Framework for Evaluating CAPTCHA Security against Advanced AI Models

Ritika Sharma, Neha Chauhan

Department of Electronics and Communication Engineering, KIET Group of Institutions, Ghaziabad, India

ABSTRACT

The ability area between people and bots in acknowledging connected and distorted figures becomes progressively smaller with advances of segmentation and Optical Character Recognition (OCR) technologies. This trend would likely make text CAPTCHAs APIs eventually ineffective. The procedure this is certainly fundamental creating these obfuscations is to cause them to become quick sufficient that users aren't dissuaded from attempting an answer, but nonetheless also hard to solve making use of provided computer system system vision formulas. Principal Focus for this jobs are to find the possibilities away from learning the written text that is real a given CAPTCHA API. This is actually open generation, such as for example Tesseract to find such a probability we have to first, Implementation a CAPTCHA Generation Algorithm in a programming language utilizing some CAPTCHA. Then apply Image Heuristics of CAPTCHA Image that is including alignment Noise Reduction filters etc. The CAPTCHA's Heuristics alongside Filtering information will be wanted to an OCR Library, such as GOCR to search for the CAPTCHA's Text out in the Decryption that is main algorithm. Eventually, chance for effective CAPTCHA are analyzed for every comments CAPTCHA and system this is really total is determined. Some practices we now have discussed in this thesis provide more than 70% rate of success, so when the faulty CAPTCHA demands are re-evaluated by the lack and number count this is really limiting that CAPTCHA decryption will probably be efficient in successive assaults.

INTRODUCTION

CAPTCHA (Computers and Humans Apart from fully automatic to inform area Turing Test), additional human interactive proof (HIP) is recognized as the two tests and the grading of the answers in the creation of an automated computer program Turing test is given by. CAPTCHAs artificial intelligence (AI) to plan the overthrow of the current computer or can not be solved by bots are installed on, but that are solvable by humans hurry. The word "captcha" Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford (all of Carnegie Mellon University) was created in 2003 by [1]. This is a term that include "capture" and the "fully automatic field Turing test to inform Computers and Humans Apart" to stand is for. In other word it is a test that can distinguish humans from computers to portray. Basic requirement of this test wis

1. Easily solved by humans
2. Easily generated and evaluated, but
3. Not easily solved by computer

Over the past decade, captchas can be generated by different number of ways number of different ways, each one painted quality to meet the fluctuating degrees. CAPTCHAs most commonly observable tests showed a photo of the user that needs a little combination of sound and distortion present in obfuscated alphanumeric functions are to identify.

The trial this is certainly honest organizing these problems is to cause them to become facile plenty that people are not delayed from endeavoring an answer, however yet too tough to solve using obtainable computer sight algorithms. Text CAPTCHAs are almost entirely utilized in genuine applications. In a text CAPTCHA, acts are intentionally related and altered to get rid of credit by bots.

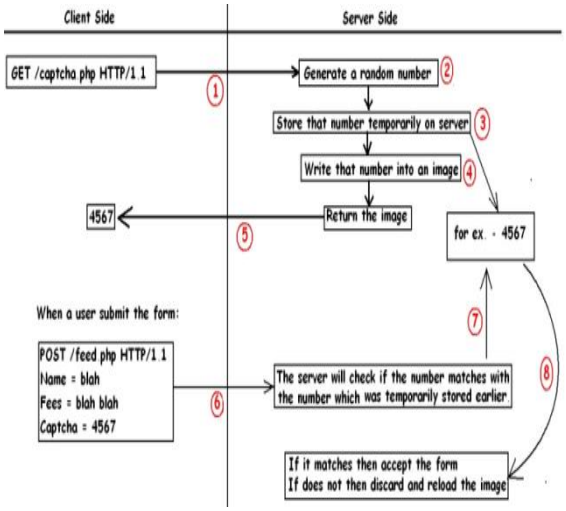


Figure 1 Working of CAPTCHA [5]

1) Working of CAPTCHA

First enable myself give a brief believed concerning how the CAPTCHA works in an internet application.Firstly the client produces CAPTCHA and dispatch it to the host next host makes the quantity that is arbitrary shops that number temporarily in the server next the server each and every and every single duration yields a picture alongside an innovative new random digit and include that number into an image and returns that picture to the client. In order to make this clearer, Allow me offer you an illustration :- Presume afterward onset the feedback type you became text that is insufficient and a CAPTCHA. Presume at a period of time that is exact CAPTCHA filled alongside lots for ex. "4567". So if you use that program "4567" the form is going to be provided prosperously. Now if you try to provide the proper execution alongside the quantity that is diffrent's was filled preceding alongside the disparate type, next the request will not accord that form. If you go in the CAPTCHA this is certainly proper next demand will accord that kind.

2) Limitations of CAPTCHA

1. Usability is always an important factor in designing a CAPTCHA.
2. You'll be able to improve the security of the text this is certainly present adding sound and distortion, and arranging figures more firmly.
3. But There is a limit to the distortion and noise that humans can tolerate in a challenge of a text CAPTCHA.
4. These measures, however, would also make the characters harder for humans to recognize, resulting in a higher error.

1) Attacks on Text based CAPTCHA

A last of exactly how CAPTCHA happens to be followed above the complete many years is instructive. Larger places used CAPTCHA because their particular resources had been facile to mistreatment when it comes to motives of dispatching spam or leading nameless, illegal activity. As a consequence CAPTCHAs are extensively used than ahead of time, that becomes the general public percentage of present login system this is certainly site. Though, the CAPTCHA execution is complex and risky lacking design this is certainly deliberate. The CAPTCHA plan with its website could be facilely cracked with only a little enumerated practices.

- Text-based CAPTCHAs are definitely less "secure" than their image/audio counterparts.
- While accessible to visually weakened users, reasoning questions require greater ability this is certainly intellectual image CAPTCHAs.
- Neural Networks can be used to train and recognize text based CAPTCHA.

INTRODUCTION CAPTCHA APIS (RECAPTCHA)

reCAPTCHA and supplementary CAPTCHA API ability providers validate an incredible number of CAPTCHAs every day that is single protect thousands of internet sites opposing the bots. A safeguard CAPTCHA validation and creation ecosystem forms the basis associated with the general public belief perfect

amid the CAPTCHA provider together with consumer. A collection of damage can transpire if each constituent of this ecosystem is compromised.

CAPTCHA API Woking

CAPTCHA API providers typically proposal both CAPTCHA validation and creation solutions. The subscribing web pages whichever utilize the continuing libraries and plugins; or comprise their particular to eat these types of services. A person that is regular alongside an internet request that relies on a CAPTCHA provider is summarized below:

1. A person demands a full page that needs CAPTCHA validation.
2. The came back web page contains an embedded <img> (or <script>) label to recover the CAPTCHA picture from the CAPTCHA provider.
3. Upon parsing the embedded tags, the browser retrieves a CAPTCHA from the CAPTCHA provider and displays it to your individual.
4. The user fills when you look at the form industries, enters the CAPTCHA answer and submits the page to the web application.
5. The web application then submits the CAPTCHA treatment for the CAPTCHA supplier for confirmation.
6. The CAPTCHA supplier responds to your internet application with failure or fortune message.
7. predicated on CAPTCHA provider's response, the web application enables or denies the demand.

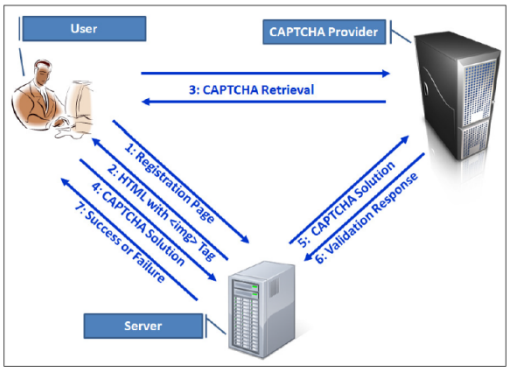


Fig 2 A typical validation flow with CAPTCHA providers

8. Steps 5 and 6 play a crucial role in the CAPTCHA validation scheme and must be securely implemented to prevent attacks against CAPTCHA validation process.

RELATED WORK

Matt. May et al., 2005 [1] In this research paper a common method of limiting access to services made available over the Web is visual verification of a bitmapped image. This paper presents a major problem to users who are blind, have low vision, or have a learning disability such as dyslexia. This document examines a number of potential solutions that allow systems to test for human users while preserving access by users with disabilities.

Jon Bentley et al., 2006 [2] This paper makes two primary contributions to CAPTCHA engineering. The first is applying the framework of assurance to the area, and thereby quantifying an important property of any CAPTCHA: how much assurance does the challenge string provide against various attackers? They apply a preliminary version of this theory to "Implicit CAPTCHAs" in which the user clicks on a navigation aid, potentially without even realizing that he has thereby passed a test.

Mohammad Hassan Shirali-Shahreza et al., 2006 [3] In this research paper Nowadays, many daily human activities such as education, trade, talks, etc are done by using the Internet. In such things as registration on Internet web sites, hackers write programs to make automatic false registration that waste the resources of the web sites while it may also stop it from functioning. Therefore, human users should be distinguished from computer programs. To this end, this paper presents a method for distinction of Persian and Arabic-language users from computer programs based on Persian and Arabic texts. Their proposed algorithm is based on adding a background to the image of a meaningless Persian/Arabic randomly generated word. This method relies on the

difficulty of automatic separation of background from Persian/Arabic writing, due to the presence of many diacritical dots and signs.

Andy Schlaikjer et al., 2007 [4] This work focuses on development of an alternative aural CAPTCHA technology based on a speech transcription task. The principal goals of this paper are

(1) to provide a better quality of service for visually impaired web users who currently have few alternatives for accessing web services protected by CAPTCHAs based on visual perception tasks,
(2) as a side effect of CAPTCHA use, collect meaning data, such as transcriptions of speech found in online audio streams, and
(3) deploy the CAPTCHA publicly to increase the general awareness of accessibility concerns on the web for users with disabilities.

Toward these ends, an experimental corpus of human transcriptions of short audio clips was created to support aural CAPTCHA experimentation. Results suggest that the techniques investigated represent viable aural reCAPTCHA mechanisms.

Jeremy Elson et al., 2007 [5] In this research paper they present Asirra, a CAPTCHA that asks users to identify cats out of a set of 12 photographs of both cats and dogs. Asirra is easy for users; user studies indicate it can be solved by humans 99.6% of the time in fewer than 30 seconds. Barring a major advance in machine vision, they expect computers will have no better than a 1/54,000 chance of solving it. Asirra's image database is provided by a novel, mutually beneficial partnership with Petfinder.com. In exchange for the use of their three million images, they display an "adopt me" link beneath each one, promoting Pet finder's primary mission of finding homes for homeless animals. They describe the design of Asirra, discuss threats to its security, and report early deployment experiences. They also describe two novel algorithms for amplifying the skill gap between humans and computers that can be used on many existing CAPTCHAs.

Graig Sauer et al., 2008 [6] In this research paper CAPTCHAS are widely used on websites to differentiate between humans and computers. Audio CAPTCHAs provide an alternative interface that is accessible to blind users and users with low vision who are unable to see visual CAPTCHAs. They present a small user study suggesting that one existing audio CAPTCHA is highly error prone and time consuming. They propose a new CAPTCHA solution that combines audio sounds (e.g., bird chirping) and visual images (e.g., bird). Preliminary user tests of this new solution have been highly encouraging.

Jeff Yan et al., 2008 [7] In this research paper CAPTCHA is now almost a standard security technology, and has found widespread application in commercial websites. Usability and robustness are two fundamental issues with CAPTCHA, and they often interconnect with each other. This paper discusses usability issues that should be considered and addressed in the design of CAPTCHAs. Some of these issues are intuitive, but some others have subtle implications for robustness (or security). A simple but novel framework for examining CAPTCHA usability is also proposed.

Chun-Ming Leung 2009 [8] The authors describe Addressing recent online banking threats, the main challenges are to enable safe online banking on a compromised host, and solving the general ignorance of security warning. There are costly hardware solutions proposed for login authentication to transaction verification. However, they are always looking for a usable solution with higher acceptance and less effort. CAPTCHA is primarily used to anti bot automated login, also, CAPTCHA base application can further provides secure PIN input against key logger and mouse-logger for Bank's customer. However, assuming users are always unconscious of security warning, under this interesting condition, CAPTCHA alone is nothing to anti-phishing. But, the CAPTCHA idea is still worth to be developed. In this paper, they present the Extended CAPTCHA Input System (ECIS), which they firstly extend the CAPTCHA idea to defend Real-Time Man-In-The-Middle (RT-MITM) attack and their proposed CR-MITM attack. The trick is to employ a moving CAPTCHA for input of One Time-Password (OTP) with time restriction, which can depress MITM auto-relaying of information as well as human assisted MITM attack. Their solution reuses the large scale shipped OTP token which can save huge amount of money instead of re-design and shipping of a new hardware solution.

Bin B.Zhu et al., 2010 [9] In this research paper they systematically study the design of image recognition CAPTCHAs (IRCs) in this paper. They first review and examine all IRCs schemes known to us and evaluate each scheme against the practical requirements in CAPTCHA applications, particularly in large-scale real-life applications such as Gmail and Hotmail. Then they present a security analysis of the representative schemes they have identified. For the schemes that remain unbroken, they present their novel attacks. For the schemes for which known attacks are available, they propose a theoretical explanation why those schemes have failed. Next, they provide a simple but novel framework for guiding the design of robust IRCs. Then they propose an innovative IRC called Cortcha that is scalable to meet the requirements of large-scale applications.

OCR and CAPTCHA Attacks

A powerful CAPTCHA picture design may be the basis for an anti-automation system this is certainly skilled. Like encryption, the CAPTCHA image design should be afflicted by scrutiny that is methodical its effectiveness opposing automatic text removal. An alarming number of sites rely on home-grown CAPTCHA picture sketches that suggestion protection that is slight subjected to common picture processing methods and OCR tools.OCR-assisted CAPTCHA brute-forcing An approach of brute-forcing CAPTCHAs is by leveraging OCR computer software. CAPTCHAs are duplicated innately and resolved offline employing a few motors that are OCR. Also, in the event that CAPTCHA implementation is susceptible to the in-session CAPTCHA brute-force vulnerability discussed above, the method this is certainly OCR-assisted be used to considerably cut the amount of endeavors needed seriously to calculate the proper resolution in a live HTTP session. The seeking practices current CAPTCHA that is OCR-assisted brute-force.

1) Each CAPTCHA is afflicted by several OCR engines, and aftermath tend to be combined. The image below displays an example whereas a CAPTCHA was subjected to two disparate machines which are OCR aftermath were combined. The picture assumes that the CAPTCHA implementation is vulnerable to an in-session CAPTCHA brute-force attack. Here the OCR1 endeavor shall dispatch rGsyg, provoking a deep failing. The OCR that is subsequent will r6sy9, yet again provoking the failure. As both the resolutions vary by two functions, they could be accompanied to get an answer r6syg that is right.

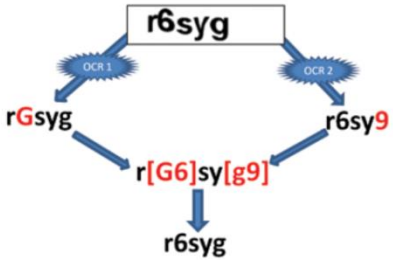


Figure 3 A CAPTCHA solutions that combines results of two difference OCR engines.

2) After removing text from CAPTCHA employing an OCR engine, a discerning brute-force can also be attempted. For example, let's accept that the effect is came back because of the OCR motor as TE5T12. The energy this is certainly brute begins by altering the early character "T" and maintaining the many benefits of the additional five characters—and next moves on into the subsequent personality and so forth. Later on this, two acts are brute-force in tandem, pursued by three, and over the length this is certainly whole. This technique, like supplementary brute-force methods is elevated on resource and duration necessities.

3) At periods, OCR motors could provide solutions being partly proper. Such circumstances, methods like simple character replacement techniques can be utilized to show up at correct CAPTCHA option. For instance, "l" is replaced by "I,""G" by "C," "S" by "5," and so on. The effectiveness of this technique can be improved if the CAPTCHA character set is recognized and next relevant substitutions can be carried out. As an example, it will likely be benign to substitute "5"with "S" to appear at the proper quality whenever we realize that CAPTCHA encompasses simply uppercase acts while the OCR quality encompasses a number "5.

THE CAPTCHA CLIPPING ATTACK

An attacker could possibly be in a position to impersonate the CAPTCHA supplier and undermine the anti automation protection because the website's request host deeds as a client to CAPTCHA supplier and the demand server regularly neglects to validate the CAPTCHA provider's individuality and the program integrity checks. CAPTCHA validation replies are generally Boolean (fake or true, accomplishment or wreck, bypass or flounder, 0 or 1). The answer structure and its particular content are additionally freely available as percentage of CAPTCHA provider's API documents. This permits an assailant to facilely build the set this is certainly finite of replies, impersonate the CAPTCHA provider, and current destructive CAPTCHA validation when it comes to request servers. To exploit this vulnerability an attacker performs the following:

1. The assailant acts as a application that is genuine and submits a lot of demands into the web application.
2. At the same time, he/she intercepts CAPTCHA validation requests, masquerades as the CAPTCHA provider and approves all submitted requests.

   Masquerading because the CAPTCHA provider and never forwarding the CAPTCHA validation demands to the CAPTCHA that is actual provider the CAPTCHA Clipping Attack.

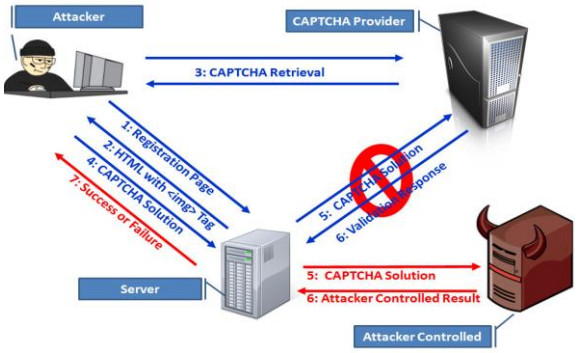


Fig 4 Image demonstrates CAPTCHA Clipping Attack

OPTICAL CHARACTER RECOGNITION

Optical character recognition, typically abbreviated to OCR, could be the technical or transformation this is certainly electric of images of handwritten, typewritten or imprinted text into machine-encoded text. Its thoroughly utilized as a type of information entry from a sort this is certainly little of report data foundation, whether papers, sales receipts, mail, or each wide range of printed records. It is a technique that is general public of imprinted texts so that they can be digitally hunted, kept additional compactly, exhibited on-line, and utilized in contraption procedures such as for instance contraption interpretation, text-to-speech and text mining. OCR is a earth of scutiny in outline credit, manmade intellect and computer eyesight.

Early versions demanded to be programmed alongside images each and every character this is certainly single and handled one font at the same time. "smart" arrangements alongside a degree this is certainly elevated of reliability for many fonts tend to be today common. Just a little arrangements are designed for replicating result this is certainly formatted closely approximates the first scanned page encompassing photographs, columns and supplementary non-textual elements.

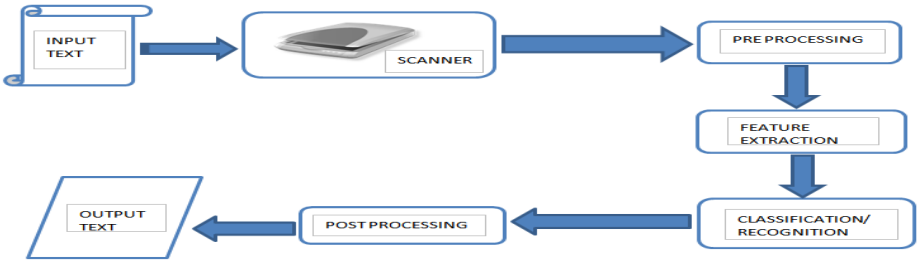


Fig 5: The basic Working of an Optical character recognition system.

Just about all scripts which can be indian cursive in the wild making all of them difficult to understand by devices. Programs like Devanagari, Gujarati, Bengali and countless others have conjuncts or joint-characters segmentation this is certainly rising. The standard of paper, scanning resolution, photographs in texts etc requests a challenging picture processing task to increase that, various fonts of assorted sizes used for creation texts above the many years. Additionally, it needs huge know-how that is linguistic implement post-processing.

APPLICATIONS OF OCR TECHNOLOGY

OCR technology has found various uses over the years it can be used but not limited to:

1. Data entry for business documents, e.g. check clearing
2. Automatic number plate recognition
3. Importing business card information into a contact list
4. More quickly make textual versions of printed documents, e.g. book scanning for Project Gutenberg
5. Make electronic images of printed documents searchable, e.g. Google Books
6. Converting handwriting in real time to control a computer (pen computing)
7. Defeating CAPTCHA antibot systems, though these are specifically designed to prevent OCR

In the 2000s, OCR happens to be made accessible as a web ability, in a cloud nature this is certainly computing, plus in mobile demands like real-time interpretation of foreign-language signals on a smart-phone. Various business and foundation this is certainly available plans tend to be accessible for the majority of public including plans, encompassing Latin, Cyrillic, Arabic, Hebrew, Indic, Chinese, Japanese, and Korean functions.

TYPES OF OCR SYSTEM

Intelligent personality recognition (ICR) - additionally targets handwritten print script or cursive text one glyph or personality at the same time, usually concerning machine discovering. Artificial neural systems could be made indifferent to both affine and transformations that are non-linear .Intelligent term recognition (IWR) - additionally targets handwritten print script or text that is cursive one word at the same time. This really is particularly helpful for languages where glyphs are not separated in cursive script. Steps involved in a OCR Process .OCR is usually an "offline" procedure, that analyzes a static document. Handwriting movement scurtiny can be utilized as input to handwriting recognition. There are assorted steps encompassed in it as follows

1. Binarization: Convert an image from color or grey scale to black-and-white (called a image that is "binary because there are two main colors). This will be required for the smoothness recognition algorithm; in other situations, the algorithm performs better on the original image and so this step is missed in some cases.
2. Line removal: Cleans up non-glyph boxes and lines
3. Layout "zoning" or analysis: Identifies columns, paragraphs, captions, etc. as distinct blocks. Especially crucial in multi-column layouts and tables.
4. Line and term detection: Establishes standard for character and word forms, separates words if necessary.
5. Character isolation: For per-character OCR, multiple characters which can be connected due to image artifacts needs to be separated; single characters which are broken into multiple pieces due to artifacts must be connected.
6. Normalize aspect scale and ratio

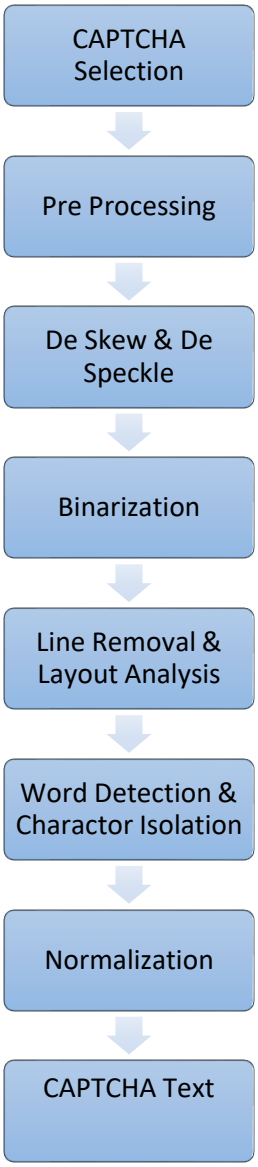


Fig 6 Steps involved in OCR Process for Text CAPTCHA

CHARACTER RECOGNITION

There are 2 honest kinds of core OCR algorithm, that could produce a catalog that is ranked of numbers. Matrix coordinating involves contrasting a photo to a kept glyph on a pixel-by-pixel foundation; it is also recognized as "pattern matching" or "pattern recognition". This relies on the feedback glyph being precisely remote from the others regarding the picture, and on the stored glyph becoming in a font this is certainly similar at the scale that is alike. This system is most effective alongside typewritten text and does not work very well after brand fonts that are brand-new encountered. This is actually the method the actual this is certainly OCR that is main required instead straight.Feature removal decomposes glyphs into "features" like lines, shut loops, range relationship, and range intersections. They are compared alongside an hypothetical representation that is vector-like of personality, which will cut to 1 or glyph this is certainly additional. Completed techniques of feature detection in computer sight is put on the kind of OCR, this is certainly typically identified in "intelligent" handwriting credit and even many OCR software this is certainly current. Nearest friend classifiers for example the k-nearest acquaintances algorithm are used to huge difference this is certainly huge features alongside saved glyph features and choose the match this is certainly nearest.

Post-processing-OCR precision can be increased if the output is constrained by a lexicon - a catalog of words which get to transpire in a document. This may be, as an example, most of the words when you look at the

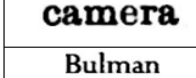
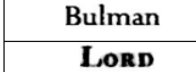
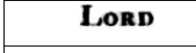
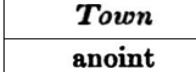
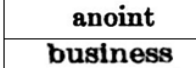
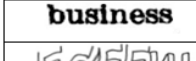
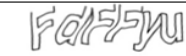
English speech, or a extra technical lexicon for a field that is specific. This method can be challenging in the event that document encompasses terms maybe not when you look at the lexicon, like proper nouns.
The production stream could be an ordinary text stream or file of functions, but extra urbane OCR arrangements can support the early design associated with page and create, as an example, an annotated PDF that includes both the first image of the page and a searchable representation this is certainly textual.
"Near-neighbor evaluation" makes usage of co-occurrence frequencies to correct errors, by noting that precise words are often identified collectively. For example, "Washington, D.C." is normally distant general public this is certainly extra English than "Washington DOC".Understanding of the syntax associated with the speech becoming scanned can additionally aid determine if a expressed word is probable is a verb or a noun, for example, permitting larger accuracy.

1) Using OCR Engines to Recover CAPTCHA

- CAPTCHAs tend to be projected to be facile for people to exceptionally resolve, but hard for computer systems going in automatically. Cheaters and spammers have gotten concerning CAPTCHAs by bypassing this system to a single more web site, whereas men and women go in this system to be entry to just a little function that is supplementary. An application in order to become admission to an (often pornographic) image as an example, the people consider they truly are resolving a mystery or typing.
- Outside undertakings such as BUSTING, AICAPTCHA and PWNTCHA have shown methodologies and aftermath indicating that countless regarding the plans are overpowered by computer systems alongside amid 88% and 100% reliability, using personality recognition this is certainly optical.
- The tate associated with the art that is fine solvers utilized a three duration way encompassing of preprocessing, segmentation and connection phases. Preceding examinations have instituted that arrangements joining segmentation that is rehearse contraption discovering considerably outperform off the ledge OCR arrangement at destroying captchas. The precision of circumstances associated with art work speech recognizer doesn't surpass 1%, whereas a rehearse classifier can go beyond 75% for example, eBay audio captcha. This three duration way works as follow: early, the solver preprocesses the captcha to really make it better to analyze, by way of example by removing colors or by requesting decrease that is sound. Upcoming, the solver endeavors to segment the captcha into chunks that encompass specifically one character, for example by utilizing a clustering algorithm from the picture. Eventually, a classifier, such as a prop vector contraption (SVM) or a neural web, is used to realize that personality is encompassed in almost every chunk that is solitary.

RESULTS AND ANALYSIS

Table.1 Result of various CAPTCHA's

CAPTCHA	Original Text	OCR	Errors	Error Rate
	Camera	camera	1	0.14285…
	Bulman	Bulman	0	0
	LORD	Lolm	3	0.75
	Thomas	Thomas	0	0
	Town	Town	0	0
	Anoint	Anoint	0	0
	business	Business	0	0
	FdFFYu	17e07FfiMfl	8	0.88888…
	Hfnhv	Hfllfr	4	0.8
	Pritio	pT\'{Q	6	0.85714..
	Person	Pfrson	2	0.33333..

Resultant Success Rate Success Rate $= \frac{\sum_{i=1}^{n} \text{Error Rate}}{n}$

The Resultant Success rate of the CAPTCHA Recognizer using Tesseract OCR Libraries for selected set of 10 CAPTCHAS is:

$\sum_{i=1}^{n}$ Error Rate = 0.37722

We Collected 12 CAPTCHAS and Success Rate for,

Success Rate= 0.37722/12

= 0.31435 * 100= 31.43%

CONCLUSION AND FUTURE SCOPE

CAPTCHAs can be used in endeavors to end automatic media from giving deeds that degrade the standard of capability of a given system. CAPTCHAs are furthermore utilized to minmise computerized postings to websites being assorted. CAPTCHAs have actually countless needs that are supplementary of good use protection. Its likely to improve the defense of an text that is continuing by systematically including noise and distortion, and arranging acts additional securely. These actions, though, should furthermore result in the functions harder for humans to comprehend, promising in a higher mistake rate. There clearly was a check to the sound and distortion that humans can tolerate in an endeavor of a text CAPTCHA. Usability is definitely an subject this is certainly essential arranging a CAPTCHA. By-design, Text CAPTCHAs are facile and simple to resolve by people. Their particular encounter that is inferior them attractive to locale operators who are distressed of each defense that may coil away possible visitors. Though, this high quality this is certainly alike made them facile to strike. The resolving CAPTCHAs using Open Basis OCRs, Displaying that CAPTCHAs susceptible to such assaults in this thesis, we've debates.

REFERENCES

[1] Matt. May, "Inaccessibility of CAPTCHA." Alternatives to Visual Turing Tests on the Web. I: W3C (red.), W3C Working Group Note, work in progress (2005).

[2] Jon Bentley and Colin Mallows. "CAPTCHA challenge strings: Problems and improvements." In Electronic Imaging 2006, pp. 60670H-60670H. International Society for Optics and Photonics, 2006.

[3] Mohammad Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza. "Persian/Arabic Baffletext CAPTCHA." J. UCS 12, no. 12 (2006): 1783-1796.

[4] Andy Schlaikjer, "A dual-use speech CAPTCHA: Aiding visually impaired web users while providing transcriptions of Audio Streams." LTI-CMU Technical Report (2007): 07-014.

[5] Jeremy Elson, John R. Douceur, Jon Howell, and Jared Saul. "Asirra: a CAPTCHA that exploits interest-aligned manual image categorization." In ACM Conference on Computer and Communications Security, pp. 366-374. 2007.

[6] Graig Sauer, Harry Hochheiser, Jinjuan Feng, and Jonathan Lazar. "Towards a universally usable CAPTCHA." In Proc. of the 4th Symp. On Usable Privacy and Security (SOUPS'08), Pittsburgh, PA, USA. 2008.

[7] Jeff Yan and Ahmad Salah El Ahmad. "Usability of CAPTCHAs or usability issues in CAPTCHA design." In Proceedings of the 4th symposium on Usable privacy and security, pp. 44-52. ACM, 2008.

[8] Leung, Chun-Ming. "Depress phishing by CAPTCHA with OTP." In Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on, pp. 187-192. IEEE, 2009.

[9] Bin B.Zhu, Jeff Yan, Qiujie Li, Chao Yang, Jia Liu, Ning Xu, Meng Yi, and Kaiwei Cai. "Attacks and design of image recognition CAPTCHAs."