Secure CAPTCHA Generation

Submitted By

Kajol Patel

15MCEI21

DEPARTMENT OF COMPUTER ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2017

Secure CAPTCHA Generation

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering
(Information and Network Security)

Submitted By

Kajol Patel

(15MCEI21)

Guided By

Dr. Ankit Thakkar

तमसो मा ज्योतिर्गमय

NIRMA
UNIVERSITY

INSTITUTE OF TECHNOLOGY

NAAC ACCREDITED ‘A’ GRADE

COMPUTER ENGINEERING DEPARTMENT
INSTITUTE OF TECHNOLOGY
NIRMA UNIVERSITY
AHMEDABAD-382481

May 2017

Certificate

This is to certify that the major project entitled "**Secure CAPTCHA Generation**" submitted by **Kajol Patel (Roll No: 15MCEI21)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering (Information and Network Security) of Nirma University, Ahmedabad, is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-II, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Dr. Ankit Thakkar
Guide & Associate Professor,
Information Technology Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sharada Valiveti
Associate Professor,
Coordinator M.Tech CSE(INS)
Institute of Technology,
Nirma University, Ahmedabad

Dr. Sanjay Garg
Professor and Head,
Computer Engineering Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Alka Mahajan
Director,
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Kajol Patel**, Roll. No. **15MCEI21**, give undertaking that the Major Project entitled "**Secure CAPTCHA Generation**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science and Engineering (Information and Network Security)** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student
Date:
Place:

Endorsed by
Dr. Ankit Thakkar
(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Dr. Ankit Thakkar**, Associate Professor, Information Technology Department, Institute of Technology, Nirma University, Ahmedabad for his valuable guidance and continual encouragement throughout this work. The appreciation and continual support he has imparted has been a great motivation to me in reaching a higher goal. His guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

I deeply appreciate the invaluable support and concern of **Dr. Sharada Valiveti**, Coordinator M.Tech INS, Computer Engineering Department, Institute of Technology, Nirma University.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr. Alka Mahajan**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation she has extended throughout the course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department and Information Technology Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

The completion of this project would not have been possible without the prayers of my parents and family. To my friends, who were the source of constant motivation and upliftment, thank you for listening, offering advice and supporting me always.

- Kajol Patel
15MCEI21

Publication related to Research

International Conference Publication

- Kajol Patel and Ankit Thakkar, “A simple and efficient text-based CAPTCHA verification scheme using virtual keyboard”, International Conference on Information and Communication Technology for Intelligent Systems (ICTIS 2017), presented in March 2017 and yet to be published.

Abstract

Digital media becomes an effective way of communication which is available round the clock to everyone including humans and machines. This put the requirement for machines to differentiate between human and machine as far as access of the website or its relevant services is concerned. CAPTCHA (*Completely Automated Public Turing test to tell Computer and Human Apart*) is a test that helps machines (or programs) to differentiate between human and machine. CAPTCHA should be easy for users to solve and difficult for bots to attack. A simple and efficient text-based CAPTCHA verification scheme is proposed which is easy for human and hard for bots. The proposed work uses virtual keyboard, eliminates input-box, and does verification on the basis of the positions of the characters. The work is extended by using handwritten characters in the virtual keyboard and randomizing the positions of the CAPTCHA and keyboard. Response time analysis of both types of virtual keyboards and machine has been performed and results are discussed.

Abbreviations

AI	Artificial Intelligence
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans Apart
CaRP	CAPTCHA as Graphical Passwords
CBIR	Content Based Image Retrieval
CNN	Convolution Neural Network
CV	Computer Vision
HIP	Human Interaction Proof
IMAGINATION	IMAge Generation for INternet AuthenticaTION
KLM	Keystroke Level Model
RIS	Reverse Image Search
SEMAGE	SEmantically MAtching imaGEs
OCR	Optical Character Recognition

Contents

List of Tables

List of Figures

Chapter 1

Introduction

CAPTCHA is used in websites to prevent automated interactions by bots. For example, Gmail improves its service by blocking access to automated spammers, eBay blocks automated programs that flood the websites, and Facebook protects its site by limiting the creation of fraudulent profiles [1]. In November 1999, slashdot.com released a poll for voting to select the best college of CS in the US. In this poll, automated programs were created by students of the Carnegie Mellon University and the MIT that repeatedly voted for their colleges. This incident put the requirement of using CAPTCHA for online polls to ensure that only humans are allowed to participate in polls [2]. CAPTCHA are used in many web applications (or web services) like search engines, password systems, online polls, account registrations, prevention of spam, blogs, messaging and phishing attack detection etc. [3].

CAPTCHA can be broadly classified as text-based, image-based, audio-based and video-based CAPTCHA. This research focuses on text-based CAPTCHA only. Text-based CAPTCHA uses distorted characters forming a string or word which user has to recognize and pass the test. In image based, images are presented to user and he/she has to identify the object in image. Audio CAPTCHA uses audio clips which contains spoken words which user have to listen and recognize correctly to pass the test. Sound can be spoken words or may be related to images [4]. Text-based CAPTCHAs are widely used as it is simple and user-friendly. Few examples of text-based CAPTCHA are Gimpy, EZ-Gimpy, MSN-CAPTCHA, and Baffle-Text etc. In Gimpy CAPTCHA, ten random words are selected from a dictionary and displayed to the user. These words are displayed to the user using distorted images. Noise can be added to the images so that it would be difficult for a machine to identify the CAPTCHA. To access web service, the user must correctly enter the characters of the given images. In EZ-Gimpy CAPTCHA, only one word is selected from a dictionary and displayed to the user after applying misshape/distortion.

The idea is to launch a Artificial Intelligence problem which is difficult so that mainly two purpose can be served that is either bots and legal users are differentiated or it helps in advancing AI. Natural language processing, character recognition, speech recognition are different tough AI problems that have been used as the basis for CAPTCHAs [5]. CAPTCHA is a security measure that presents to the user the challenges that are difficult for machine to recognize but easy for human. The basic working flow of CAPTCHA is shown in Fig 1.1. First the random string i.e. a is generated using random function. Image is then generated including the string such that the humans can easily recognize but machines cannot. The image is then embedded in webpage and posted to the client. User identifies the string in the image i.e. b. The results are compared to previous values and if they are same then the user is legitimate otherwise is considered illegal and not allowed to enter the website or webpage [6].

1.1 Applications of CAPTCHA

As the web applications and its complexity increases security issues also increased. Legal liability and credibility of the organisation are harmed due to consequences of a security threats which can also decrease the trust of the users. Mostly the malicious software agents automates the misuse of web resources which degrades the quality of service for genuine user [7]. So, it is important for service provider to prevent such threats and differentiate humans from bots. Because of this reasons CAPTCHA is widely used by many web sites. CAPTCHA is type of challenge-response test designed to deal with such issues and threats. CAPTCHAs are used for many applications like [8]-

- Online polls- An automated program was developed that increases the vote for thousand of times. CAPTCHA is used in submission process of votes where it prevents bots from participating in polls. So, online polling must be protected using CAPTCHA.

- Preventing Comment Spam in Blogs- For raising ranks of webpages programs are developed that post unnecessary comments on the blogs or message boards. To

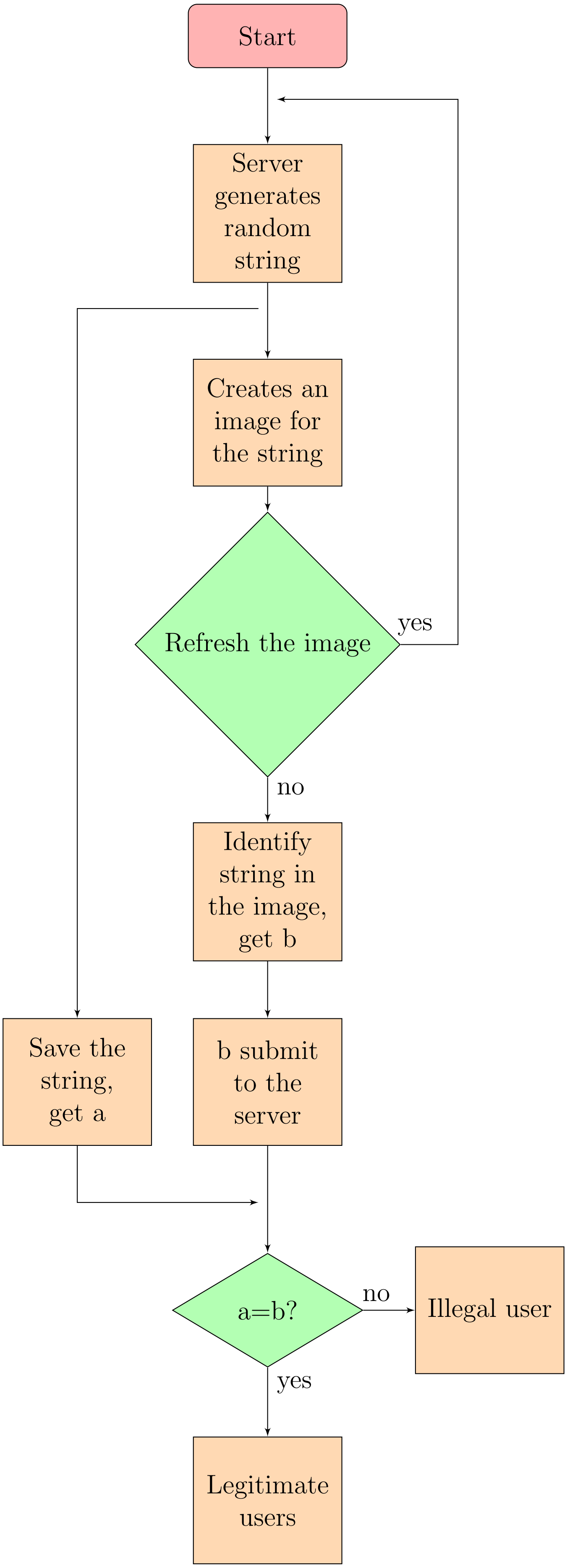


Figure 1.1: Basic working flow of CAPTCHA[6]

prevent those comment spams CAPTCHA can be used so that human can only post the comments and also user will not need to sign up before posting comment.

- Preventing Dictionary Attacks- In password systems, computer can try all possible combinations from dictionary till it reach to the correct one. CAPTCHA prevents the system from this attempts by requiring a user to solve CAPTCHA after a certain no of unsuccessful logins.

- Protecting Email Addresses From Scrapers- CAPTCHA prevents email addresses to be retrieved by scrapers while crawling through web. It hides the email address until the user enters the correct CAPTCHA.

- Protecting Registration of Websites- Email service providers like Gmail, Yahoo and MSN uses CAPTCHA to prevent spammers (or automated bots) from creating thousands of accounts.

- Search Engine Bots- CAPTCHAs are used to protect web pages by not allowing bots to enter the websites because to prevent web pages to be known to others easily, it is necessary to keep them unindexed. CAPTCHAs are used by administrators to keep Web spiders from indexing sites for search engines like Google. Since the site contains personal or private information that should not be searchable, administrators don't want to allow Web spiders to their site and they simply don't want the extra system load caused by all the spiders running across the Internet [9].

- CAPTCHA are also used as graphical passwords. A new security primitive based on hard AI problems was introduced in [10], known as CaRP (*CAPTCHA as Graphical Passwords*). It is click-based method where to derive a password a sequence of clicks on an image is used. For every attempt of login, a new CaRP image is generated and images used in CaRP are CAPTCHA challenges. A number of security problems are addressed by CaRP such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks[10].

Some systems use CAPTCHAs in place of a user account and password for pseudopublic files such as research papers and shareware programs. This prevents people from downloading and archiving an entire Web site or ftp server. Google used reCAPTCHA which was not only used for anti-bot and anti-spam mechanism but was also used for digitizing books. Luis designed reCAPTCHA mechanism in a way so that it delivers words that remained unrecognized by Optical Character Recognition (OCR) while digitizing a book or other text to the user as CAPTCHA.

In [11], a study is done on understanding the CAPTCHA with economic context where they have focused on business of solving CAPTCHAs. They showed that CAPTCHA must be viewed from an economic perspective as seen by a robust and mature CAPTCHA solving industry that bypasses the underlying technological issue completely. Today, large no of providers buy and sell CAPTCHA solving services in bulk.

Most of the text-CAPTCHAs are cracked by OCR attacks and to prevent from OCR-attacks, CAPTCHA can be made more complex with noise and distortion that affects the usability of users. Simplicity makes text-based CAPTCHA as preferred choice of implementation, at the same time there is a need to protect the CAPTCHAs from boats. Hence, a new method for CAPTCHA verification that makes easy for users to read and input the characters of the CAPTCHA, and at the same time, it makes difficult for bots to input the CAPTCHA characters is proposed. This approach uses a virtual keyboard to take input from the user, eliminate the use of input box and compares the CAPTCHA character based on the position of the characters instead of contents of the CAPTCHA.

Chapter 2

Literature Survey

Various CAPTCHA techniques have been designed to provide secure authentication for online applications. The different hard artificial intelligence problems like speech recognition, character recognition, natural language understanding and processing, etc. have been used as the basis for CAPTCHAs. Basic four different categories of CAPTCHA: text-based, image-based, audio-based and video-based are discussed in following subsections.

2.1 Text-based CAPTCHA

CAPTCHAs based on text are very simple and effective. In 1997, an AltaVista team began to work on a system to prevent Internet bots to attack the search engine by adding the active URL's to the AltaVista search engine platform. They developed the algorithm that creates the printed image that was generated randomly [12]. In 2000, Yahoo's famous Messenger chat service was hit by bots which directed publicizing links toward irritating human clients of chat rooms. Yahoo, alongside Carnegie Mellon University, built up a CAPTCHA called EZ-GIMPY, which randomly pick a lexicon word and distort it with a wide assortment of picture impediments. User have to recognize the word and if user is able to input it correctly, he/she passes test. [2].

The text-CAPTCHA can be any arithmetic operations like - "What is nine plus one (9+1=?)" or can be any text within the image. Text-based CAPTCHA can be Gimpy, Ez-Gimpy, MSN-CAPTCHA and Baffle-Text. Example of text based CAPTCHA is shown in Fig 2.1. In Gimpy based, 10 random words are selected from dictionary and are displayed to the user. These words are displayed in an image and are distorted. Noise is added in an image so that machine fails to identify. To access the web service user must enter the words from the given image. In Ez-Gimpy based, unlike Gimpy, only one word is selected from dictionary to be displayed and misshape/distortion is applied. This method was already broken by OCR. In MSN-based, fixed length of 8 uppercase characters and digits were used. Distortion in image was produced using warping. MSN CAPTCHA was broken by yan [13]. In Baffle-text dictionary words are not used, instead pronounceable text is created and user has to identify that text in order to access service [14].

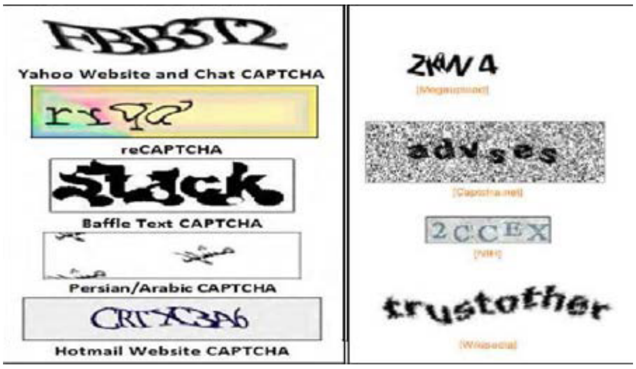


Figure 2.1: Examples of Text-based CAPTCHA[5]

Early text CAPTCHAs were broken by computer vision algorithms. Shape context matching method was used that can identify the word in an image of EZ-Gimpy and Gimpy CAPTCHA and were cracked by object recognition algorithms with 92% and 33% success [15]. Distortion techniques were developed which helped to crack EZ-Gimpy CAPTCHA and 4-letter Gimpy-r with success rate of 99% and 78% [16]. Many machine learning attacks are performed using neural network which can easily recognize the characters in CAPTCHA. It is suggested that CAPTCHA should be designed in such a way that segmentation is difficult [17]. Methodology of improved text-CAPTCHA is presented in [18] which is more secured and robust which includes combination of mathematical equation and alphanumeric word. Results of this CAPTCHA was compared with other styles of CAPTCHA namely Gimpy, EZ-gimpy, Megaupload, Securimage and Cryptography.

In [19], a CAPTCHA named Clickspell based on both text-based and image-based CAPTCHAs was proposed. In this CAPTCHA, user has to click on characters order by order displayed in CAPTCHA image. Characters are of randomly choosen word from the dictionary. Also the meaning of the word is shown above the image.

Narges Roshanbin and James Miller in [20] proposed CAPTCHA named ADAMAS which was based on Unicode as input and homo-glyphs in virtual keyboard. It uses Unicode characters which are visually similar so that detection of characters is difficult. It uses different randomization techniques to decrease formations of pattern. To prevent segmentation attacks, it uses colors for characters and their background in proportionate amount. ADAMAS consists of a test and keyboard. User have to find correct match for each Unicode character of test area in keyboard.

In [21], a 3D CAPTCHA is proposed where characters or numbers that are selected randomly are shown on cube faces to the users. Users have to identify the letters and type each character into the input boxes. A rotator is provided to rotate the cube. The disadvantage of this CAPTCHA is that it consumes more time to solve the CAPTCHA. KLM (*Keystroke Level Model*) is used to estimate the execution time of the task. A 3D drag-n-drop CAPTCHA was proposed in [22] where 3D characters embedded in the image are displayed to the user. As the character appears in the image user have to drag-n-drop the characters into the respective blank blocks. Summary of different kinds of text-CAPTCHAs are given in Table 2.1.

Table 2.1: Summary of Text-CAPTCHAs

Author	**Title**	**Year**	**Methodology**	**Advantages**	**Disadvantages**
[23]	CAPTCHA	1997	Randomly generated an image of printed text	Prevented the Internet bots to attack the search engine from adding the active URL's to the AltaVista search engine platform.	OCR-attacks
Simard et al.[24]	Using Character Recognition and Segmentation to Tell Computers from Humans	2003	User must type the correct ASCII distorted string provided	String of random distorted characters were used to make difficult for computers to recognize	Low cost Segmentation attack was done successfully to break Microsoft CAPTCHA

Continued on next page

Continued from previous page

Author	**Title**	**Year**	**Methodology**	**Advantages**	**Disadvantages**
Ince et al.[21]	Execution time prediction for 3d interactive CAPTCHA by keystroke level model	2009	3D text-CAPTCHA where characters or numbers that are selected randomly are shown on cube faces to the users. Users have to identify the letters and type each character into the input boxes	Robust against OCR attacks as it uses drag-n-drop property and characters are displayed on cube faces	Time-consuming because of cube rotator
Chaudhari et al.[22]	3D drag-n-drop CAPTCHA enhanced security through CAPTCHA	2011	3D characters embedded in the image are displayed to the user. As the character appears in the image user have to drag-n-drop the characters into the respective blank blocks.	Resistance to pre-processing and segmentation	It takes more time
Hwang, Kuo-Feng and Huang et al.[19]	A spelling based capt -cha system by using click	2012	Clickspell is both text and image-based CAPTCHA where user is asked to spell a random word by clicking distorted letters	Provides the dictionary function for users to learn the definition(s) of the spelling words	Time-consuming
Roshanbin et al.[20]	ADAMAS: Interweaving unicode and color to enhance CAPTCHA security	2016	ADAMAS consists of a test and keyboard. User have to search correct match for each Unicode character of test area in keyboard	Resistance to pre-processing, recognition and segmentation attacks	It is quite complex
Misako Goto et al.[25]	Text-Based CAPTCHA Using Phonemic Restoration Effect and Similar Sounds	2014	Based on phonemic restoration and recognition of similar sounds abilities of human	Usable and hard to be broken by computers	Some similar words are not recognized correctly like “fear” instead of “fair”

2.2 Image-based CAPTCHA

In CAPTCHA based on images user have to guess the images that have some similar properties or have to identify the object in the image. The main advantage of this CAPTCHA is that pattern recognition is hard AI problem [26]. Hence, pattern recognition technique is difficult to apply. There are many different kind of image CAPTCHA based on various patterns or different concepts that humans can recognize. Some Image-CAPTCHA are based on click based systems where users don't need to type. Example of image-CAPTCHA is shown in Fig 2.2 where the user is asked to click the flower from the set of the images. If user clicks the correct image then he/she passes the test successfully.

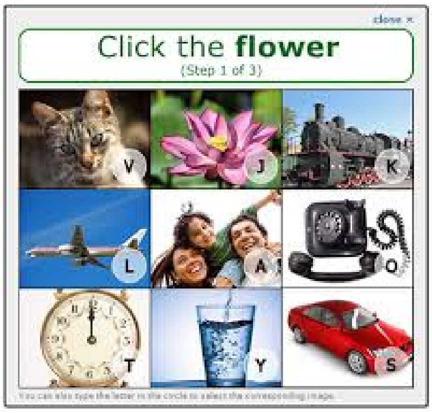

close ×
Click the flower
(Step 1 of 3)
V
J
K
L
A
O
T
Y
S
You can also type the letter in the circle to select the corresponding image.

Figure 2.2: Example of Image-based CAPTCHA[13]

Bongo and Pix CAPTCHA are some of the image-CAPTCHA. In Bongo, user is displayed with two series of blocks, the left and the right. The blocks in the left series differ from those in the right, and the user have to find the characteristic that sets them apart. In Pix, user is presented with six images of particular object and user have to identify what are those images of. Images can also be distorted to make it difficult or complex. One form of image CAPTCHA is face detection based CAPTCHA where user have to recognize faces like FaceDCAPTCHA, Avtar CAPTCHA, etc. Different kinds of image-based CAPTCHA are discussed below.

Ritendra Datta, Jia Li, and James Z. Wang in [27] put forward the image-CAPTCHA named IMAGINATION (*IMAge Generation for INternet AuthenticaTION*) for producing image CAPTCHAs that are user friendly and also robust against attacks because of distorting images. This system used pseudo randomness. It was based on geometric patterns where user have to mark center of image and proper category should be selected based on list.

Shirali-Shahreja, M.H. and Shirali-Shahreja:proposed Multilingual CAPTCHAs in 2007. In this method some images are shown and user has to choose the image of certain object. All the messages are shown in native language which is easy for user. User does not need to be familiar with English language [28].

In October 2007, Microsoft Research team proposed image-based authentication system known as Asirra [29] that depends on large database of images of pets from different animal shelters. The user must select all images describing either dogs or cats from a set of 12 random images of both categories. But this approach can lose security if database is compromised.

In [30] Rich Gossweiler, Maryam Kamvar and Shumeet Baluja presented a CAPTCHA based on image's orientation which is not language dependent. In this CAPTCHA randomly rotated images are provided and user has to adjust them in upright orientation. This method is easy for humans. The major advantage of this CAPTCHA is that it does not need the prior knowledge of labels.

Bin B. Zhu and his team designed an image recognition CAPTCHA named Cortcha (*Context-based Object Recognition to Tell Computers and Humans Apart*) where set of objects and an image is provided to the user and he/she has to identify an object that is detached from the image and have to place it back to its original position in the image [31]. They also presented attacks against image-CAPTCHA and guidelines for designing robust image recognition CAPTCHA.

In [32], a new CAPTCHA was proposed based on scene tagging. It depends on relationships of objects in image. In this method, user will be given image containing multiple objects with the question. For example, question can be like 'What is the name of object below ball' to which the answer will be the name of the object lying below the ball in the image given.

Shardul Vikram, Yinan Fan and Guofei Gu proposed SEMAGE (*SEmantically MAtching imaGEs*) a new image-based two-factor CAPTCHA. In this CAPTCHA, the user have to select images that looks semantically similar from the set of the image. In implementation they simply crawled the web to automatically gather images. But this schemes have legal issues like directly using crawled images. Also generating large and correct database is challenging [33].

In [34], CAPTCHAll was proposed where user has to identify objects from the images and those images are presented with the challenging text asking user to click the particular object's image.

To prevent from Reverse Image Search (RIS) engines and Computer Vision (CV) attacks a method of securing image generation for image-CAPTCHAs is presented in [35] based on noise addition with different styles of image CAPTCHA where user have to select or type the category which describes the image. Some challenges were very difficult to solve because very few hints were provided to identify what actually the picture depicts.

In [36] a new image CAPTCHA is proposed named CAPTCHAStar based on user interaction. Several small white squares (stars) are presented to the user randomly placed inside a squared black space (drawable space). The user is asked to change the position of the stars by moving her cursor until she is able to recognize a shape. In particular, CAPTCHAStar creates such a shape starting from a picture randomly chosen among a huge set of pictures.

Darryl DSouza, Phani C. Polina and Roman V. Yampolskiy in [37] proposed Avtar CAPTCHA based on face recognition where the user will be given avtar faces and human faces from which they have to identify avtar faces. 12 grayscale images were provided to the user.

In [38], Gaurav Goswami,Brian M. Powell, Mayank Vatsa, Richa Singh and Afzel Noore proposed FaceDCAPTCHA where users have to identify the faces of humans which are distorted with complex background. It uses the limitations of machine algorithms like they cannot distinguish between cartoon faces and real ones. In this CAPTCHA user will be provided with distorted images of both fake and real faces and they have to identify real one by marking the center (approximately) of real faces. If user marks the correct faces they passes the test.

In 2014, Vinay Shet talks about new CAPTCHA named NoCAPTCHA reCAPTCHA in Google Security Blog. This CAPTCHA is click based and is very user-friendly. However if the risk analysis engine developed to help reCAPTCHA fails to predict the users which are genuine then the system will prompt one more test to identify humans and that test would include set of images with the phrase like "select the images of car" [39].

In [40], a Chimera CAPTCHA is proposed that requests users to select only a chimera object (that cause a feeling of strangeness because its appearance is different from ones judged by common sense) that is merged from two 3D objects, in a question image, which consists of some 3D objects and the chimera object. If a user clicks only chimera objects in a question image, the system identifies the user as a human. Table 2.2 includes different kinds of image-based CAPTCHA with their advantages and disadvantages.

Table 2.2: Summary of Image-CAPTCHAs

Author	**Title**	**Year**	**Methodology**	**Advantages**	**Disadvantages**
Datta et al.[27]	IMAGINATION: a robust image-based CAPTCHA generation system	2005	Based on geometric patterns where user have to mark center of image and proper category should be selected based on list.	User-friendly and robust against automated attacks like random attacks. It removes ambiguity problem in labeling images hence making easy for users.	Side channel attacks can be carried out
Shirali-Shahreza et al.[28]	Multilingual CAPTCHA	2007	Set of images are shown and user has to choose the image of specific object.	User don't need to know English language because messages will be shown in native language	Only seven languages are supported
Elson et al.[29]	Asirra: a CAPTCHA that exploits interest-aligned manual image categorization	2007	User have to select the images describing either dogs or cats from a set of 12 random images.	Large database and less frustrating for humans.	Assira requires more space on screen and can lose security if database is compromised
Gossweiler et al.[30]	What's up CAPTCHA?: a CAPTCHA based on image orientation	2009	User has to adjust the randomly rotated images into upright orientation.	A prior knowledge of labels is not required and is language independent	Random guess attack is possible

Continued on next page

Continued from previous page

Author	Title	Year	Methodology	Advantages	Disadvantages
Matthews et al.[32]	Scene tagging: image-based CAPTCHA using image composition and object relationships	2010	Depends on relationships of objects where user have to answer the question related to the given image containing multiple objects.	No need of large correctly tagged image database	Random guessing attack
Aditya Raj et al.[41]	Picture CAPTCHAs With Sequencing: Their Types and Analysis	2010	Based on sequencing in pictures	User don't need to type anything and resistant to random guessing attacks	Difficult for users to understand and so can be time-consuming
Vikram, Shardul et al.[33]	SEMAGE: A new image based two-factor CAPTCHA	2011	User have to select images that looks semantically similar from the set of the image	Language-independent, highly-flexible for customizations and resistant against bot-attacks	Fails to automatically generate challenge database
Darryl DSouza et al. [37]	Avatar CAPTCHA: Telling computers and humans apart via face classification	2012	Based on face detection where user has to detect avtar(artificial) faces	User-friendly	Small database used
Obimbo et al. [34]	CAPTCHAll : An Improvement on the Modern Text-based CAPTCHA	2013	User has to identify objects from the image displayed	Avoids distortion and is usable	Labeling content is subjective; same content might be labeled differently by different users.

Continued on next page

Continued from previous page

Author	Title	Year	Methodology	Advantages	Disadvantages
Goswami et al. [38]	FaceDCAPTCHA: Face detection based color image CAPTCHA	2014	Users have to identify the faces of humans from the set of cartoon and human faces which are distorted with complex background.	Lower machine learning attack rates	Storage issue and security is lost if database compromised
[42]	Introducing "No CAPTCHA re-CAPTCHA"	2014	Click based re-CAPTCHA	Better accessibility and advanced security	If cookies are not kept by the browser (such as Private browsing), the old reCAPTCHA system is used.
Mauro Conti et al. [36]	CAPTCHA-Star! A novel CAPTCHA based on interactive shape discovery	2015	Based on user-interaction and ability of humans to recognize shapes	Usable and resilient against traditional and automated ad-hoc attacks	It is not secure against all possible attacks

2.3 Audio-Based CAPTCHA

Visually disabled users were facing difficulties in solving CAPTCHA. So, especially for them audio based CAPTCHA was developed. It contains a download-able audio clips which the user should listen and can then submit the correct word [13]. Also the audio clip is distorted and presented to the user. Many audio CAPTCHA were proposed from which one of them was a novel sound based CAPTCHA [43] that exploits the gaps between human voice and synthetic voice. In this CAPTCHA user have to read the phrase given to pass the test. It was proved for human voice the success rate of 97%. In [44] a new type of CAPTCHA was proposed that can be used by both kind of users whether he/she is visually impaired or not. They included both the image and audio file. But with this approach the limitation was it's finite database of combination of image and sound.

In 2007, reCAPTCHA was developed and was acquired by Google in 2009. It provides websites with images of words that are difficult for OCR (*Optical Character Recognition*) software to detect. It also contains audio CAPTCHA option. In reCAPTCHA audio CAPTCHA , users success rate was very low because of its vocabulary and distortion techniques used. It was very difficult for users to understand the words[45]. In 2012, reCAPTCHA started using images of house numbers from Google's Street View project, in addition to scanned words. In 2014, reCAPTCHA developed another system where users are asked to select one or more images from nine images.

Audio CAPTCHA were used by many websites. In eBay audio CAPTCHA fixed data field of 10 digits and 6 spoken characters were used. It was available in different languages depending on sites. It has high user success rate and was less vulnerable then Google as Google audio CAPTCHA contained beeps at the beginning which helps attacker to identify when CAPTCHA will begin. One of the highest success rate of 95% was achieved by Slashdot. It uses strong data field of letters and words. The speaker in this audio along with saying whole word also spells it which make easy for users to recognize. It uses variable length strings so it makes CAPTCHA harder [45]. For VoIP environments, most suitable CAPTCHA was audio CAPTCHA. An audio CAPTCHA was developed for use in VoIP systems. Their algorithm consists of attributes of CAPTCHA like vocabulary, noise ,time,etc. They used combination of all attributes to make CAPTCHA robust [45].

In [46], an audio CAPTCHA was described where a real time audio of specific sounds are played like of bell or piano and user have to identify those sounds from series of 10 sounds. It does not allows replays and requires real time interaction during playback. User may get frustrated because of prohibiting replays specially with long signals. In [47], an audio CAPTCHA was proposed based on the same idea of recognizing acoustic sounds but this CAPTCHA does not require real-time interaction during playback and unlimited number of replays are allowed. In [48], to confuse speech recognizer additional unnecessary speech sounds are added in the audio. User has to identify meaningful words.

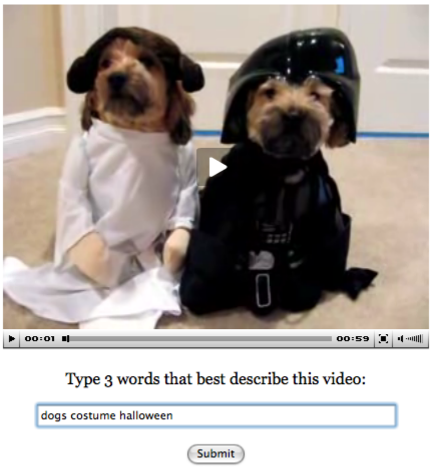
Different kinds of audio-based CAPTCHA are summarized in Table 2.3.

Author	**Title**	**Year**	**Methodology**	**Advantages**	**Disadvantages**
Jonathan Holman et al.[44]	Developing usable CAPTCHAs for blind users	2007	Both visual and audio CAPTCHA where both image and audio go along with the same answer	Usable for both users with and without visual impairments	Small database
Gao et al.[43]	An audio CAPTCHA to distinguish humans from computers	2010	User have to read the phrase given to pass the test.	It needs less space for audio files and exploit the gaps between human voice and synthetic voice	Kind of synthetic voice software used is uncertain
Yannis Soupionis et al.[45]	Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony	2010	Based on VOIP attributes like background and intermediate noise, character variations, different announcers in a random and automated way	Resistant against bot attacks	No evaluation for its effectiveness by tools
Hendrik Meutzner et al.[47]	A Non-speech Audio CAPTCHA Based on Acoustic Event Detection and Classification	2016	Based on classification of acoustic sound events	Independent of language skills and allows replays	User may get confuse with sounds of acoustic events
Hendrik Meutzner et al.[48]	Constructing Secure Audio CAPTCHAs by Exploiting Differences between Humans and Machines	2015	Artificial unnecessary speech sounds are added to confuse speech recognizers	No distortion and usable	Small vocabulary of words

Table 2.3: Audio-CAPTCHAs

2.4 Video-based CAPTCHA

In this CAPTCHA, video will be displayed to the user and user has to enter the words into box describing the video. User will fail the test if the entered tags does not match with the ground truth tags. Video CAPTCHAs use videos rather than images or text. In one of the CAPTCHA, users are shown You Tube videos and ask them to tag descriptive keywords. A new CAPTCHA was presented in [49] where user provides 3 words for describing the video. Test is passed only when the user's tag matches with the automatically generated tags. To test their CAPTCHA they followed the methodology: Firstly they aimed to discover behaviours of video tagging of users, then they estimated attack success rates on some samples. Finally they validated the parameters of the video CAPTCHA.


Type 3 words that best describe this video:

dogs costume halloween

Figure 2.3: Example of Video-based CAPTCHA[5]

In [50], a content based video CAPTCHA was presented which was generated from youtube videos that conatins label of the person who uploaded the video. An example of video based CAPTCHA is shown in Fig 2.3. Video-based CAPTCHA are unbreakable by OCR techniques and they are not affected by laundry attacks. NuCAPTCHA is one of the CAPTCHA technique words are shown flying and in the background small video is playing. User have to recognize those flying words[51]. This words are easy to recognize as it does not involve any distortion, overlapping, warping, etc. It sometimes provides greater security than text-based and image-based CAPTCHA. In [52], scheme is proposed to enhance CAPTCHA schemes by providing random movements to put objects in motion. Random set of characters would be moving in dynamic fashion.

To prevent bot attacks Kameswara Rao, Kavya Sri and Gnana Sai proposed a novel video CAPTCHA where an advertisement is shown to the user which is predefined. Multiple options are provided from which user has to select the one by identifying product relating to the advertisement [5]. In [53], a new CAPTCHA was proposed based on 3D animation and recognition of moving objects in videos. They use characters as the content of verification code but they change the carrier of those words from still images to vivid 3D animation. They also proposed a new design principle known as zero knowledge per frame principle so that each animation frame would not leak any information about verification codes content, so that it makes current computer programs encounter difficulties to attacks using OCR methods. In [54], instead of asking user to analyse, user will be asked to produce something i.e user has to perform some gestures like moving hand, saying yes/no, etc. This gestures will be captured by webcam. Different kinds of video-CAPTCHAs are summarized in Table 2.4.

Author	Title	Year	Methodology	Advantages	Disadvantages
Jing-Song Cui et al.[53]	A CAPTCHA implementation based on moving objects recognition problem	2010	Based on 3D animation and recognizing moving objects presented in videos	Could resist against OCR techniques	Need to improve its security
Rao, Kameswara and Sri et al.[5]	A Novel Video CAPTCHA Technique To Prevent BOT Attacks	2016	Multiple options are provided from which user has to select the one by identifying product relating to the advertisement shown.	Because the user has to recognize the commercial product from many products, it is very difficult for bots to identify the objects presented in the video correctly	It takes more buffering time and requires more memory space
Kurt Alfred Kluever et al.[49]	Evaluating the Usability and Security of a Video CAPTCHA	2008	Video-based CAPTCHA where user has to provide three words that describes the video	Usable and secure against frequency-based attack	Language dependent, streaming videos exposes the ID of video
Kurt Alfred Kluever et al.[50]	Balancing Usability and Security in a Video CAPTCHA	2009	Based on content-based video labeling	Enjoyable for users and public database is used(tags from the YouTube video uploaded by public are used)	Language dependent
Maria De Marsico et al.[54]	FATCHA: the CAPTCHA are you!	2015	Based on some gesture like moving head captured through web-cam	Provide both registration and authentication	Not usable for all type of users and need large database of videos

Table 2.4: Video-CAPTCHAs

2.5 Issues of CAPTCHA

There are many issues with CAPTCHA including issues with design, implementation, usability, etc. With making CAPTCHAs complex it also affects the usability of users. In [55], various tests were conducted and examined that how different CAPTCHAs and their complexity affects the user experience.

In [56], several experiments and user studies were carried out regarding the use of English and regional CAPTCHA tests on non-English pages of multilingual websites and results were obtained in terms of accuracy and response time. The CAPTCHA image implemented in English reduces the usability of CAPTCHA tests and also can make such features inaccessible for users of regional language who do not know English language. There are some uncover impact factors of text-CAPTCHA discussed in [57] and it is shown that how the factors like characters displayed, gender of users, their educational background affects the correctness of the CAPTCHA. The requirement for newer technologies has led to thoughts about using human senses rather than human thinking capabilities, to verify human presence. In [58], a comparison of all skin detection techniques is mentioned with their issues and the main drawback is the fact that the different skin colors might cause different bandwidths to be reflected, which can be overcome during implementation.

2.5.1 Text-based CAPTCHAs issues

Distortion- To make CAPTCHA more complex more distortion or noise is added like various lines, blurred letters, variations, multiple fonts etc due to which users gets confused and are not able to identify them which leads to usability issues. To make CAPTCHAs usable response time low, accuracy must be high and perceived difficultly need to be less [3]. Distorted characters creates ambiguity which are difficult for users to identify and they have to attempt multiple times which also affects the security [59].

Character size- Size of the character also affects the security of CAPTCHA because larger the character size their is larger probability of random guessing attacks and that also lead to more characters look similar causing confusion [59].

Length- Length of the string should be large as it can secure the result more. CAPTCHAs should be of variable length as fixed-length CAPTCHA can be easily attacked.

Dictionary attacks- Strings from the dictionary words should be used in CAPTCHA as it would be more easy for humans to recognize meaningful words than random strings. But this scheme can also make easy for machine to attack. Also random strings when distorted are very difficult for humans to recognize. So, one way to overcome this issue can be use of pronounceable strings which are not purely random and also can reduce dictionary attacks.

Colour- To make segmentation difficult, colour plays important role in it. But it depends on the design of the CAPTCHA. If the design includes that the background colour of the image is different than the characters included then it is very easy to extract the string from the image. Using coloured background decreases the usability of users as it can confuse them [60]. Also the characters having different colours can lead to fatal design issue.

One of the biggest bank of China using text-based CAPTCHA was targeted and it's vulnerabilities like fixed-character length of text, only lower case characters were used, etc were identified in [61]. The characters were not segmentation resistant. Also they showed some methods through which their CAPTCHA can be easily cracked. The site megaupload.com used Megaupload CAPTCHA which was one of the largest file uploading and sharing websites. This mechanism uses connected characters and parts are removed when characters connects horizontally. But these CAPTCHAs were attacked and cracked at success rate of 82% [62]. In [63] they proposed a new segmentation method for connected characters using BP neural network and drop-falling algorithms. This method can solve CAPTCHAs having connected characters but fails if it seriously distorted or overlapped characters. In [64], Visual CAPTCHAs provided at CAPTCHAservice.org were attacked and cracked. They exploited design errors and using simple naive pattern recognition algorithms they were successful in breaking many visual CAPTCHAs.

Microsoft CAPTCHA was vulnerable to to low-cost segmentation attack. A no of text CAPTCHA were cracked with overall success rate of 60% and they achieved more than 90% segmentation success rate [65]. In [66], novel approach was discussed which was used in breaking text-based CAPTCHA with variable text and orientation using segmentation and recognition. SVM classifier is used in recognizing straightened characters. They achieved segmentation success rate of 82% for reCAPTCHA 2011. Financial institutions have also deployed CAPTCHAs for protecting their services. In [67], new image processing techniques and pattern recognition algorithms were proposed to break e-banking CAPTCHA. They got success rate of almost 100%. In [68] an algorithm was proposed to defeat rotated text-CAPTCHA by transformation and segmentation using their adaptive system.

2.5.2 Image-based CAPTCHAs issues

CAPTCHA based on images can be difficult to recognize for the people who have low vision or colour blindness problem. The basic image based CAPTCHA have common weakness that is small number of possible solutions due to which random guessing can be easily done. In some CAPTCHAs images of things are not used like a beach or a cat because images are difficult to have an exact same answer for an particular object. An image of a beach may generate various form of responses like sea, sand, ocean, and so on. But a CAPTCHA system that uses strings or words is paired with a particular solution.

Mainly two types of attacks are possible to break image CAPTCHA- Random guessing attack and Pictionary based attack. In pictionary based attack, bot maintains the dictionary of pictures. This attack exploits the fact that images can be repeated in CAPTCHA. But this attacks are defeated by using concept of sequencing in pictures where user has to determine logical sequence of object pictures based on tags provided with pictures [41]. Content-based image retrieval techniques can easily identify similar images. In Image based CAPTCHA system also needs the knowledge of labels in advance. To make CAPTCHA harder noise is introduced in images which can prevent bot attacks but it affects the accessibility of humans.

In [69], it is shown that how the functionality of image based web services can act as an attack that can easily solve the challenges used in the image CAPTCHA. They proposed an attack based on image web services, CAPTCHA design flaws, regular expression power, etc. Various attacks are carried on image CAPTCHAs schemes. In [31], Machine-learning and segmentation attacks were presented against the image-CAPTCHAs like IMAGINATION, Assira, ARTiFACIAL and framework of designing robust CAPTCHA was provided using the results and lessons from the attacks.

2.5.3 Audio-based CAPTCHA issues

Audio CAPTCHA also contains noise so that it is not broken by speech recognition techniques. But this noise also leads to usability problem. Because of noise some confusing characters makes difficult for user to hear like ’a’ and ’8’ are similar in sound. The language in which letters are read are sometimes not understandable to humans.

Google used a fixed data of ten digits which was inadequate and it was vulnerable to attacks. MSN audio CAPTCHA were also vulnerable as it uses very weak and constant noise in background. But it was very easy for humans and had a high success rate. In [70] they tried to break the audio CAPTCHA. They followed the method of first splitting files into parts of characters spoken or noise. They used KNN, AdaBoost and SVM classifiers.

Main issue of audio CAPTCHA is the same as with the visual one because just like it is sometimes difficult to recognize which individual characters are being used, in the same way it is also difficult to differentiate individual sounds. Behind the words that are spoken there exist so much noise that user is unable to identify the spoken words. Noise is added to prevent automated attacks but it seems that it is affecting user's usability more. In [71], researchers proved that DeCAPTCHA was successfull in defeating most commercially available audio CAPTCHAs, including Authorize (89% of the time), eBay (82%), Microsoft's Live.com website (49%), Yahoo (45%), and Digg (41%). These all sites were vulnerable to machine learning attacks. DeCAPTCHA is a two-phase audio CAPTCHA solver which is based on non-continuous speech that helps in breaking modern audio CAPTCHAs .

2.5.4 Video-based CAPTCHA issues

Video CAPTCHAs are not breakable by OCR techniques but due to its large size users faces difficulty in downloading video. These CAPTCHAs are very difficult to use and is time-consuming. In some video CAPTCHAs user have to provide three words describing video. Computer vision techniques can be used to located frames with text-segments in them, OCR them, and submit these as tags. To locate videos with similar content, Content-based Video Retrieval systems could be used and can submit them. Content of the video can be indicated using Audio analysis. Video CAPTCHAs can be main issue for blind people. It also increases computation load on server. Mainly because of the large size of file user have problem to download them and get the CAPTCHA. Video CAPTCHAs are not so popular because it is the difficult to provide a reasonable amount of videos, storage is required, and everyone cannot watch and understand them.

Issues of different types of CAPTCHA are summarized in table 2.5.

Type of CAPTCHA	**Issues**	**Attacks**
Text-based CAPTCHA	• Distortion affects usability because of confusing characters • Character size leading to random guessing attacks • Fixed-length strings can be easily attacked • Issues in presentation like font type and size, image size, use of colour affects usability	• One of the biggest bank of China using text-CAPTCHA was targeted due to its vulnerabilities like fixed-length characters[61] • Megaupload CAPTCHA used by megaupload.com was cracked [62] • Visual CAPTCHAs provided at CAPTCHAservice.org were cracked due to design errors using simple naive pattern recognition algorithms [64] • Microsoft CAPTCHA was vulnerable to low-cost segmentation attack [65] • In 2011 segmentation success rate of 82% was achieved for re-CAPTCHA [66]
Image-based CAPTCHA	• Difficult for people who have colour blindness problem • Random guessing issue due to less no of possible solutions • Pictionary based attack • System needs the knowledge of labels in advance • Distortion in images affects the usability	• Machine learning and segmentation techniques were used to attack image-CAPTCHAs like IMAGINATION and Assira [31]. • Web-services based attacks • Deep learning techniques are used to break semantic image-CAPTCHAs [72]
Audio-based CAPTCHA	• Noise in audio makes difficult for user to differentiate some characters like ’a’ and ’8’ and hence affects the usability • Language problem • Data-set issue	• KNN, AdaBoost, SVM classifiers and many techniques are used to break audio CAPCTHAs [70] • Due to use of inadequate data Google was vulnerable to attacks as it used fixed data of 10 digits • MSN audio CAPTCHA was vulnerable due to use of weak and constant noise in background • DeCAPTCHA was successful in defeating many commercially available audio CAPCTHAs like Authorize (89% of the time), eBay (82%), Microsoft’s Live.com website (49%), Yahoo (45%), and Digg (41%) [71]
Video-based CAPTCHA	• Large file size • Time-consuming • Increases computation load on server	• Computer vision techniques and content-based video retrieval systems can be used to break video-CAPTHAs

Table 2.5: Issues of CAPTCHA

2.6 Comparison of different kinds of CAPTCHA

Mainly there are three different methods of implementing CAPTCHA - OCR method, Visual Non-OCR method and non-visual. In OCR based CAPTCHAs user is provided with some text or word in form of image. User have to type the text from the image. Text in the image would be distorted because of presence of various variations so that it would be difficult for OCR algorithms to recognize them. These methods are very commonly used in many websites like MSN, Yahoo, Google, etc [73]. People with low vision or who have disability like Dyslexia mainly have problems with this technique.

To overcome the drawback of OCR CAPTCHAs, some visual methods were proposed. For example, user will be given a picture with the text that 'Click on Mango'. User must then click on image where Mango is seen. User have to identify object rather than reading distorted text. This methods are easy but are very rarely used because of low security. Also random guess attacks can be performed on this type of CAPTCHA.

Audio CAPTCHA is non-visual CAPTCHA where an audio clip is to be heard by user and he/she has to type the spoken word. Audios are added with noise to make difficult for speech recognition techniques to recognize. When these method was evaluated in [74] it was proved that these CAPTCHA is easy for machines but more hard for humans as large no of users were unable to pass the test. Also the machine learning based attacks to audio CAPTCHA have successfully solved 45% of Yahoo and 49% of Microsoft audio CAPTCHA and it is seen that the difference between human and computer audio capabilities is significantly less than the difference between human and computer visual processing [71].

According to the tests conducted for evaluating user experience in [55] the most frustrating CAPTCHA was text-based. People found difficulty in recognizing the distorted characters. Arithmetic based CAPTCHA was found less frustrating than text-based. Also the participants found image-based CAPTCHA more enjoyable than any other. According to them the new CAPTCHA that is 'NO CAPTCHA' where user has to check the box was the least frustrating test for users. But the mother tongue of the participants in this study was not English so results might be affected especially for text-based. In [75], a study was presented about how much tough is CAPTCHA for humans. They collected image CAPTCHAs and audio CAPTCHAs and they found that audio CAPTCHA is more harder to solve than image CAPTCHA. They identified that non-native speakers of English were more slower. A survey[76] was done based on user affinity of choices and concerned about usability features of current CAPTCHA schemes. The results are the features that users select as usable ones. In this survey users have chosen image-based CAPTCHA as the best scheme.

2.7 Breaking of CAPTCHA

Nowadays OCR techniques have been developed which can easily break the CAPCTHA. Main tasks in breaking CAPTCHA includes segmentation and then further character recognition. Segmentation process divides the image into parts and then they are sent to character recognition process where characters are identified using classifiers. But if an image contains any overlapping letters or distortion then segmentation is not so easy. Content Based Image Retrieval (CBIR) methods are used for segmentation of an image in different areas, identification of regions of interest and extraction of semantic content expressed by the image or part of it [3]. In [77], techniques that were used to break Teabag 3D CAPTCHA are described. There are different techniques through which a CAPTCHA scheme can be broken.

Pre-processing includes separating characters from background by adaptive binarization that is convert into gray-scale image. The noise or distortion added in background is removed in pre-processing. Segmentation techniques includes segmenting the images into parts which includes single characters. There are many segmentation methods like using vertical projection. A histogram is created which represents the number of character pixels per column in image. Many CAPTCHAs are recognized using active deep learning. In [78] a CAPTCHA solving technique is proposed that trains the deep CNN (Convolution Neural Network) using small set of images initially and then exploits the test samples to improve the classifier. New samples are selected from test set based on their uncertainty. Their approach improves the performance of the network.

Breaking CAPTCHA with DeCAPTCHA-DeCAPTCHA works by considering the voice energy spikes. To do so it applies a discrete Fourier transform (DFT) to the wave file and then isolates the energy spikes. DeCAPTCHA uses a supervised learning algorithm that looks at these decompositions to build the model which it uses to recognize digits [79].

Audio-CAPTCHAs can be cracked using several machine learning techniques like mel-frequency cepstral coefficients (MFCC), perceptual linear prediction (PLP), and relative spectral transform-PLP (RASTA-PLP) that are used to extract features from speech. Techniques like AdaBoost, SVM, and k-NN are also used to break CAPTCHA [70]. Simple Naive pattern recognition algorithms were successful in breaking many visual CAPTCHAs [64].

Chapter 3

Proposed Method

To reduce bot attacks, more complex CAPTCHAs are generated with distortions and noise that affects the usability of users. Users get frustrated because of refreshing the CAPTCHA many times as they face difficulty in reading characters of the CAPTCHAs due to noise. Hence, instead of making CAPTCHA more complex, security can be increased by developing a new CAPTCHA verification method which is difficult for the bots but easy for the humans to pass the verification process. A new approach is proposed using Virtual Keyboard.

In the proposed approach, text-based CAPTCHA is created without noise that makes easy for the user to read and pass the test in a single attempt in most cases. The user uses the virtual keyboard to input CAPTCHA word. However, this word is stored in the form of the position of the characters. The keys pressed by the users are also highlighted and the sequence number is assigned to each character pressed by the user. The sequence number of a particular character can be viewed by the user by placing the mouse pointer over the specific key. This method avoids the use of textbox to take input from the user which makes it difficult for bots to input the CAPTCHA characters.

In addition to that, the proposed approach adds complexity by randomization of keys of virtual keyboard. It should be noted that the proposed approach compares the CAPTCHA text using key positions of the key pressed by the user rather actual value of keys. The flowchart of proposed method is shown in Fig 3.1.

To make scheme more difficult for bots, the proposed method is extended by using handwritten characters in the virtual keyboard. The use of handwritten virtual keyboard makes difficult for bots to identify the characters. The use of handwritten characters makes the test between humans and computer more stringent. Humans have knowledge of handwritten characters and can recognize them easily than bots.

A dataset of English handwritten characters used in this approach is taken from Chars74K dataset [80]. The dataset consists of 64 classes (0-9, A-Z, a-z), segmented characters from natural scenes, handwritten characters and synthesized characters from computer fonts. This approach uses only handwritten characters from the mentioned dataset that includes 55 sample per class. In this dataset [80], both English and Kannada symbols are available. The dataset consists of :

- 64 classes
- 7705 characters acquired from natural scenes
- 3410 handwritten characters
- 62992 synthesised characters from computer fonts

In addition to that, positions of CAPTCHA and virtual keyboard is randomized and can be displayed at any position on the screen. Hence, with the characters of the virtual keyboard, the position of CAPTCHA image and keyboard is also randomly displayed on every refresh of the page.

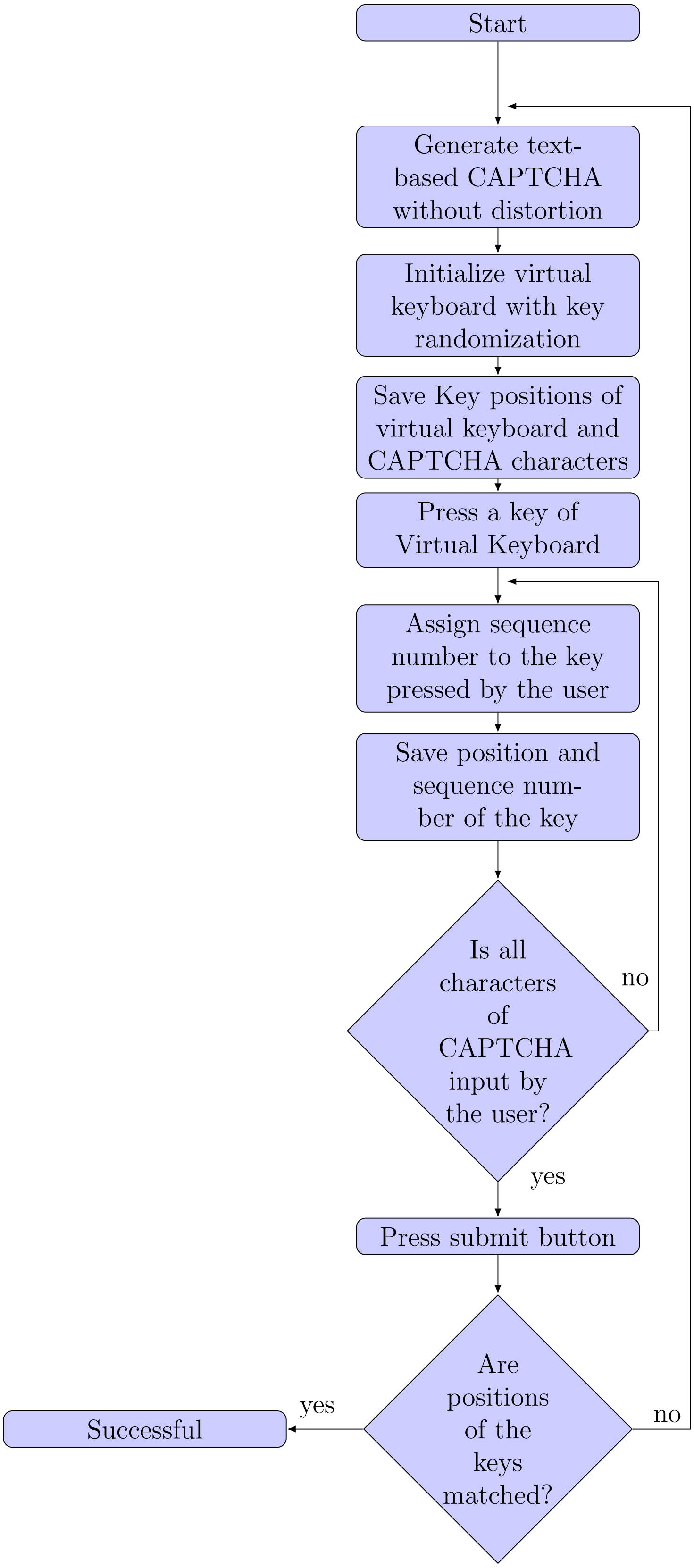

Start
Generate text-based CAPTCHA without distortion
Initialize virtual keyboard with key randomization
Save Key positions of virtual keyboard and CAPTCHA characters
Press a key of Virtual Keyboard
Assign sequence number to the key pressed by the user
Save position and sequence number of the key
Is all characters of CAPTCHA input by the user?
no
yes
Press submit button
Are positions of the keys matched?
yes
no
Successful

Figure 3.1: Basic working flow of Virtual Keyboard

Chapter 4

Simulation Setup and Results Discussion

The proposed approach is verified using JAVA language. A CAPTCHA image of random characters generated by the server is displayed to the user. It should be noted that the proposed approach does not generate fixed length CAPTCHA. In addition to that noise is removed to increase readability of the CAPTCHA. When a page is loaded, the positions of the characters are saved. When the user clicks the submit button, the position and sequencing of the CAPTCHA-text is compared with the position and sequencing of the virtual keyboard keys pressed by the user. If the positions are matched, the user gets the access of the required services provided by the server otherwise, the page will be refreshed and a CAPTCHA test begins with a new text-CAPTCHA and keyboard.

An example of CAPTCHA test is shown in the Figure 4.1. The characters of the keyboard get highlighted as the user clicks the character of the keyboard. This helps the user to identify the characters which have been input by the user. This can be evident through Figure 4.2. Each character is assigned a unique sequence number as soon as the user clicks on it. This sequence number helps the user to order the characters which have been input by him. The sequence number of character 's' is shown to the user when a mouse hovers on the character 's'. This can be evident through Figure 4.3. A user is required to click on submit button when all characters are input by the user.

The example of handwritten virtual keyboard is shown in Fig. 4.4. To test the usability of both the virtual keyboards with handwritten and typed characters, response time analysis was carried out. This analysis was done to compare the response time taken

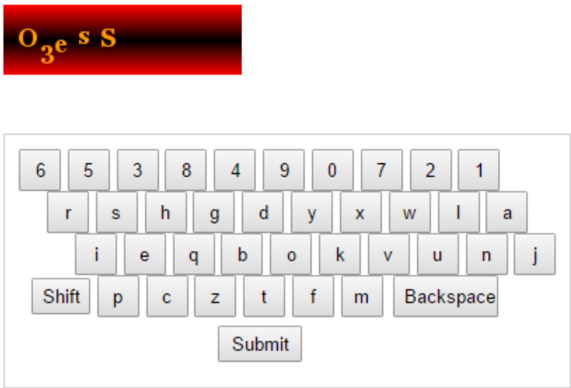


Figure 4.1: Snapshot of Captcha and Keyboard

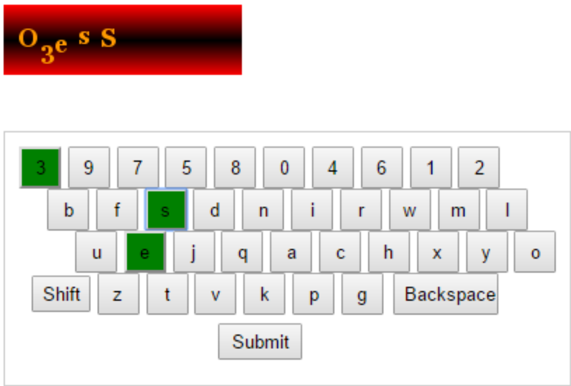


Figure 4.2: Snapshot of keyboard with keys highlighted

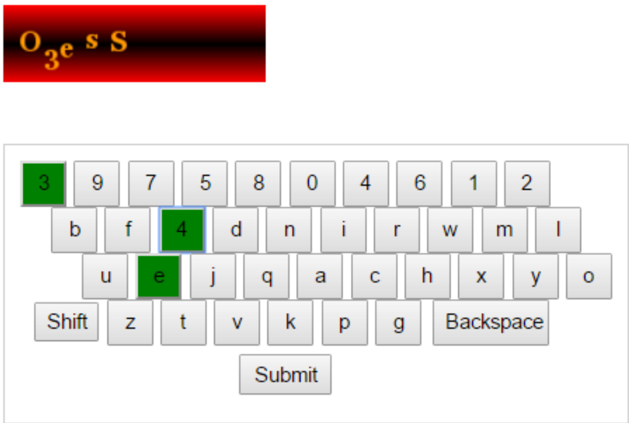


Figure 4.3: Snapshot of sequence displayed on mouseover

by user and machine to enter the CAPTCHA. For response time of machine, total 30 CAPTCHAs that were generated by the proposed approach were tested by machine and time taken to break each CAPTCHA was noted. The Tesseract tool was used to break these CAPTCHAs. The system on which the tool was tested has following properties-

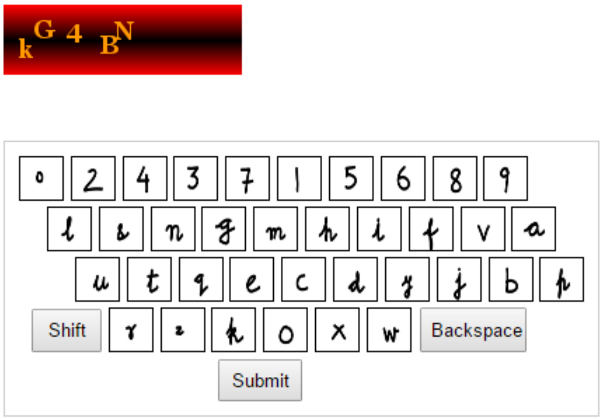


Figure 4.4: Snapshot of Captcha and Virtual Keyboard with handwritten characters

- Processor- Intel(R) Core(TM)i5-3210M CPU @ 2.50 GHz
- System type- 32-bit Operating System, x64-based processor

The 20 CAPTCHAs that were successfully identified by the machine were used for taking response time of the human users.

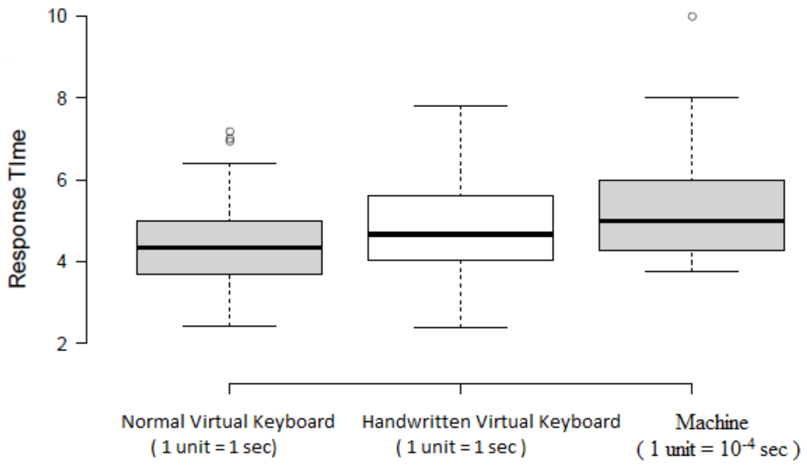


Figure 4.5: Box-Plot of response time analysis

The response time analysis on virtual keyboard with both typed and handwritten characters was performed. The CAPTCHA used here had a variable length between 5-8 characters. All the users were asked to enter the CAPTCHA 2-3 times and average response time per character of the user was calculated. The response time of machine to break those CAPTCHAs was also collected and compared. This experiment included a

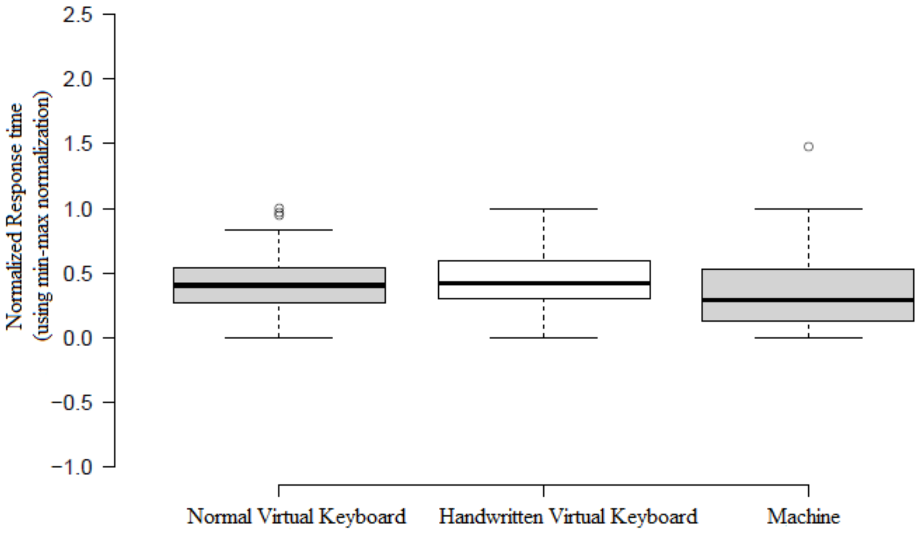


Figure 4.6: Normalized Box-Plot of Response Time Analysis

set of 121 people of varied ages including M.Tech and B.Tech students and faculties of different departments. This collected data is represented in form of Box plot as shown in Fig 4.5. The response time per character of machine was in milliseconds that was converted to seconds*10^4 to compare with response time of normal (typed) and handwritten virtual keyboard. The data of both the virtual keyboards and machine are normalized to 0-1 range using max-min normalization and plotted as shown in Fig 4.6.

Analysis shows that humans takes more time to enter the CAPTCHA than machine. Also, text using keyboard with handwritten characters takes more time to be entered than using keyboard with typed characters. 55 different samples of handwritten characters are used to make the CAPTCHA test more complex. However, some users faced difficulty in identifying handwritten characters and hence took more time to enter the CAPTCHA text.

Chapter 5

Conclusion

For improving the security of the CAPTCHA, a simple and efficient CAPTCHA verification scheme that differentiate between human and machine is proposed. The proposed approach generates a simple text-based CAPTCHA which is easy to read by humans and hence, humans can pass the test in a single attempt as far as possible. At the same time, use of virtual keyboard along with randomized key positions makes it difficult for machines to pass the CAPTCHA test. The proposed approach uses virtual keyboard to take input for CAPTCHA verification, eliminates the input box that makes difficult for boats to decide where to input CAPTCHA text, and uses of position-based verification in place of comparing contents of the CAPTCHA text.

The proposed approach is extended by randomizing positions of the CAPTCHA and virtual keyboard, and both can take any position on the screen. Further the handwritten characters are used to initialize the virtual keyboard to make more harder for bots. In addition to that, response time analysis of both types of virtual keyboards is calculated according to which the time taken by user to enter CAPTCHA using handwritten virtual keyboard is more than using virtual keyboard with typed characters. The machine takes much lesser time than humans to enter the same CAPTCHA.

Bibliography

[1] E. Bursztein, M. Martin, and J. Mitchell, "Text-based captcha strengths and weaknesses," in *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 125–138, ACM, 2011.

[2] S. Choudhary, R. Saroha, Y. Dahiya, and S. Choudhary, "Understanding captcha: Text and audio based captcha with its applications," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, 2013.

[3] M. T. Banday and N. A. Shah, "A study of captchas for securing web services," *arXiv preprint arXiv:1112.5605*, 2011.

[4] G. Sauer, H. Hochheiser, J. Feng, and J. Lazar, "Towards a universally usable captcha," in *Proceedings of the 4th Symposium on Usable Privacy and Security*, vol. 6, p. 1, 2008.

[5] K. Rao, K. Sri, and G. Sai, "A novel video captcha technique to prevent bot attacks," *Procedia Computer Science*, vol. 85, pp. 236–240, 2016.

[6] C. Lei, "Image captcha technology research based on the mechanism of finger-guessing game," in *Third International Conference on Cyberspace Technology (CCT 2015)*, pp. 1–4, IET, 2015.

[7] C. A. Fidas, A. G. Voyiatzis, and N. M. Avouris, "On the necessity of user-friendly captcha," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2623–2626, ACM, 2011.

[8] "The official captcha site." `http://captcha.net`, 2016. last checked: 09.10.2015.

[9] C. Pope and K. Kaur, "Is it human or computer? defending e-commerce with captchas," *IT professional*, vol. 7, no. 2, pp. 43–49, 2005.

[10] B. B. Zhu, J. Yan, G. Bao, M. Yang, and N. Xu, “Captcha as graphical passwordsa new security primitive based on hard ai problems,” *IEEE transactions on information forensics and security*, vol. 9, no. 6, pp. 891–904, 2014.

[11] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, “Re: Captchas-understanding captcha-solving services in an economic context.,” in *USENIX Security Symposium*, vol. 10, p. 3, 2010.

[12] B. Yale, “The captcha: A history, a problem, possible solutions.” `http://www.informit.com/blogs/blog.aspx?uk=Why-Are-CAPTCHAs-So-Awful`, 2014. last checked: 08.10.2015.

[13] N. Divyashree and T. S. Kumar, “A survey on captcha categories,” *International Journal Of Engineering And Computer Science*, vol. 5, 2016.

[14] B. S. Saini and A. Bala, “A review of bot protection using captcha for web security,” *IOSR Journal of Computer Engineering*, vol. 6, pp. 36–42, 2013.

[15] G. Mori and J. Malik, “Recognizing objects in adversarial clutter: Breaking a visual captcha,” in *Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on*, vol. 1, pp. I–134, IEEE, 2003.

[16] G. Moy, N. Jones, C. Harkless, and R. Potter, “Distortion estimation techniques in solving visual captchas,” in *Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on*, vol. 2, pp. II–23, IEEE, 2004.

[17] J. Yan and A. S. El Ahmad, “Captcha robustness: A security engineering perspective,” *Computer*, vol. 44, no. 2, pp. 54–60, 2011.

[18] K. Kaur and S. Behal, “Designing a secure text-based captcha,” *Procedia Computer Science*, vol. 57, pp. 122–125, 2015.

[19] K.-F. Hwang, C.-C. Huang, and G.-N. You, “A spelling based captcha system by using click,” in *Biometrics and Security Technologies (ISBAST), 2012 International Symposium on*, pp. 1–8, IEEE, 2012.

[20] N. Roshanbin and J. Miller, “Adamas: Interweaving unicode and color to enhance captcha security,” *Future Generation Computer Systems*, vol. 55, pp. 289–310, 2016.

[21] I. F. Ince, Y. B. Salman, M. E. Yildirim, and T.-C. Yang, “Execution time prediction for 3d interactive captcha by keystroke level model,” in *Computer Sciences and Convergence Information Technology, 2009. ICCIT’09. Fourth International Conference on*, pp. 1057–1061, IEEE, 2009.

[22] S. Chaudhari, A. Deshpande, S. Bendale, and R. Kotian, “3d drag-n-drop captcha enhanced security through captcha,” in *Proceedings of the International Conference & Workshop on Emerging Trends in Technology*, pp. 598–601, ACM, 2011.

[23] Wikipedia, “Captcha — wikipedia, the free encyclopedia.” `https://en.wikipedia.org/w/index.php?title=CAPTCHA&oldid=750691307`, 2016. [Online; accessed 21-November-2016].

[24] P. Y. Simard, R. Szeliski, J. Benaloh, J. Couvreur, and I. Calinov, “Using character recognition and segmentation to tell computer from humans,” in *Document Analysis and Recognition, 2003. Proceedings. Seventh International Conference on*, pp. 418–423, IEEE, 2003.

[25] M. Goto, T. Shirato, and R. Uda, “Text-based captcha using phonemic restoration effect and similar sounds,” in *Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International*, pp. 270–275, IEEE, 2014.

[26] V. P. Singh and P. Pal, “Survey of different types of captcha,” *International Journal of Computer Science and Information Technologies*, vol. 5, no. 2, pp. 2242–2245, 2014.

[27] R. Datta, J. Li, and J. Z. Wang, “Imagination: a robust image-based captcha generation system,” in *Proceedings of the 13th annual ACM international conference on Multimedia*, pp. 331–334, ACM, 2005.

[28] M. H. Shirali-Shahreza and M. Shirali-Shahreza, “Multilingual captcha,” in *Computational Cybernetics, 2007. ICCC 2007. IEEE International Conference on*, pp. 135–139, IEEE, 2007.

[29] J. Elson, J. R. Douceur, J. Howell, and J. Saul, “Asirra: a captcha that exploits interest-aligned manual image categorization.,” in *ACM Conference on Computer and Communications Security*, vol. 7, pp. 366–374, 2007.

[30] R. Gossweiler, M. Kamvar, and S. Baluja, “What’s up captcha?: a captcha based on image orientation,” in *Proceedings of the 18th international conference on World wide web*, pp. 841–850, ACM, 2009.

[31] B. B. Zhu, J. Yan, Q. Li, C. Yang, J. Liu, N. Xu, M. Yi, and K. Cai, “Attacks and design of image recognition captchas,” in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 187–200, ACM, 2010.

[32] P. Matthews, A. Mantel, and C. C. Zou, “Scene tagging: image-based captcha using image composition and object relationships,” in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 345–350, ACM, 2010.

[33] S. Vikram, Y. Fan, and G. Gu, “Semage: a new image-based two-factor captcha,” in *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 237–246, ACM, 2011.

[34] C. Obimbo, A. Halligan, and P. De Freitas, “Captchall: An improvement on the modern text-based captcha,” *Procedia Computer Science*, vol. 20, pp. 496–501, 2013.

[35] D. Lorenzi, P. Chattopadhyay, E. Uzun, J. Vaidya, S. Sural, and V. Atluri, “Generating secure images for captchas through noise addition,” in *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*, pp. 169–172, ACM, 2015.

[36] M. Conti, C. Guarisco, and R. Spolaor, “Captchastar! a novel captcha based on interactive shape discovery,” in *International Conference on Applied Cryptography and Network Security*, pp. 611–628, Springer, 2016.

[37] D. D’Souza, P. C. Polina, and R. 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.

[38] G. Goswami, B. M. Powell, M. Vatsa, R. Singh, and A. Noore, "Facedcaptcha: Face detection based color image captcha," *Future Generation Computer Systems*, vol. 31, pp. 59–68, 2014.

[39] V. Shet, "Are you a robot? introducing no captcha recaptcha." `https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html`, 2014.

[40] M. Fujita, Y. Ikeya, J. Kani, and M. Nishigaki, "Chimera captcha: A proposal of captcha using strangeness in merged objects," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 48–58, Springer, 2015.

[41] A. Raj, A. Jain, T. Pahwa, and A. Jain, "Picture captchas with sequencing: Their types and analysis," *International Journal for Digital Society (IJDS)*, vol. 1, no. 3, pp. 208–220, 2010.

[42] "recaptcha." `https://www.google.com/recaptcha/intro/index.html`, 2014. [Online; accessed 12-November-2016].

[43] H. Gao, H. Liu, D. Yao, X. Liu, and U. Aickelin, "An audio captcha to distinguish humans from computers," in *Electronic Commerce and Security (ISECS), 2010 Third International Symposium on*, pp. 265–269, IEEE, 2010.

[44] J. Holman, J. Lazar, J. H. Feng, and J. D'Arcy, "Developing usable captchas for blind users," in *Proceedings of the 9th international ACM SIGACCESS conference on Computers and accessibility*, pp. 245–246, ACM, 2007.

[45] Y. Soupionis and D. Gritzalis, "Audio captcha: Existing solutions assessment and a new implementation for voip telephony," *Computers Security*, vol. 29, no. 5, pp. 603–618, 2010.

[46] J. Lazar, J. Feng, T. Brooks, G. Melamed, B. Wentz, J. Holman, A. Olalere, and N. Ekedebe, "The soundsright captcha: an improved approach to audio human interaction proofs for blind users," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2267–2276, ACM, 2012.

[47] H. Meutzner and D. Kolossa, “A non-speech audio captcha based on acoustic event detection and classification,” in *Signal Processing Conference (EUSIPCO), 2016 24th European*, pp. 2250–2254, IEEE, 2016.

[48] H. Meutzner, S. Gupta, and D. Kolossa, “Constructing secure audio captchas by exploiting differences between humans and machines,” in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 2335–2338, ACM, 2015.

[49] K. A. Kluever, “Evaluating the usability and security of a video captcha.” `http://scholarworks.rit.edu/theses/163`, 2008.

[50] K. A. Kluever and R. Zanibbi, “Balancing usability and security in a video captcha,” in *Proceedings of the 5th Symposium on Usable Privacy and Security*, p. 14, ACM, 2009.

[51] B. Vaishakh and G. Harish, “Captchas: Survey of existing techniques and a new approach,” in *National Conference on Recent Trends in Computer Technology Technology Technology*, pp. 70–73, 2011.

[52] K. Anjitha and I. Rijin, “Captcha as graphical passwords-enhanced with video-based captcha for secure services,” in *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 213–217, IEEE, 2015.

[53] J.-S. Cui, J.-T. Mei, W.-Z. Zhang, X. Wang, and D. Zhang, “A captcha implementation based on moving objects recognition problem,” in *E-Business and E-Government (ICEE), 2010 International Conference on*, pp. 1277–1280, IEEE, 2010.

[54] M. De Marsico, L. Marchionni, A. Novelli, and M. Oertel, “Fatcha: the captcha are you!,” in *Proceedings of the 11th biannual conference on italian SIGCHI chapter*, pp. 118–125, ACM, 2015.

[55] R. Gafni and I. Nagar, “Captcha–security affecting user experience,” *Issues in Informing Science and Information Technology*, vol. 13, 2016.

[56] M. T. Banday and N. A. Shah, "Challenges of captcha in the accessibility of indian regional websites," in *Proceedings of the Fourth Annual ACM Bangalore Conference*, p. 31, ACM, 2011.

[57] T. Tamang and P. Bhattarakosol, "Uncover impact factors of text-based captcha identification," in *Computing and Convergence Technology (ICCCT), 2012 7th International Conference on*, pp. 556–560, IEEE, 2012.

[58] U. Seksaria, M. Namratha, A. Rai, and C. Shree, "Modernization of captcha using skin detection sensors: A survey," *International Journal of Computer Applications*, vol. 138, 2016.

[59] J. Yan and A. S. 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.

[60] K. Kaur and S. Behal, "Captcha and its techniques: A review," *Kiranjot Kaur et al,/(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 5, no. 5, pp. 6341–6344, 2014.

[61] X. Ling-Zi and Z. Yi-Chun, "A case study of text-based captcha attacks," in *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on*, pp. 121–124, IEEE, 2012.

[62] A. S. El Ahmad, J. Yan, and L. Marshall, "The robustness of a new captcha," in *Proceedings of the Third European Workshop on System Security*, pp. 36–41, ACM, 2010.

[63] P. Lu, L. Shan, J. Li, and X. Liu, "A new segmentation method for connected characters in captcha," in *Control, Automation and Information Sciences (ICCAIS), 2015 International Conference on*, pp. 128–131, IEEE, 2015.

[64] J. Yan and A. S. El Ahmad, "Breaking visual captchas with naive pattern recognition algorithms," in *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pp. 279–291, IEEE, 2007.

[65] J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoft captcha," in *Proceedings of the 15th ACM conference on Computer and communications security*, pp. 543–554, ACM, 2008.

[66] O. Starostenko, C. Cruz-Perez, F. Uceda-Ponga, and V. Alarcon-Aquino, "Breaking text-based captchas with variable word and character orientation," *Pattern Recognition*, vol. 48, no. 4, pp. 1101–1112, 2015.

[67] S. Li, S. Shah, M. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking captchas," in *Proceedings of the 26th Annual Computer Security Applications Conference*, pp. 171–180, ACM, 2010.

[68] Y. Wang and M. Lu, "A self-adaptive algorithm to defeat text-based captcha," in *2016 IEEE International Conference on Industrial Technology (ICIT)*, pp. 720–725, IEEE, 2016.

[69] D. Lorenzi, J. Vaidya, S. Sural, and V. Atluri, "Web services based attacks against image captchas," in *International Conference on Information Systems Security*, pp. 214–229, Springer, 2013.

[70] J. Tam, J. Simsa, S. Hyde, and L. V. Ahn, "Breaking audio captchas," in *Advances in Neural Information Processing Systems*, pp. 1625–1632, 2008.

[71] E. Bursztein, R. Beauxis, H. Paskov, D. Perito, C. Fabry, and J. Mitchell, "The failure of noise-based non-continuous audio captchas," in *2011 IEEE symposium on security and privacy*, pp. 19–31, IEEE, 2011.

[72] S. Sivakorn, I. Polakis, and A. D. Keromytis, "I am robot:(deep) learning to break semantic image captchas," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 388–403, IEEE, 2016.

[73] S. Shirali-Shahreza and M. H. Shirali-Shahreza, "Accessibility of captcha methods," in *Proceedings of the 4th ACM workshop on security and artificial intelligence*, pp. 109–110, ACM, 2011.

[74] J. P. Bigham and A. C. Cavender, "Evaluating existing audio captchas and an interface optimized for non-visual use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1829–1838, ACM, 2009.

[75] E. Bursztein, S. Bethard, C. Fabry, J. C. Mitchell, and D. Jurafsky, “How good are humans at solving captchas? a large scale evaluation.,” in *IEEE Symposium on Security and Privacy*, pp. 399–413, 2010.

[76] R. Pakdel, N. Ithnin, and M. Hashemi, “Captcha: a survey of usability features,” *Research Journal of Information Technology*, vol. 3, pp. 215–228, 2011.

[77] V. D. Nguyen, Y.-W. Chow, and W. Susilo, “Breaking a 3d-based captcha scheme,” in *International Conference on Information Security and Cryptology*, pp. 391–405, Springer, 2011.

[78] F. Stark, C. Hazırbas, R. Triebel, and D. Cremers, “Captcha recognition with active deep learning,” in *Workshop New Challenges in Neural Computation 2015*, p. 94, Citeseer, 2015.

[79] E. Bursztein and S. Bethard, “Decaptcha: breaking 75% of ebay audio captchas,” in *Proceedings of the 3rd USENIX conference on Offensive technologies*, p. 8, USENIX Association, 2009.

[80] T. de Campos, “The chars74k dataset: Character recognition in natural images. university of surrey. guildford, surrey, uk,” 2012.