

- Text-based CAPTCHAs are definitely less "**secure**" than their image/audio counterparts.
- While accessible to visually impaired users, logic questions require greater cognitive ability than image CAPTCHAs.
- Neural Networks can be used to train and recognize text based CAPTCHA.
- Heuristic checks: Heuristics are discoveries in a process that seem to indicate a given result. It may be possible to detect the presence of a robotic user based on the volume of data the user requests, series of common pages visited, IP addresses, data entry methods, or other signature data that can be collected.
- Online CAPTCHA Services: Emergence online CAPTCHA breaking services had made it possible to hijack CAPTCHA without any effort by the user.

IV. OPTICAL CHARACTER RECOGNITION

Optical character recognition, usually abbreviated to **OCR**, is the mechanical or electronic conversion of scanned images of handwritten, typewritten or printed text into machine-encoded text[4]. It is widely used as a form of data entry from some sort of original paper data source, whether documents, sales receipts, mail, or any number of printed records. It is a common method of digitizing printed texts so that they can be electronically searched, stored more compactly, displayed on-line, and used in machine processes such as machine translation, text-to-speech and text mining. OCR is a field of research in pattern recognition, artificial intelligence and computer vision .Early versions needed to be programmed with images of each character, and worked on one font at a time. "Intelligent" systems with a high degree of recognition accuracy for most fonts are now common. Some systems are capable of reproducing formatted output that closely approximates the original scanned page including images, columns and other non-textual components

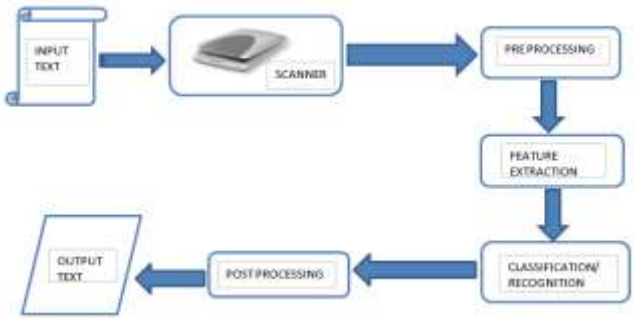

Figure 2 the basic Working of an Optical character recognition system [4]

Due to high development cost and requirement of highly skilled programmer there are very few open source OCR Engines available. This section gives introduction to major Open source engines.

A. **GOCR (JOCR):** GOCR is an OCR (Optical Character Recognition) program, developed under the GNU Public License. It converts scanned images of text back to text files. Started by Joerg Schulenburg the program, GOCR can be used with different front-ends, which makes it very easy to port to different OSs and architectures. It can open many different image formats, andGOCR can handle single-column sans-serif fonts of 20–60 pixels in height. It reports trouble with serif fonts, overlapping characters, handwritten text, heterogeneous fonts, noisy images, large angles of skew, and text in anything other than a Latin alphabet. GOCR can also be used to translate barcodes.

B. **Tesseract OCR Engine:** Tesseract is a free softwareoptical character recognition engine for various operating systems. Originally developed as proprietary software at Hewlett-Packard, it had very little work done on it in the following decade. It was then released as open source in 2005 by Hewlett Packard and UNLV. Tesseract development has been sponsored by Google since 2006.[6] It is released under the Apache License, Version 2.0.

Tesseract is probably the most accurate open source OCR engine available. Combined with the Leptonica Image Processing Library it can read a wide variety of image formats and convert them to text in over 60 languages. It was one of the top 3 engines in the 1995 UNLV Accuracy test. Between 1995 and 2006 it had little work done on it, but since then it has been improved extensively by Google. It is released under the Apache License 2.0.Tesseract was in the top 3 OCR engines in terms of character accuracy in 1995. It is available for Linux, Windows and Mac OS X, however, due to limited resources only Windows and Ubuntu are rigorously tested by developers.

The initial versions of Tesseract could only recognize English language text. Starting with version 2 Tesseract was able to process various languages including indian scripts. Almost all Indian scripts are cursive in nature making them hard to recognize by machines. Scripts like Devanagari, Gujarati, Bengali and many others have conjuncts or joint-characters increasing segmentation difficulties. To add to that, various fonts of various sizes used for printing texts over the years, the quality of paper, scanning resolution, images in texts etc asks for a challenging image processing job. Also, it requires huge linguistic know-how to apply post-processing.

V. RELATED WORK

Tamang, T. et al, 2012 [6] the authors delineate Presently, CAPTCHA is an vital mechanism to gain admission to the needed system. Though, there are a little difficulties for users in typing CAPTCHA even though they are authorized persons. As the Text-based CAPTCHA is the most accepted mechanism amongst all the CAPTCHA methods, the difficulties of this text-based are learned and drawn out. The aftermath of this discover have shown that the gave character(s), genders of users, and their educational background are a little of the vital factors ascertaining the correctness of CAPTCHA typing by its users. Therefore, producing a Text-based CAPTCHA have to use the appropriate character(s), that additionally joining alongside the educational background and genders of the users.

Kuo-Feng Hwang et al., 2012 [7] The authors delineate CAPTCHA has been extensively utilized for stopping malicious plans to admission web resources automatically. In this paper, a new kind CAPTCHA arrangement will be proposed. The counseled scheme, shouted Click spell, joined the features of text-based and image-based CAPTCHAs. Click spell asks users to spell a randomly selected word by clicking distorted messages for bypassing the test. Users can discover the definition(s) of the selected word. In supplement, Click spell can add an advertisement picture optionally. Cheers to the advertisement picture, Click spell enhanced the skill of confrontation to the attack by malicious programs. Their preliminary examination displayed that Click spell is useful in the aspects of protection and usability.

Saxena, A. et al., 2012 [8] The authors delineate CAPTCHAs are popularly utilized methods to discriminate humans and automated applications. Such methods are frequently functional in investment deals, email conception, online surveys, data downloads etc. Starting from a extremely primitive period of bestowing the users alongside a easy alphabetical thread to asking employing to do convoluted calculations, CAPTCHAs have come a long method in words of refinement of human-bot distinction. Though in this procedure, these CAPTCHAs have capitulated their human friendliness, whichever because of the sound being added to the CATPCHA examinations or because of the complications of the trials thrown to the user emerging in bad experience. The established CAPTCHAs additionally flounder to seize into report the exceptional needs of the omnipresent mobile devices. These mobile mechanisms have insufficient limitations like tiny display span, manipulated display

resolution, color combinations of the display, processing manipulation etc. Also, they have exceptional gains of stroke sensitive input mechanisms, voice inputs, voice outputs etc. In this paper, they present a scheme for a CAPTCHA ability on Cloud, that is specific to mobile application. They duly ponder the demand of usability and presentation that is needed for a mobile mechanism in their implementation. The counseled CAPTCHA framework proposals scalable and flexible implementation opportunities in countless verticals and domains. One more exceptional feature of their framework is that they furnish the ability for distributed verification. This considerably enhances the efficiency at the CATPCHA creation as well as reduces the reply period for the user authentication as human.

D'Souza, D. et al., 2012 [9] The authors delineate this paper introduces Avatar CAPTCHA, an picture established way to discriminate human users from computer plans (bots). The counseled CAPTCHA asks users to recognize avatar faces from a set of 12 grayscale pictures encompassed of a blend of human and avatar faces. Experimental aftermath indicate that it can be resolved 62% of the period by human users alongside an average accomplishment period of 24 seconds and a affirmative user locale of 90%. It is projected to be safeguard opposing computer plans (bots). Employing brute power attack the accomplishment rate for a bot to resolve it is 1/4096.

Kiran Jain Azad et al., 2013 [10] In this scrutiny paper The frank trial in arranging these obfuscating CAPTCHAs is to make them facile plenty that users are not dissuaded from endeavoring a resolution, yet too tough to resolve employing obtainable computer vision algorithms. As Current knowledge grows this gap though becomes slimmer and thinner. It is probable to enhance the protection of an continuing text CAPTCHA by system-apically adding sound and distortion, and arranging acts extra tightly. These measures, though, should additionally make the acts harder for humans to understand, emerging in a higher error rates and higher Web burden .This paper presents insufficient of most alert aggressions on text CAPTCHAs continuing today.

Achint Thomas et al., 2013 [11] In this paper Interactive websites use text-based Captchas to stop unauthorized automated interactions. These Captchas have to be facile for humans to decipher as being tough to crack by automated means. In this work they present a framework for the systematic discover of Captchas alongside these two contesting objectives. They onset by abstracting a set of distortions that describe present and past business text-based Captchas. By way of user studies, they quantify the method human Captcha resolving presentation varies alongside adjustments in these distortion parameters. To quantify the result of these distortions on the accuracy of automated solvers (bots), they counsel a learning-based algorithm that performs automated Captcha segmentation driven by character recognition. Aftermath display that their counseled algorithm is generic plenty to resolve text-based Captchas alongside extensively fluctuating distortions lacking needing the use of hand coded picture processing or heuristic rules.

Quan-Bin Ye et al., 2013 [12] The authors delineate A CAPTCHA (Completely Automated Area Turing examination to notify Computers and Humans Apart) is a protection mechanism that can be utilized to discriminate amid humans and machines. Most continuing CAPTCHA arrangements are vulnerable opposing a so-called "third party human attack." The third party human attack employs retained human to resolve trials so that the CAPTCHA arrangements will no longer be effective. In this paper, they design an effectual and competent aspect to protect the attack. Pursuing the aspect, they design and examine a novel CAPTCHA arrangement, Drag-n-Drop Interactive Masking CAPTCHA (DDIM CAPTCHA), to deal alongside both the established aggressions and the third party human attack. The DDIM CAPTCHA retains the frank necessities of CAPTCHAs and adds the properties of contact and masking. Across a sequence of analyses and examinations, the counseled Drag-n-Drop CAPTCHA can be asserted to be a good way for placement to remedy the flaws of present CAPTCHA systems.

Tao Men et al., 2013 [13] The authors delineate CAPTCHA (also recognized as verification code) is generally utilized to promise the login protection of the interactive websites. At present, the most accepted verification program is picture CAPTCHA that can discriminate the human user from the computer by recognizing acts in the image. Even though the picture CAPTCHA is harmless at commencing, outstanding deals of CAPTCHAs have been cracked by the computers alongside the progress of picture processing knowledge and manmade intellect technology. This paper presents a new vibrant CAPTCHA established on inverted color. The acts color and the background color in the CAPTCHA are inverted suitably, the interference lines are added in the foreground picture and multi-frame vibrant pictures are compounded to safeguard the CAPTCHA has larger discernible results, and therefore, it is facile for the human to individuality the real data as hard to remove the interference data by normal picture processing technology. Hypothetical scrutiny and simulation examinations clarify that the CAPTCHA is harmless and efficient.

YunhangShen et al., 2014 [14] In this paper, they discover the trial of hacking CAPTCHA (Completely Automated Area Turing examination to notify Computers and Humans Apart), that is extensively utilized to recognize contraption and human in webpage registration and authorization. Extra specially, they target at to click Chinese CAPTCHA that is presently accepted in mobile request scenario, that is far extra challenging and left unexploited in scrutiny previously. Their main believed is a multiscale Corner established Construction Ideal termed CSM alongside a extremely effectual outline matching, that is amazingly precise in seizing the intrinsic statistics of to click Chinese CAPTCHA opposing the others.

Max Jaderberg et al., 2014 [15] In this work they present a framework for the credit of usual scene text. Their framework does not need each human-labeled data, and performs word credit on the finished picture holistically, departing from the character established credit arrangements of the past. The deep neural web models at the center of this framework are trained merely on data produced by a synthetic text creation engine –

synthetic data that is exceedingly realistic and adequate to substitute real data, providing us infinite numbers of training data. This excess of data exposes new possibilities for word credit models, and here they ponder three models, every single one "reading" words in a disparate way: via 90k-way lexicon encoding, character sequence encoding, and bag-of-N-grams encoding.

Min Wang et al., 2014 [16] In this scrutiny paper CAPTCHA is a completely automated plan projected to discriminate whether the user is a computer or human. As the setbacks of Internet protection are worsening, it is of outstanding meaning to do scutiny on CAPTCHA. This article starts from the credit of CAPTCHAs, next analyses the flaws in its design and gives corresponding credit propositions according to assorted flaws, in the end proposals suggestions connected to the enhancement of CAPTCHAs. Firstly, this article briefly introduces the frank steps across the decoding procedure and their principles. And across every single pace they select methods that are larger adapted to the features of disparate CAPTCHA images.

HaichangGao et al., 2014 [17] In this paper CAPTCHA is nowadays usually utilized as average protection knowledge to notify computers and humans apart. The most extensively used CAPTCHAs are text-based schemes. In this paper, they document how they have broken such a text-based scheme that uses the "connecting acts jointly (CCT)" principle. CAPTCHAs of this kind can be categorized into three types: CAPTCHA alongside overlap but no sound arcs; CAPTCHA alongside sound arcs but no overlap; and CAPTCHA lacking sound arcs and overlap. Yahoo!, Baidu CAPTCHA and reCAPTCHA were selected as representatives of the three types.

AriyanZarei et al., 2014 [18] This paper bestowing protection for web servers opposing unwanted and automated registrations has come to be a large concern. To stop these kinds of fake registrations countless websites use CAPTCHAs. Amid all kinds of CAPTCHAs OCR-Based or discernible CAPTCHAs are extremely common. Truly discernible CAPTCHA is an picture encompassing a sequence of characters. So distant most of discernible CAPTCHAs, in order to challenge opposing OCR plans, use a little public implementations such as cloaking the acts, random arrangement and rotations of acts, etc. In this paper they requested Gaussian Blur filter, that is an picture makeover, to discernible CAPTCHAs to cut their readability by OCR programs. They finished that this method made CAPTCHAs nearly unreadable for OCR plans but, their readability by human users yet stayed high.

Zhu, B.B. et al, 2014 [19] The authors delineate Countless protection primitives are established on hard mathematical problems. Employing hard AI setbacks for protection is growing as an thrilling new paradigm, but has been under-explored. In this paper, they present a new protection primitive established on hard AI setbacks, namely, a novel relations of graphical password arrangements crafted on top of Captcha knowledge, that they call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of protection setbacks totally, such as online estimating aggressions, relay aggressions, and, if joined alongside dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be discovered merely probabilistically by automatic online estimating aggressions even if the password is in the find set. CaRP additionally proposals a novel way to address the well-known picture hotspot setback in accepted graphical password arrangements, such as Bypass Points that frequently leads to frail password choices. CaRP is not a panacea, but it proposals reasonable protection and usability and appears to fit well alongside little useful requests for enhancing online security.

Carlos Javier Hernández-Castro et al., 2015 [20] In this scrutiny paper Human Interactive Proofs (HIPs) are a frank protection compute on the Internet to circumvent countless kinds of automatic attacks. Recently, a new HIP has been projected to raise security: the Political Entitlements CAPTCHA. It employs the empathy capacity of humans to more reinforce the protection of a well recognized OCR CAPTCHA, Scrimmage. In this paper, they investigate it from a protection outlook, pointing out its design flaws. Then, they craft a prosperous side-channel attack, leveraging a little well-known contraption discovering algorithms.

Miss. Desai Sucheta ,2015 [21] In this paper we focus on differentpossibilities or ways of DOS attack as wellas detection and prevention of DOS attack.In this paper, we coveredan overview of the DoS problem, availableDoS attack tools, defense challenges andprinciples, and a classification of availableDoS prevention mechanism.This paper will give the detailsof plan and implementation of applicationwhich will detects and prevents DOS attack.

VI. CONCLUSION

Over the past few years, an increasing number of public web services have attempted to prevent exploitation by bots and automated scripts, by requiring a user to solve a Turing-test challenge (commonly known as a CAPTCHA – Completely Automatic Public Turing test to tell Computers and Human Apart) before using the service. These efforts may be crucial to the success of these sites in various ways. For example, Gmail improves its service by blocking access to automated spammers, eBay improves its marketplace by blocking bots from flooding the site with scams, and Facebook limits creation of fraudulent profiles used to spam honest users or cheat at games. Any CAPTCHA has two main demands: (a) be easy for human to solve and (b) be very hard for a computer script to solve. Those to demands appear to contradict with each other. In the reality where the OCR, image recognition and Machine Learning techniques are well studied it is very hard to design a good CAPTCHA that will still be solvable by humans.

VII. FUTURE SCOPE

There is a constant need to improve current CAPTCHAs and to develop new CAPTCHAs in order to safely secure against developing programs which can create thousands of e-mail accounts used for malicious purposes, stuff online polls with ballots, and develop worms and viruses contained in emails. New CAPTCHAsare still in development and are being tested

against known attacks on other CAPTCHAs as well as other possible attacks. CAPTCHAs are now being more and more used in businesses to protect against intruders so it is essential that current CAPTCHAs APIs be improved upon in terms of success rate in order to prevent a computerized attack on a system holding sensitive data. Main Focus of future work is to find out the Probabilities of finding out the real text behind a given CAPTCHA API service. To find such a probability we will have to first, implement and study CAPTCHA APIs. The Online OCR of CAPTCHAs form API Services will be implemented in Tesseract.

VIII. REFERENCES

[1]. Motoyama, Marti, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. "Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context." In USENIX Security Symposium, vol. 10, pp. 4-1. 2010.

[2]. Von Ahn, Luis, Manuel Blum, Nicholas J. Hopper, and John Langford. "CAPTCHA: Using hard AI problems for security." In Advances in Cryptology—EUROCRYPT 2003, pp. 294-311. Springer Berlin Heidelberg, 2003.

[3]. Doan, anhai, raghuramakrishnan, and alon y. Halevy. "crowdsourcing systems on the world-wide web." communications of the acm 54, no. 4 (2011): 86-96.

[4]. Mori, Shunji, Hirobumi Nishida, and Hiromitsu Yamada. Optical character recognition. John Wiley & Sons, Inc., 1999.

[5]. Smith, Ray. "An Overview of the Tesseract OCR Engine." In ICDAR, vol. 7, pp. 629-633. 2007.

[6]. Tamang, Tsheten, and PattarasineeBhattarakosol. "Uncover impact factors of text-based CAPTCHA identification." In Computing and Convergence Technology (ICCCT), 2012 7th International Conference on, pp. 556-560. IEEE, 2012.

[7]. Kuo-Feng Hwang, Cian-Cih Huang, and Geeng-Neng You. "A Spelling based CAPTCHA system by using click." In Biometrics and Security Technologies (ISBAST), 2012 International Symposium on, pp. 1-8. IEEE, 2012.

[8]. Saxena, Ashutosh, Nitin Singh Chauhan, K. R. Sravan, AparajithSrinivasanVangal, and David Palacios Rodrguez. "A new scheme for mobile based CAPTCHA service on Cloud." In Cloud Computing in Emerging Markets (CCEM), 2012 IEEE International Conference on, pp. 1-6. IEEE, 2012.

[9]. D'Souza, Darryl, Phani C. Polina, and Roman V. Yampolskiy. "Avatar captcha: Telling computers and humans apart via face classification." In Electro/Information Technology (EIT), 2012 IEEE International Conference on, pp. 1-6. IEEE, 2012.

[10]. Kiran Jain Azad, "CAPTCHA: Attacks and weaknesses against OCR Technology." Global Journal of Computer Science and Technology 13, no. 3 (2013).

[11]. Achint Thomas, KunalPunera, Lyndon Kennedy, Belle Tseng, and Yi Chang. "Framework for evaluation of text captchas." In Proceedings of the 22nd international conference on World Wide Web companion, pp. 159-160. International World Wide Web Conferences Steering Committee, 2013.

[12]. Ye, Quan-Bin, Te-En Wei, Albert B. Jeng, Hahn-Ming Lee, and Kuo-Ping Wu. "DDIM-CAPTCHA: A Novel Drag-n-Drop Interactive Masking CAPTCHA against the Third Party Human Attacks." In Technologies and Applications of Artificial Intelligence (TAAI), 2013 Conference on, pp. 158-163. IEEE, 2013.

[13]. Men, Tao, Deming Wang, Yan Sun, and Mingrong Wang. "A novel dynamic CAPTCHA based on inverted colors." In Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on, pp. 796-799. IEEE, 2013.

[14]. YunhangShen, RongrongJi, Donglin Cao, and Min Wang. "Hacking Chinese Touclick CAPTCHA by Multi-Scale Corner Structure Model with Fast Pattern Matching." In Proceedings of the ACM International Conference on Multimedia, pp. 853-856. ACM, 2014.

[15]. Max Jaderberg, Karen Simonyan, Andrea Vedaldi, and Andrew Zisserman. "Synthetic data and artificial neural networks for natural scene text recognition." arXiv preprint arXiv:1406.2227 (2014).

[16]. Min Wang, Tianhui Zhang, Wenrong Jiang, and Hao Song. "The recognition of CAPTCHA." Journal of Computer and Communications 2, no. 02 (2014): 14.

[17]. HaichangGao, Wei Wang, Ye Fan, Jiao Qi, and Xiyang Liu. "The Robustness of "Connecting Characters Together" CAPTCHAs." Journal of Information Science and Engineering 30, no. 2 (2014): 347-369.

[18]. AriyanZarei, "Improve CAPTCHA's Security Using Gaussian Blur Filter." arXiv preprint arXiv:1410.4441 (2014).

[19]. Zhu, B., Jeff Yan, GuanboBao, M. Mao, and NingXu. "Captcha as Graphical Passwords–A New Security Primitive Based on Hard AI Problems." (2014): 1-1.

[20]. Carlos Javier Hernández-Castro, David F. Barrero, and María D. R-Moreno. "A Machine Learning Attack against the Civil Rights CAPTCHA." In Intelligent Distributed Computing VIII, pp. 239-248. Springer International Publishing, 2015.

[21]. Miss. Desai Sucheta ,Miss.AnushkaPawar, Miss.RenusheTejasvita, Mr.Naik L. S. "Survey on Dos Attack detecton: Location guard and Captcha." In Rajendra Mane College of Engineering & Technology, Ambav, Devrukh. In International Journal of Engineering Trends and Technology (IJETT) – Volume22 Number 4- April2015.

.