A REVIEW ON CAPTCHA GENERATION AND EVALUATION TECHNIQUES

Mir Aman Sheheryar, Pradeep Kumar Mishra and Ashok Kumar Sahoo
Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, India
E-Mail: ashoksahoo2000@yahoo.com

ABSTRACT

Tremendous scope in the field of designing and cracking CAPTCHAs (an acronym and stands for “Completely Automated Public Turning Test to tell Computers and Humans Apart”) are in demand now-a-days. In the applicability part of designing and cracking, new gateways for computing research are obtained. Designing better CAPTCHA mean better security for systems in means of withstanding against odds and the breaking of current existing system refers to the advancement of artificial intelligence (AI) which is done by exploring the loopholes in system. CAPTCHA is basically used as a protection from malicious programs like Bots and evading deliberate attempts of accession by parties other than humans. For web security, we are using different type of CAPTCHA depending upon the parameters and approaches used for generation of particular primitive. In this paper, need, aspects like, design, strength, weakness and results obtained by various researchers in this field are explored. This will also help various researchers to carryout research in this direction.

Keywords: CAPTCHA, OCR, Bots, GUI.

INTRODUCTION

In many applications, specially, when interacting with automatic machines (or computers) it is mandatory that the interaction initiated from a human being or not. In order to do this, the term CAPTCHA has been introduced by John Langford, Nicholas J. Hooper and Luis Von Ahn [1] in the year 2000 at Carnegie Mellon University. The CAPTCHA has been invented to add the ability to protect information and actions from the malicious intents of the bots. Till date, a variety of schemes have been developed for drafting the CAPTCHA in secure and efficient way among which some grew old and some are achieving the aim. It involves implementation of Human Interactive Proof (HIP) which is a set of protocols used to determine the difference between computer programs and human users. These are put into place to prevent automated programs pretending to be as human users that involve in spamming, unauthorized malicious activities that include credit-card frauds, peeping into and illegal access to information that is meant to be available for valid users. The ability of a CAPTCHA lies in the fact that it should be understood and identified quickly by naive users (humans) and shall remain difficult to identify by a Bot, at the time when CAPTCHA test is performed. CAPTCHAs are a brilliant improvisation to implement Turing test. In turning test questions are asked to two users, one of which is human and other is a machine or computer. Both users pretend to be same (human) and similarly try to mislead the CAPTCHA system asking the test. On the basis of their response, CAPTCHA system has to decide among the two which one is legitimate (or human being) and which one is ambiguous other than human (or simply the computer). CAPTCHAs after evolution acquired different types based on the mechanism of building. Generally, it is a combined technique involving image processing and cryptography of simple structured elements that contains words and pictures. It consists of an image that is made by joining the letters (alphabets) and numbers at random or by following a particular sequence and keeping them in front or back of an unintelligible background in sequential approach and when these images are subjected through some distortion algorithm. The images get misrepresented that make optical character recognition (OCR) of the image very difficult to be obtained.

TYPES OF CAPTCHA

The appearance of CAPTCHA encounter a variety of changes since it was first created. The hierarchy of CAPTCHA is depicted in Figure-1 below. CAPTCHA comprises of various forms which add to its strength as the security primitive of bypassing the CAPTCHA is kept into consideration. It achieved in building new techniques over progress of time so as to make it much tuff to crack.

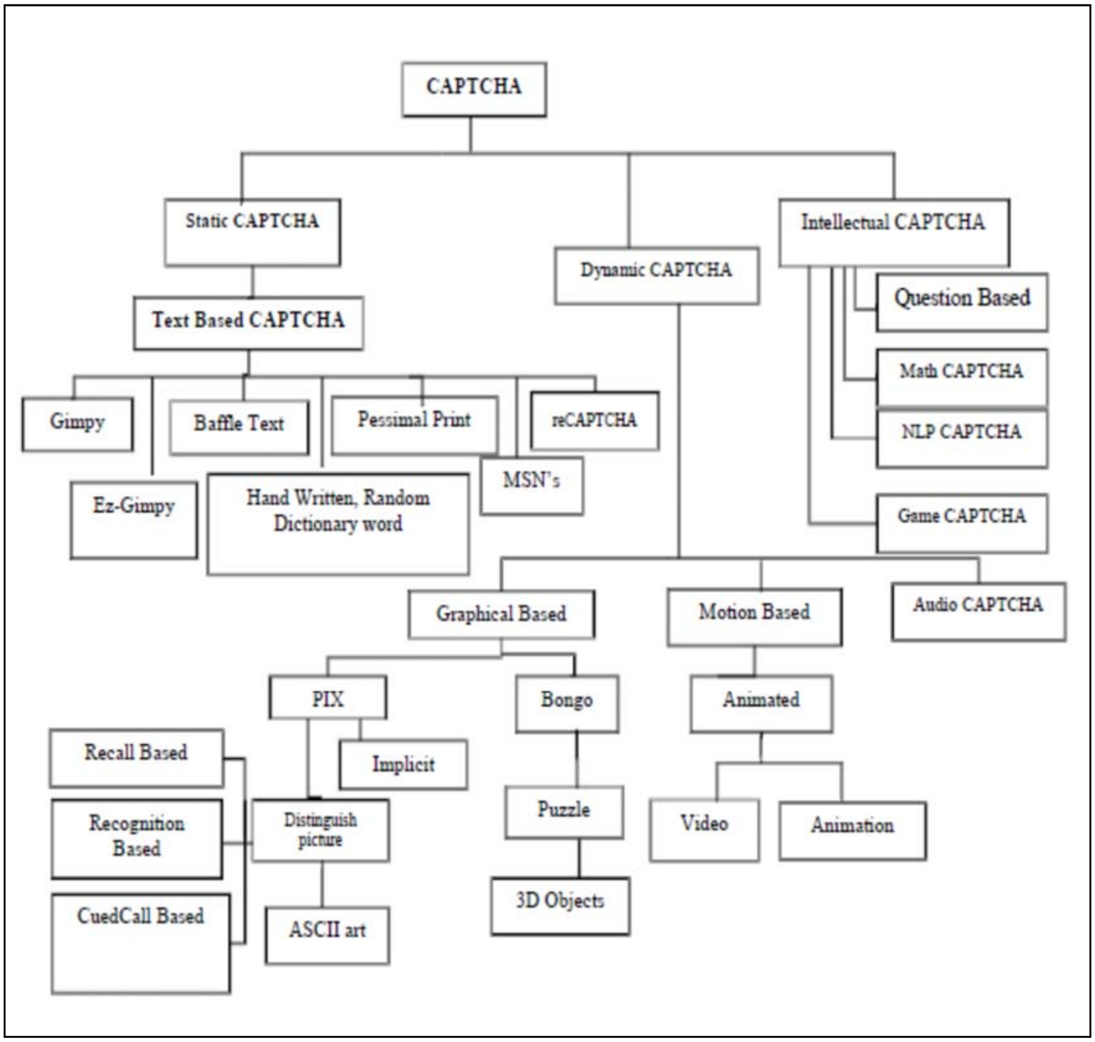


Figure-1. Hierarchy of CAPTCHA evolution.

From Figure-1, it is clear that the family of CAPTCHA system is branched among three principal systems. These principal systems are explained below. Static OCR based CAPTCHA systems are discussed in section III. Section IV carries the discussions on dynamic non OCR based CAPTCHA. In section V, features of intellectual CAPTCHA are discussed. In section VI, the application domains of CAPTCHA systems are described and finally the conclusion and future directions on research on CAPTCHA are discussed in section VII.

Static OCR based CAPTCHA systems

OCR based CAPTCHAs are primarily text based in which misrepresented image of characters are presented. The user required to identify and input the correct answer. The challenge here is stationary and hence OCR based CAPTCHAs comes under static category. The strength of static CAPTCHA relies on the misrepresentation applied to characters that include letters and numbers. For small handheld devices (such as palmtops, PDAs) the static CAPTCHA are hectic to answer. The OCR based implementation methods are presented below.

Text based CAPTCHA

CAPTCHA based on text form primary systems include gimpy, baffle text, hand written text, random word text, dictionary word text. These are based on the foundation of text in a manner they are written. Text based CAPTCHAs are easy to implement, involving users to enter the answers for the questions which only human users can solve in precise amount of time. The example questions include:

- What is the second last letter of ‘KINGKONG’?
- Which of Cat, Tiger and Snake is Pet?
- If Friday is two days after what is tomorrow?

The questions discussed above are easy to solve for humans and difficult for automated programs. With growing need for security text based CAPTCHA turned into transformed form that involves wavering the principal text. CAPTCHAs based on text are simple to lay down and implement. These CAPTCHA systems can be very effective, however requires a huge question bank. The characters represented are very small, resulting in identification problem for the user. In these CAPTCHA systems, identification can be achieved by OCR technique as described in [2, 4]. An example of text based CAPTCHA is shown in Figure-2 below.

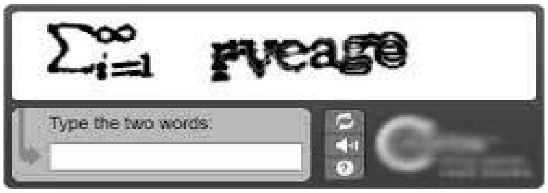


Figure-2. An example of text based CAPTCHA.

Gimpy

Gimpy is one of the greater dependable systems made for collaboration with yahoo to safeguard the chat room from Bots. The gimpy text is presented in distorted form so as to misguide the unauthorized users. The words are taken from dictionary over a certain number upon choosing. Gimpy presents the challenge in the form of overlapped text; making challenge quite confusing for Bots than actual users. In the gimpy system the users required to identify at least three words.

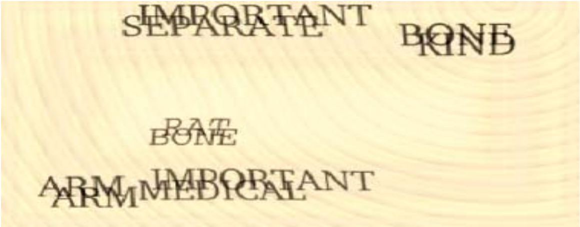


Figure-3. An example of Gimpy CAPTCHA.

Ez-Gimpy

This system is a simplified version of gimpy and is implemented by Yahoo in their sign up system. The single words are taken at random from dictionary and misrepresentation is employed so as to defeat the Bots. As the words are not imported from a dictionary hence dictionary attack is defendable. However, the CAPTCHA represented in Ez-Gimmpy broken by OCR's hence these are not good for implementation.

Figure-4. An example of Ez-Gimpy CAPTCHA.

Baffle text

This scheme uses non English pronounceable words and was developed by Henry Baird at University of California. In this technique the words generated are readable but does not specify any sense. Misrepresentation is added to characters so as to make it difficult for user and user is then asked to make the test. This technique eased out the drawbacks in gimpy based CAPTCHA which used dictionary words hence make it more difficult for Bots.

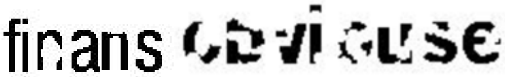


Figure-5. An example of Baffle text CAPTCHA.

Pessimal CAPTCHA

These CAPTCHA systems bears the test of presenting the text in poor form which involves decreasing the quality of text written, hence degrading the performance of OCR's [3]. The Pessimal CAPTCHA can still be cracked using Mori-Malik algorithms [3] and brute-force techniques.

Figure-6. An example of Pessimal CAPTCHA.

Hand written random dictionary word CAPTCHA:

Handwritten random dictionary word CAPTCHA was one of the solutions to web security. In [8] hand written CAPTCHA is employed to improvise the web security, the system is produced by making CAPTCHA test against the number of handwritten characters and numbers. These contents are picked at random dictionary words and numbers.These characters are further changed into image by Coloring by using appropriate randomness on server side over fixed scale.

Figure-7. An example of hand written, random, dictionary word CAPTCHA.

MSN's

It is basically the Microsoft passport CAPTCHA. It is the service provided under the zest of Microsoft

Network. This CAPTCHA system makes the use of eight characters from capital family of alphabets and numbers. The foreground Colour is kept blue and background Colour scheme is grey. Wrapping is used to misrepresenting the characters so as to make the shake effect. Thus it holds the property of being segmentation resistant.

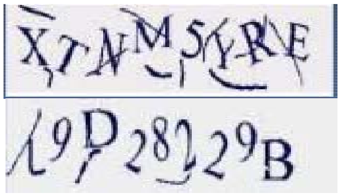
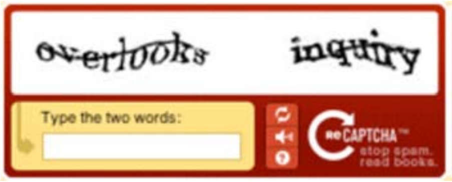


Figure-8. Examples of MSN's CAPTCHA.

reCAPTCHA

The reCAPTCHA is the other variant of CAPTCHA based on text. Without charge reCAPTCHA is availed for protection of any website against spams and Bots. In these, the danger is analysis engine and robust CAPTCHA are used to evade Bots for malicious activities on your site. Words used in reCAPTCHA for challenge are directly obtained from old books that are stored in digitized format. These words are further subjected to misrepresentation to strengthen its stand against the OCR's there by adding wrap [7]. The CAPTCHA is displayed by taken two misrepresented words from digitized format from old books.



overlooks inquiry

Type the two words:

Figure-9. An example of reCAPTCAHA.

Dynamic Non-OCR based CAPTCHA systems

Dynamic CAPTCHA also called as non-OCR based CAPTCHA mostly preferred to test the reflex efficiency of humans. It includes determining the audio and video sense. Dynamic CAPTCHA involve the text situated on the motion based approach. This category of CAPTCHA system include the graphical based, motion based and audio based CAPTCHA. The dynamic or non-OCR based implementation methods are investigated below in detail.

Graphical based CAPTCHA

These systems form one of the family branches in dynamic non-OCR based CAPTCHA that include image –based, PIX and Bongo CAPTCHA. In these systems, user is presented a test in image form and has to select in certain order as presented in GUI.

CAPTCHAs based on image

Image -based CAPTCHAs are challenging one; in this the user has to pass the tests. Here users have to guess similar images, that is, images bearing similarity as visual puzzles. In this CAPTCHA system, user is presented with an image and he/she ought to determine image given to him/her. The convenience of these CAPTCHA systems is that of arrangement recognition is hard AI problem and hence it is difficult to crack using conventional arrangement recognition technique. An example is shown in Figure-11 below.

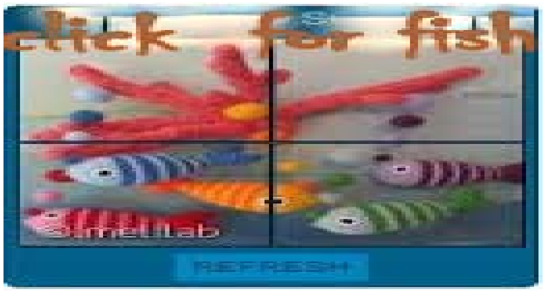


Figure-10. An example of image -based CAPTCHA.

Pix

It is one of the forms of graphical scheme**.** It is a schedule that makes the use of a database, which is of labelled image [15]. The images used in the pix are pictures of material objects like mare, desk, chair etc. The program is coded in a manner to pick a commodity in random, finds four images at random of that material from its database, misrepresent the chosen images at random, finally put the last made up image to the user for the test asking the question. Like "what are these pictures of"? An example is in Figure-11 below.

Figure-11. An example of Pix based CAPTCHA.

Implicit CAPTCHA

In these CAPTCHA systems, the user have to only make simple click [18]. In this test the picture of any object is shown as a test to the user. User have to click on certain element in displayed image like a picture of car is shown and the user is asked to click on the windshield of the car.

Distinguish pictures

Distinguish CAPTCHA system is an outcome of graphical based CAPTCHA. In this, the user need to determine answer for test asked on the basis of parameters like, recall, recognition and cued call. In recall based CAPTCHA, the user is asked to redraw last created design, which he created or chooses earlier during the registration stage. An example is shown in Figure-12 below.

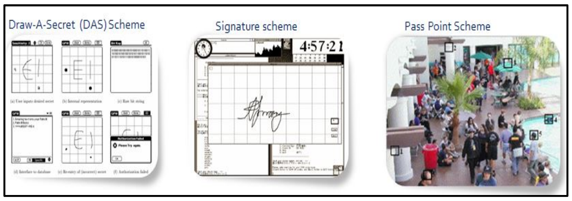


Figure-12. An example of recall based CAPTCHA.

Recognition based

In Recognition CAPTCHA, a set of images are shown to the user and the user has to undergo the authentication test by reorganizing and certifying the images that he chooses at the onset of registration time.Example is given in Figure-13 below:

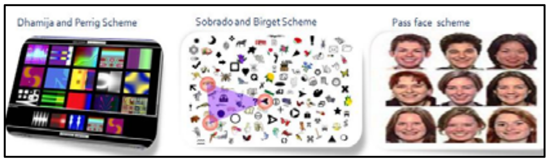


Figure-13. An example of recognition based CAPTCHA.

Cued call based

In cued call based system, the hint is given to user to remember his target. Thereby providing an extra cue that specifies the location bound in displayed image. Example of this type of CAPTCHA system is in Figure-14 below.

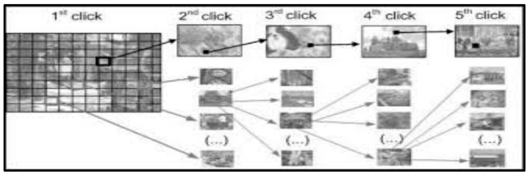
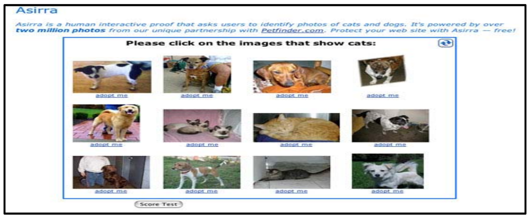


Figure-14. An example of cued call based CAPTCHA.

Asirra CAPTCHA

Asirra is an acronym that stands for “Animal Species Image Recognition for Restricting Access”. Asirra is a cat or dog labelling situation CAPTCHA design [19]. The classifiers which are efficient about 83 percent accurate, tell cats and dogs are apart that are used in *Asirra*. The reviewed versions of this system contains animal grid, animal zoo where user have to differentiate among species on click. Example is in Figure-15 below.



Asirra

Asirra is a human interactive proof that asks users to identify photos of cats and dogs. It's powered by over two million photos from our unique partnership with Petfinder.com. Protect your web site with Asirra — free!

Please click on the images that show cats:

Figure-15. An example of Asirra CAPTCHA.

ASCII Art

ASCII Art CAPTCHA system is another outcome of dynamic non-OCR based CAPTCHA used for validation. In this, a test to solve is displayed as image. The image is formed by character string using ASCII art as shown in Figure-16. The image formed in ASCII art is the combination of string with multiple lines that show the acceptance text with some misrepresentation and noise characters [17].

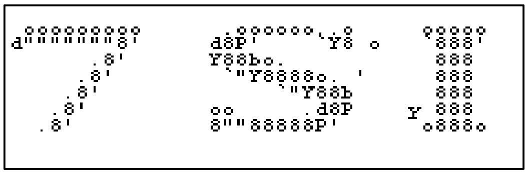


Figure-16. An example of ASCII Art CAPTCHA.

Bongo

Bongo is the second outcome of graphical CAPTCHA. Bongo [16] is a program in which users undergo through the task and are asked to solve a visual pattern recognition problem and user must certain the characteristics that differentiate the problem asked as a test. Bongo now-a-days also include presenting the jumbled puzzle and 3D objects. Example is shown in Figure-17 below.

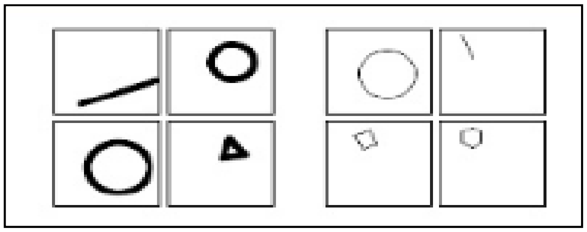


Figure-17. An example of Bongo CAPTCHA.

Puzzle based

For puzzle CAPTCHA systems, a picture is distributed into clumps depending upon the size of picture [2, 5]. For the test, the user is asked to combine these jumbled picture chunks so as to make the exact original picture. Example is shown in figure 18 below.

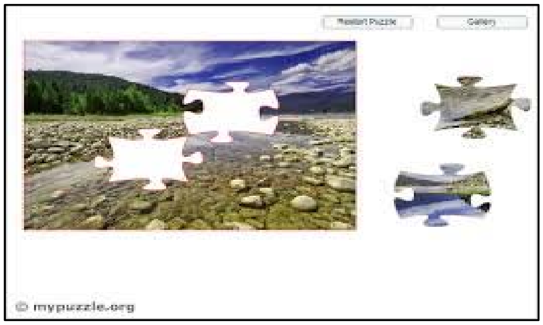


Figure-18. An example of puzzle based CAPTCHA.

3D Objects CAPTCHA

The 3D object CAPTCHA is presented in three quadrant dimensions and is good for humans and bad to machines [20, 21]. The Primary criterion is the human imagination. For a test, the user has to enter the correct sequence as asked like “the head of the walking man, the vase, the back of the chair.” An example is shown in Figure-19 below.

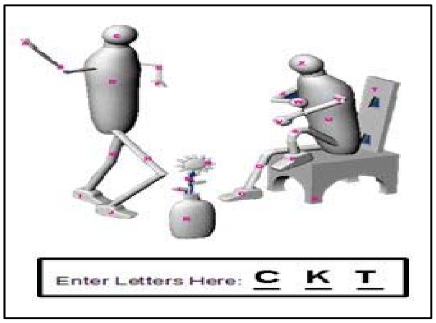


Figure-19. An example of 3D Objects CAPTCHA.

Motion based CAPTCHA

Motion based CAPTCHA involve animated CAPTCHA and video CAPTCHA which are discussed below within the scope of animation based CAPTCHA.

Animation based CAPTCHA

Animation based CAPTCHAs are that bears certain sequential motion. Further the CAPTCHA methodology combined with moving image frames in certain order form the video CAPTCHA. The video based CAPTCHA is displayed on demand to user verify the scene about. Thus CAPTCHAs are also classified on the basis on perimeter distortion whether characters, digits, or images which are discussed below.

Animated CAPTCHA

It forms one of the techniques used to employ CAPTCHA to withstand automated programs. Animated CAPTCHA present the CAPTCHA with motion containing either text or image that bears certain motions in sequenced manner. Thus CAPTHCAs is giving a challenge test to the users or humans to check his/her response. An example is shown in Figure-20 below.

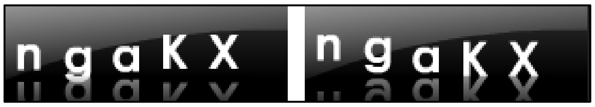
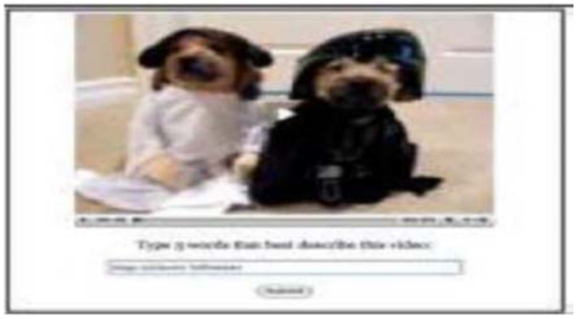


Figure-20. An example of animated CAPTCHA.

Video based CAPTCHA

Video based CAPTCHA system is something different then animation based CAPTCHA and is rarely employed. In video-based CAPTCHAs, video is described by word tags added to video. The tags added are three words (tags) and in order to pass the test the tag selected by user should necessary match the automatically produced tags. This system can be composed if any CAPTCHA system uses video as a medium to display test to user [2,6]. An example is shown in Figure-21 below.



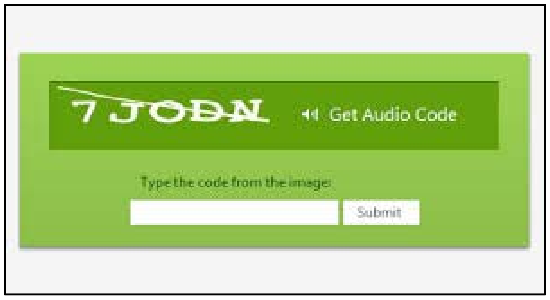
Type 3 words that best describe this video:

Figure-21. An example of video based CAPTCHA.

Audio based CAPTCHA

Over the last decade, audio CAPTCHA make its position in the CAPTCHA establishment and proved beneficial to visually impaired users.

Audio based CAPTCHA systems primarily depend on the sound. Audio CAPTCHAs were introduced and advanced for optically impaired users. This contains audio-clips which user can be downloaded. In audio CAPTCHA, firstly, the user listens to the spoken word and after that submits that spoken word [2]. The audio-based system is formulated on the distinction in the skill of listening among automated machines, humans in identifying announced language dialect. The sound clip is presented to the user and user is challenged as a test to fed exactly same words as sounded in the audio CAPTCHA clip [6]. An example is shown in Figure-22 below.



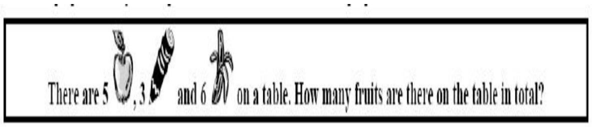
Type the code from the image:

Figure-22. An example of audio based CAPTCHA.

Intellectual CAPTCHA system

Question based CAPTCHA

In Question Based CAPTCHA system, a question is asked as a test as described in [11] to determine the ability of user. The test presented in question based CAPTCHA can only be answered by genuine user (say human). To eradicate the limitations, dynamic question based CAPTCHA systems are also proposed. An example is shown in Figure-23 below.

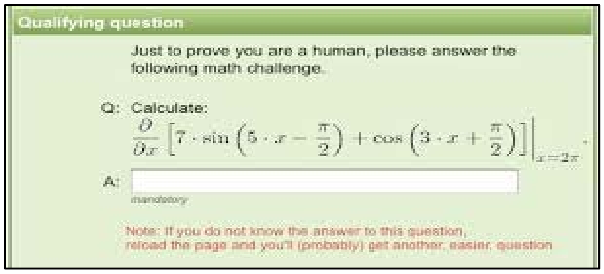


There are 5 , 3 and 6 on a table. How many fruits are there on the table in total?

Figure-23. An example of question based CAPTCHA.

Math CAPTCHA

Math CAPTCHA systems make the use of logical as well as reasoning based series of tasks assigned as CAPTCHA challenge to the users in order to prove the users are human. As proposed in [10], the mathematical CAPTCHA based on basic arithmetic operations (+, -, *). In this CAPTCHA challenge, a series of mathematical equations are put to user to solve. The hardness of these type of CAPTCHA system can be increased and decreased on numerous implementations. An example is shown in Figure-24 below.



Qualifying question

Just to prove you are a human, please answer the following math challenge.

Q: Calculate:

$$\frac{\partial}{\partial x}\left[7 \cdot \sin\left(5 \cdot x - \frac{\pi}{2}\right) + \cos\left(3 \cdot x + \frac{\pi}{2}\right)\right]\Big|_{x=2\pi}$$

A:

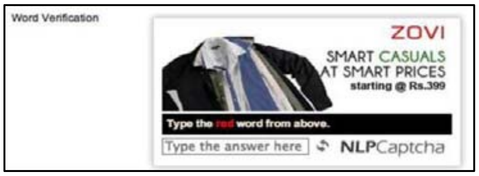
mandatory

Note: If you do not know the answer to this question, reload the page and you'll (probably) get another, easier, question

Figure-24. An example of Math CAPTCHA.

NLP CAPTCHA

Natural Language processing CAPTCHA relies on the human capacity of NLP. For this the readily available advertisement are taken into consideration for implementation. These advertisements are combined to form the CAPTCHA test as described in [12]. Thus by having NLP in place, users do not get lost in the clutter misrepresentation. An example is shown in figure 25 below.



Word Verification

ZOVI

SMART CASUALS AT SMART PRICES starting @ Rs.399

Type the red word from above.

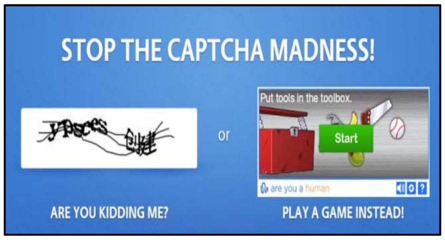
Type the answer here

NLPCaptcha

Figure-25. An example of NLP CAPTCHA.

Game CAPTCHA

For the replacement of annoying CAPTCHA, game CAPTCHA was proposed [13]. In game CAPTCHA, small game database is used to implement the test .The mini games are interacting with convenience difficulty [14]. Game CAPTCHA system is usually good for touch screen devices and mobile devices like smart phones. Flaw in this system is that it is inappropriate for desktop implementation. An example is shown in Figure-26 below.



STOP THE CAPTCHA MADNESS!

or

Put tools in the toolbox.

Start

are you a human

ARE YOU KIDDING ME?

PLAY A GAME INSTEAD!

Figure-26. An example of game CAPTCHA.

APPLICATION DOMAINS

Web form registrations

Internet sites which provide free registration to avail their services are vulnerable to bots as well. These bots may also be in automated script forms which can register millenary email accounts on the cyber space, thus consumes the adored capacity of web which leads to slow down of network nodes.

Likewise for online polling sites

User response is gathered in the form of questionnaires for polling sites. So as to assure that the response is made by human only before filling the response CAPTCHA system is used.

Avoiding web crawling

If site on cyber space doesn't want to get indexed by a search engine, CAPTCHA system can be employed to overcome this scenario.

In the field of E-Ticketing

For efficient prevention of dictionary attacks and E-mail spam CAPTCHA systems can be very useful. CAPTCHA moreover offers armour versus relay attacks, an increasing risk to get around through CAPTCHA defence mechanism. Thus the CAPTCHA provocations are delivered to human solvers, whose observations are fed back to the proposed application.

Counter comment spams in blogs

In order to overcome with the comment spam (example "get free credit card is here"), which are usually put into place to increase the traffic inflow to a sight by raising search engine rank, CAPTCHA systems can be useful.

Securing website enrolment

To hinder automatic website enrolments usually performed by Bots, one can rely on CAPTCHA systems. By placing CAPTCHA mechanism one can ensure that the website enrolment is surely done by humans, hence saving up lots of space over web.

RESTRAIN DOMAINS

There are various restrain domains while dealing with a CAPTCHA system. The designing of CAPTCHA determine that the CAPTCHA should be sound enough to address the accuracy, response time, recognized difficulty and comfort of using the scheme. On the ground of current investigation, different types of CAPTCHAs are available. The current available CAPTCHAs are mixed with certain limitations mentioned below:

1. Using session id of known CAPTCHA image, security system can be breached without using OCR symbols [23].
2. Machine learning techniques explored the vulnerability of CAPTCHA system (proposed in [23]).
3. Segmentation combined with involution neural networks to draft machine learning for character recognition [24, 28, 29].
4. Shared server based vulnerability in which the other virtual host may leave the site of CAPTCHA issuer exposed [23].
5. Retyping/re-entering CAPTCHA got difficult even for large users as the outcome of misrepresentation of characters in image.

Apart from the above limitations, we touted out the procedural approach that delimits the CAPTCHA which are as under in tabulated form:

A. Existing CAPTCHA model issues (strength and weakness).
B. Issues affecting the CAPTCHA design based on usability.

Table-1. Strength and weakness of CAPTCHA systems.

CAPTCHA Type	Strength	Weakness	Drawbacks
Text based	Distorted text image is presented for the test to user.	Involving more distortion /misrepresentation make it difficult for humans to read. Modern OCR's algorithms can achieve over 90% success of cracking.	In text images, user has some problem to identify the correct text or characters. Multiple fonts. Font size. Blurred Letters Wave Motion. It can be easily identified by OCR techniques.
Images based	Questions to be solved by users are presented in image form and hectic for OCR's to crack.	When in case of repeated response not user beneficial, problem for colour-blind people. Some achievements in this field need touch screens devices. Images can be reorganized differently for different times by same user also.	Some users face problem of image identification those have low vision or due to blurring of images.
Audio based	CAPTCHA is read aloud to user for retyping. The challenge like reCAPTCHA.	Extra features are required for listening. Still traced out by OCR's. Futile for users with hearing impairments and visual disorder.	It is available in English therefore end user must have a comprehensive English vocabulary. Character that have similar sound. Output hardware is required.
Video based	Video is displayed to user and the user has to answer depending upon the test asked. OCR's can't crack.	Require high bandwidth, concentration required to reorganize the event in video.	Due to large size of file, users face problem to download video and find correct CAPTCHA.
Puzzle based	Difficult for OCR's. Chunked image frames add security to test.	Ability to solve image required. Solving puzzle take time to arrange in exact order so as to make exact image that is presented in test.	The task is not easy for users because puzzle based CAPTCHA take more time to solve the puzzle and identify actual arrangement of puzzles.

Table-2. Implementational issues in designing CAPTCHA.

Category	Usability issues	
Misrepresentation	Misrepresentation mechanism and level. (how much distortion to apply)	
	Confusing characters. (Like 6/G, b/5, S/s, Z/z, ”nn” as m, ”vv” as w, ”cl” as d and so on).	
	Friendly to Alien? (Language barrier)	
Content	Character set. (with increase in size, large possibilities of random guessing are more)	
	String length (how much)	How long? (Fixed or not)
		Predictable or not?
	Random or dictionary word/string (Avoiding phonetic generation)	
	Obnoxious word. (Avoiding community based words like” chink, negro”)	
Presentation	Font type and size (visible to naked eye)	
	Use of Colour (Attention grabbing or camouflage or irritating)	
	Image Size. (how big or too small)	
	Integration with web pages. (Dynamic or static)	

SECURING CAPTCAHAs

After going through relevant literature the following points are figured out for the procedural ways for securing CAPTCHA against attacks.

a) CAPTCHA system is protected if it is overpriced for crackers involving human solvers [22, 23].

b) Protection is achieved to test the CAPTCHA against attacks.

Table below further summarizes attacks and counter measures towards attacks performed on text based CAPTCHA and image based which are widely used.

Table-3. Various attacks and countermeasures on CAPTCHA.

Attacks on text based CAPTCHA	Countermeasures
▪ Attack using real time human user Relay Attack. ▪ Attack using OCR + dictionary for sensing word CAPTCHA. ▪ Removing the level of background noise. ▪ Spaces filling inside characters which are hallow. ▪ Fixing broken lines so as to calculate space between the pixels.	▪ Adding more levels of communication between user and CAPTCHA. ▪ Increasing misrepresentation to letters like wrapping, scaling, rotating. ▪ Increasing the intensity of distortion.
Attacks on image based CAPTCHA	**Countermeasures**
▪ Indirect attack for obtaining the solution from client side in case of game based CAPTCHA. ▪ Exhaustion of database using human involvement. ▪ Hitting queries to leaked data base for ascertaining the solution. ▪ Attack using machine learning for object recognition. ▪ Random guessing. ▪ Pure relay attack.	▪ Employing encryption or code perplexity. ▪ Make the use of software database creators like web crawler. ▪ Processing the object to be displayed in advance before subjecting them to test. But this is inappropriate to match the original object and test objects. ▪ Inflate the lookup space in order to increase the solution cost of computation. ▪ Raising the possibility of correct answers. ▪ Pointing doubtful pattern moments and instigate observable features.

COMPARATIVE ANALYSIS

[Mauro Conti et al, 2015] proposed a CAPTCHA system and named it as CAPTCHA Star which is an image based CAPTCHA. In their proposed work, [25] the user has to determine the difference in the shape of objects produced as test. The work was focused on the usability of the proposed approach against automated attacks. The system was tested ad-hoc basis. The evaluation of the system is described in the Table-4 below.

Table-4. Performance of CAPTCHA star.

CAPTCHA Design	Indirect attack	Exhaustion of DB	Leak of DB	Pure relay attack	Stream relay attack	Machine Learning	Random Chance
Asirra	✓	✓	✓	✓	Low	Low	0.02%
Collage	✓	✓	✓	✓	Low	High	16.60%
Deep	✓	✓	✓	✓	Low	High	0.20%
Motion	✓	✓	✓	✓	Low	High	25.00%
Video	✓	✓	✓	✓	Low	High	0.30%
Noise	✓	✓	✓	✓	mid	Mid	~ 0.00%
Cursor	✓	✓	✓	✓	Low	Low	~ 0.00%
Jigsaw	✓	✓	✓	✓	Low	Mod	6.66%
PlayThru	×	×	×	×	High	High	~ 0.00%
CAPTCHaStar	✓	✓	✓	✓	High	High	0.09%

The approach described by the researchers compared the result against other existing system of attacks as indirect attack, exhaustion of database, leak of database and pure relay attack. In addition, for stream relay attack and machine learning based attacks are also taken into account. Further robustness employed by making it intractable for visually impaired users, increasing the drawing space which increased the usability of drawing system.

[Sanjib Kumar Saha *et al*, 2015] in their work compares different types of CAPTCHA modals which are as under [26].

Table-5. Comparison of different types of CAPTCHA as per their attributes.

Attributes	CAPTCHA Types				
	Text	Audio	Image	Video	Cognitive
Recognizable by optional character recognition (OCR)	Yes	Yes (when included with text CA PTCHA)	Nil	Nil	Nil
Uses distorted text	Yes	Nil	Sometimes	Nil	Nil
Uses audio	Nil	Yes	Nil	Sometimes	Nil
Difficult for the hearing-impaired	Nil	Yes	Nil	Yes (if audio is included)	Nil
Uses image or video	Nil	Nil	Yes	Yes	Nil
Difficult for color-blind people	Nil	Nil	Yes	Yes	Nil
Vulnerable to content-based image retrieval	Nil	Nil	Yes	Sometimes	Nil
Requires high bandwidth	Nil	Nil	Nil	Yes	Nil
Can be perceived differently by different people	Nil	Yes (because pronunciation can differ)	Yes (when abstract images are used)	Yes	Nil

[Michael A. Kouritzin *et al*, 2013] proposed KNW-CAPTCHA in two variants hard and easy and gave the performance result after evaluation of both variants it was achieved that KNW-CAPTCHA-H [27] is good enough against attacks the results obtained are as under in tabulated form.

Table-6. Performance of KNW-CAPTCAH–H.

	NG	nT	95% confidence Interval	Time to solve
KNW-CAPTCHA	800	300	0.960±0.022	6.41s
AMT	800	3319	0.910±0.010	4.98s
Tesseract	800	300	0.000±0.000	N/A
ABBYY	800	300	0.000±0.000	N/A

Therefore, from the above results one can further harden the CAPTCHA if subjected to modification in recognition mechanism before putting the system to test, which shall result in increasing the time to decode of system. Also one can induce noise with some random pattern and for every new CAPTCHA generation it will be presented with different noise levels with varying techniques keeping confidence interval high.

CONCLUSIONS

CAPTCHA has grown into the authoritative for protection measures on the Cyber Space. In order to thwart "automated scripts", accesses against malicious networked services. Evaluation and exploration of CAPTCHA schemes were included for all along the last eight years.

Investigation on various types of CAPTCHA, the mechanism involved for implementation are described in this paper. In order to analyse stability and shortcomings of CAPTCHA schemes, those have evolved over the decade. It is ascertained that plenty of research exploration is brought to pass for CAPTCHA schemes for the capitalization. With the advent approach in the sphere of AI more CAPTCHA schemes will break in future. It is expected that this exploration will help through to get pacified idea of new flanged CAPTCHA in sphere of "web security and AI".

FUTURE WORK

Researchers will keep exploring the field of CAPTCHA based of pros and cons which will definitely open new gateways for providing security against automated scripts. Also in future, enhancement of the recognition procedure which will lead to increase the decode time for existing system there by enhancing the abilities of security by suggesting the new measures to make the field of CAPTCHA stiff to inappropriate access will be explored.

REFERENCES

[1] Ahn L. von, M. Blum and J. Langford. 2004. Telling Humans and Computer Apart Automatically. Communications of the ACM. 47(2): 57-60.

[2] Saini B. S. and Anju Bala. 2013. A Review of Bot Protection using CAPTCHA for Web Security. IOSR Journal of Computer Engineering. 8(6): 36-42.

[3] Baird Henry S., Allison L. Coates and Richard J. Fateman. 2003.Pessimal Print: A Reverse Turing Test. International Journal on Document Analysis and Recognition.5(2-3): 158-163.

[4] H. Chen-Chiung and Zong-Yu Wu. 2013. Anti-SIFT images based CAPTCHA Using Versatile Characters. International Conference on Information Science and Applications. pp. 1-4.

[5] G., Rich, Maryam Kamvar and Shumeet Baluja. 2009. What's up CAPTCHA?: A CAPTCHA Based on Image Orientation.ACM - 18th International Conference on World Wide Web. pp. 841-85.

[6] Zhang W. 2010. Zhang's CAPTCHA Architecture Based on Intelligent Interaction via RIA.2nd IEEE International Conference on Computer Engineering and Technology (ICCET). 6: 6-57.

[7] Von. Ahn L. 2009. Human Computation (reCAPTCHA). 46thACM/ IEE Design Automation Conference. pp. 418-419.

[8] R., Mukta and Nipur Singh. 2012. Random Handwritten CAPTCHA: Web Security with a Difference. International Journal of Information Technology and Computer Science (IJITCS). 4(9): 53.

[9] Monica Chew and Henry S. Baird. 2003.BaffeText: A Human Interactive Proof. The SPIE/IS&T Document Recognition and Retrieval Conference, Santa Clara.

[10] Hernandez-Castro, Carlos Javier and Arturo Ribagorda. 2010. Pitfalls in CAPTCHA Design and Implementation: The Math CAPTCHA, A Case Study. Computers and Security.29(1): 141-157.

[11] Shirali-Shahreza M. and S. Shirali-Shahreza. 2007. Question-Based CAPTCHA. IEEE International Conference on Computational Intelligence and Multimedia Applications. 4: 54-58.

[12] http://nlpcaptcha.in/ (Accessed on 02 December 2015).

[13] http:// http://areyouahuman.com/research (Accessed on 02 December 2015).

[14] http//venturebeat.com/2012/05/21/are-you-a-human-replaces-annoying-captchas-with games/captcha/ (Accessed on 03 December 2015).

[15] http://www.captcha.net/captchas/pix (Accessed on 10 December 2015).

[16] http://www.captcha.net/captchas/bongo (Accessed on 10 December 2015).

[17] http://link.springer.com/chapter/10.1007/978-1-4302-1579-0_13#page-1 (Accessed on 15 December 2015).

[18] Baird, Henry S. and Jon L. Bentley. 2005. Implicit CAPTCHAs. Conference on Electronic Imaging, International Society for Optics and Photonics. pp. 191-196.

[19] Elson J., John R. Douceur, Jon Howell and Jared Saul. 2007.Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization.ACM Conference on Computer and Communications Security. pp. 366-374.

[20] Krishnashanthi A. and K. Kuppusamy. 2014. New CAPTCHA Algorithm based on 3Dimensional. International Journal of Image Processing and Data Visualization. 1(1): 1-8.

[21] http://3dcaptcha.net (Accessed on 23 December 2015).

[22] M. Chew and J. D. Tygar. 2004. Image Recognition CAPTCHAs. The 7th International Information Security Conference, Springer.

[23] Chellapilla, K., Kevin Larson, Patrice Y. Simard and Mary Czerwinski. 2005. Building Segmentation Based Human-Friendly Human Interaction Proofs (HIPs). Conference on Human Interactive Proofs, pp. 1-26, Springer Berlin Heidelberg.

[24] Sauer Graig, Jonathan Holman, Jonathan Lazar, Harry Hochheiser and Jinjuan Feng. 2010. Accessible Privacy and Security: A Universally Usable Human-Interaction Proof Tool. Universal Access in the Information Society. 9(3): 239-248.

[25] Mauro Conti, Claudio Guarisco and Riccardo. 2015.CAPTCHaStar! A Novel CAPTCHA Based on Interactive Shape Discovery. Spolaor University of Padua, Italy, arXiv:1503.00561v1, [cs.HC].

[26] Saha, Sanjib Kumar, Abhijit Kumar Nag and Dipankar Dasgupta. 2015. Human-Cognition-Based CAPTCHAs. IT Professional.17(5): 42-48.

[27] Kouritzin, Michael A., Fraser Newton and Biao Wu. 2013. On Random Field Completely Automated Public Turing Test to Tell Computers and Humans Apart Generation. IEEE Transactions on Image Processing.22(4): 1656-1666.

[28] Sahoo, A. K. and K. K. Ravulakollu. 2014. Indian Sign Language Recognition Using Skin Color Detection. International Journal of Applied Engineering Research. 9(20): 7347-7360.

[29] Sahoo, A. K. and K. K. Ravulakollu. Vision Based Indian Sign Language Character Recognition. Journal of Theoretical and Applied Information Technology. 67(3): 770-780.