Università
degli Studi
di Padova

Dipartimento
di Ingegneria
dell'Informazione

Master Thesis in Computer Engineering Web information and data

Hunting CAPTCHA-Solving bots

Master Candidate

Anahita Abbaspour

Student ID 2005495

Supervisor

Prof. Mauro Migliardi

University of Padova

Academic Year
2023/2024

Abstract

This thesis presents a comprehensive exploration of CAPTCHAs and their evolving role in the digital landscape. Chapter 1 establishes the foundation by elucidating the critical role of CAPTCHAs in distinguishing between humans and robots. It provides an in-depth understanding of CAPTCHA technology, its performance, and various applications, examining the relationship with the Turing test. Identifying vulnerabilities and potential penetration methods, the chapter concludes with insights into Google's innovative solution, reCAPTCHA. Chapter 2 conducts an extensive examination of diverse CAPTCHA methodologies, emphasizing the need for balance in question complexity for enhanced website security and user verification. Chapter 3 explores the dynamic interplay between Artificial Intelligence (AI) and CAPTCHAs, delving into disruptions caused by AI methods like CNN and RCN. It explains "reCAPTCHA," Google's innovative approach to streamlining CAPTCHA questions, addressing OCR limitations. In conclusion, the thesis underscores the ongoing development imperative for CAPTCHA technology to counteract evolving security threats and ensure a seamless user experience in the digital landscape.

Contents

List of Figures

List of Acronyms

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart

CIA Confidentiality, Integrity and Availability

CNN Convolutional Neural Network

RCN Recursive Cortical Network

OCR Optical Character Recognition

AI Artificial Intelligence

1 Introduction

1.1 Introduction

Today, we are witnessing that web technology is progressing along with other technologies at an ever-increasing speed. According to Cisco [1] it is estimated that there will be 5.3 billion Internet users by 2023 which includes over 66% of the world population which has been able to be ubiquitous in all areas of human life in a short period of time. The existence of rapid developments in communications such as e-mail and cell phones, electronic equipment, entertainment and the transportation industry, as well as fundamental changes in commerce and medicine are just a few examples in this field.

Nevertheless, security is recognized as a major challenge facing this industry. Security threats give rise to major problems for both users and service providers. There are three fundamental aspects of security, known as the CIA triad (Confidentiality, Integrity, and Availability), especially in the context of the web security. These security goals are crucial for ensuring the safety and reliability of online systems and data. CIA is compromised [**2**]:

- Confidentiality: This refers to the protection of sensitive information from unauthorized access. When confidentiality is compromised, sensitive data becomes accessible to unauthorized individuals, leading to potential privacy breaches and misuse of the information. For example, a hacker gains unauthorized access to a database containing users' personal information, including names, addresses, and credit card numbers. This could lead to identity theft and financial losses for the affected users.

- Integrity: Integrity ensures that data remains accurate and unaltered during transmission and storage. If integrity is compromised, data can be modified or tampered with, leading to misinformation and loss of trust. For example, a malicious actor alters the content of a news website's articles before they are published. This can lead to the dissemination of false information and damage the reputation of the news outlet.

- Availability: Availability refers to the continuous and reliable access to resources and services. When availability is compromised, systems or services may become unavailable, leading to disruptions in operations and user frustration. For example, a Distributed Denial of Service (DDoS) attack overwhelms a website's servers with traffic, causing the website to become unreachable. This can result in lost sales for an e-commerce site or the inability of users to access critical information.

When any of these three security goals (CIA) are compromised on the web, it can have severe consequences :

Irreparable Damages: This emphasizes that the damages caused by compromising these security goals can be irreparable, meaning that the negative effects might be long-lasting or even permanent. This can include financial losses, reputational damage, legal consequences, and loss of user trust.

Users: Users' personal information, financial data, and privacy could be compromised, leading to identity theft, fraud, and other forms of cybercrime.

Service Providers: Service providers may suffer financial losses, damage to their reputation, and legal liabilities if they fail to adequately protect user data and ensure the availability of their services.

Denial of Service attacks are among the most destructive attacks and the most common ones in the known web environment, which with repeated requests from servers, disrupt their performance and generate heavy costs for service providers. In addition, there are user/bots who try to conduct malicious activities over the network or spam a website which leads to have the website inaccessible [3].

Service providers have always been looking for a way to prevent such incidents. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a security mechanism used to determine whether a user is human or an automated bot. While CAPTCHA itself is not directly related to all aspects of the CIA triad, it can have some indirect connections. CAPTCHA mechanisms are primarily used to prevent automated bots from accessing sensitive information or performing actions that are meant for human users. By distinguishing between humans and bots, CAPTCHAs help maintain the confidentiality of certain resources or services that are restricted to genuine users.

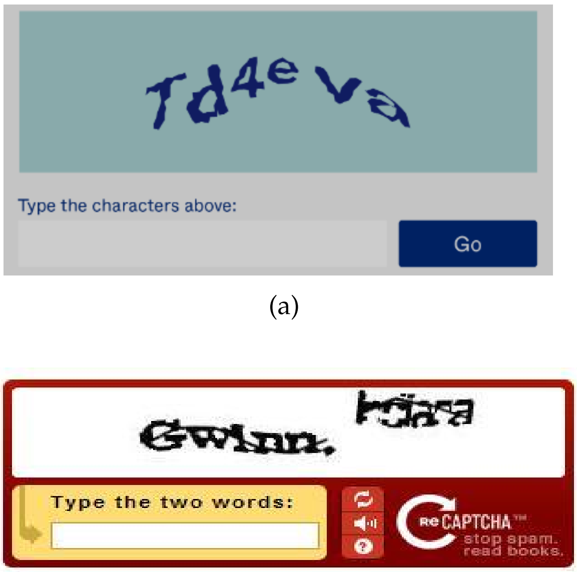
While CAPTCHAs are not directly related to data integrity, they can indirectly contribute to maintaining the integrity of certain online processes. For example, if an online voting system is protected by CAPTCHA, the integrity of the voting process is enhanced by preventing automated bots from casting fraudulent votes. Also, CAPTCHAs can impact availability in a couple of ways by preventing automated bots from overloading a website's resources through actions like spamming forms or performing DDoS attacks, CAPTCHAs contribute to maintaining the availability of the service for genuine users. In some cases, CAPTCHAs can inadvertently hinder the availability of a service by making it difficult for legitimate users to access resources. If CAPTCHAs are too complex or difficult to solve, they might frustrate users and deter them from using a website or service.

In this chapter, the general nature of CAPTCHA, its advantages and reasons for its use, description of its function, the connection with other topics in the world of computer and information, its applications in various parts of the web are discussed and finally, reCAPTCHA as an existing solution is discussed which serves the same purpose as CAPTCHA but includes additional features to enhance security and user experience [4].

1.2 The concept of CAPTCHA

Literally, CAPTCHA means a Completely Automated Public Turing test, to tell computers and humans apart. In most online shopping sites, usually in order to buy a product and before paying money on the bank site a simple and unchallenging test must be passed. In fact, the remarkable point is that the test for humans should be simple and fast. This test, which most of the Internet users have encountered many times, is called CAPTCHA [5]. One of the most widely used types of CAPTCHA is the image of several numbers or letters that a person must enter in the designated box. If the entered phrase is exactly the same as that in the picture, the person has passed the test and can complete the purchase. Figure (1.1) shows two examples of common CAPTCHAs.

The first question that is raised about this topic is why all users need to pass such a test to distinguish between humans and computers. The reason lies in the fact that some profit-seeking users are trying to mislead the system in order to take advantage of the potential security weaknesses in the site's server for



(a)

(b)

Figure 1.1: The form containing CAPTCHA (a) normal (b) more advanced

their own benefit.

Although the number of these people among the millions of Internet users is very small and they form a small minority, the destructive actions of this small group can cause irreparable damage to millions of users. For example, a free e-mail service may be bombarded with hundreds of millions of user account requests by automated programs and may fail and be unable to provide its service.

This attack is only an example of the types of attacks that are carried out against servers. CAPTCHA test helps to identify the nature of users or in other words, to determine which one is a human and which one is a malicious computer program. When web designers and programmers design various forms, the most important challenging point for them is the security of the form.

Internet bots are one of the security challenges faced by designers and owners of websites and blogs. The bots crawl around the pages and find the forms automatically, and then they (bots) complete those forms to receive services from the desired web servers.

So far, there have been various methods proposed to deal with this type of attack, the most famous of which is the use of CAPTCHA code. Perhaps the most important defect of these codes is the difficulty of using them for users so most people have trouble reading the expressions that are displayed and if it is not necessary for them, they refuse to complete the form and send it [6].

There are simpler and more effective ways to improve the security of forms or services against Internet robots. But before that, it is necessary to examine how robots work and behave which will be discussed in the following after general introductions to CAPTCHA and its working.

1.3 CAPTCHA and Turing test

CAPTCHA technology has its roots in an experiment called the Turing test. "Alan Turing", who is sometimes referred to as the father of modern computer calculations, proposed this test as an approach to investigate the possibility of machine thinking or seemingly thought-like performance in 1950 [7]. The classic Turing test is a kind of imitation game. In this game, the investigator asks the participants a question to determine whether one of the participants is a machine and the other is a real human.

The investigator cannot see the participants or hear their voices and has no way of knowing which is a human and which is a machine. If the evaluator cannot consistently distinguish the machine's responses from the human's, the machine is considered to have passed the test. The focus is on written communication rather than spoken language [8].

In CAPTCHA testing, the goal is to create a test or an obstacle that humans can easily pass, but machines cannot pass. It is necessary that the CAPTCHA program be able to provide different codes for different users.

If the image CAPTCHA displays only one static image for each user, it won't take long for a hacker to identify the letters in the form and be able to decode them or write a program that automatically enters the correct answer in the corresponding box.

All CAPTCHA tests are not in the form of a request to type the text in the image and users may be asked to follow the specific geometric shape in the photos in the specified direction using the mouse just like the test in Figure (1.2). Almost all CAPTCHAs are an auditory or visual test. The reason for this is that contrary to the human ability which is easily able to recognize and act properly against images or sounds, it is very difficult for a computer program to recognize

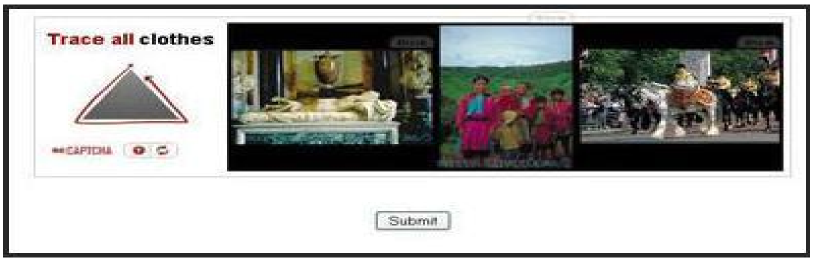


Figure 1.2: An example of a non-textual CAPTCHA

or analyze such tests. One of the alternatives to the visual test is the auditory test.

Audio CAPTCHA usually asks the user to listen to a series of letters and numbers and then enter them in the box. It's normal for the program to distort the speaker's sound a bit and it's also common to have some other sound playing in the background. These things help voice recognition programs to have problems so that attackers are not able to decrypt the CAPTCHA for their malicious purposes with the help of such programs.

The request to read the text and presenting a short interpretation of it is another option for creating a CAPTCHA. CAPTCHA text model actually tests the reader's comprehension skills which can be a challenge for computer programs. For example, CAPTCHA asks a person how his father's brother related to him, now he has to choose the answer from the list. In this list, the following words may be seen: mother, aunt, uncle, television, tree, etc. Although computer programs e.g., chatbots like ChatGPT can produce a convincing text, they sometimes fail to produce the text that is correct. In other words, the produced text can be the result of a false comprehension [**9**].

1.4 CAPTCHA MECHANISM

In this part, in order to have a deep understanding of how CAPTCHA works, its process is described step by step. Before viewing the CAPTCHA by the user, it goes through various steps and then waits for the input from the user. After entering the letters or completing the CAPTCHA process by the user, other steps will be passed. The necessary steps of each CAPTCHA, which are also shown in Figure (1.3) are [10] :

1. The user makes a service request to the server that requires CAPTCHA authentication.
2. The returned page contains an image tag or a script tag to return the CAPTCHA image from the CAPTCHA provider.
3. The browser places the CAPTCHA photo called from the CAPTCHA provider in their respective tags on the page (the user can see the photo).
4. After viewing the photo, the user enters the text in the CAPTCHA text field and sends the form to the web-based program.
5. The web application sends the answer sent by the user to the CAPTCHA provider to be confirmed.
6. The CAPTCHA provider validates the answer sent by the user and gives an answer confirming or rejecting the request.
7. Based on the answer provided by the CAPTCHA provider, the web application decides to reject or approve the request.

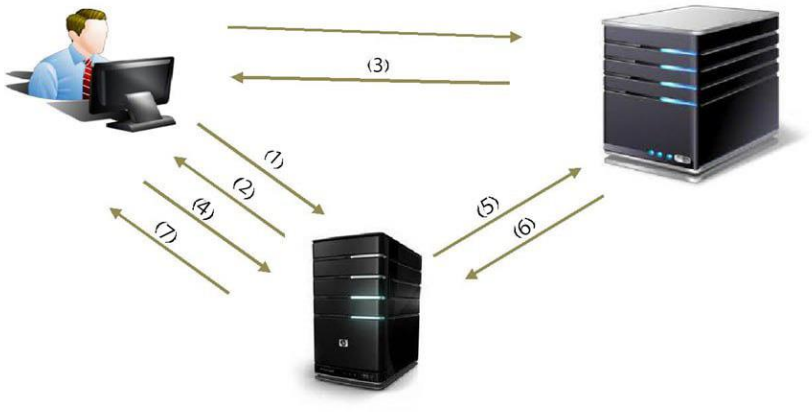


Figure 1.3: CAPTCHA function

1.5 Usage of CAPTCHA

CAPTCHA technology finds its application in a multitude of online scenarios, where increasing security, preventing misuse, and maintaining the quality of user interactions are paramount. CAPTCHA plays a pivotal role in safeguarding the digital world against the challenges posed by automated bot activity. In the following sections, various applications of CAPTCHA is investigated in different domains.

1.5.1 The role of CAPTCHA in online polls

One of the common applications of CAPTCHA is for validating online polls [**11**]. At the begging of internet, in 1991, the Slashdot site conducted a survey based on the opinion of visitors to choose the best place to study for a master's degree in computer science in the United States. The students of two universities, Carnegie Mellon and MIT, won the majority of votes by designing automatic programs called bot. While those two universities had allocated thousands of votes in this way, the other universities had collected only a few hundred votes each. If it is possible to participate in polls by creating a program and change the votes, how can we trust the results of online polls.

The CAPTCHA form can help to prevent programming to abuse the voting system. The application of CAPTCHA for validating online polls helps address both the integrity and availability aspects of the CIA triad. It prevents automated bots from tampering with the poll's results, thus maintaining the integrity of the voting process. Additionally, it contributes to the availability of the poll by ensuring that the poll remains accessible to genuine human users without being overwhelmed by bot-generated votes.

1.5.2 The role of CAPTCHA in registration forms

Registration forms on websites also often use CAPTCHA. For example, free email services such as Hotmail, Yahoo or Gmail allow users to create a free email account [**12**] .Usually, users must enter their personal information in the relevant boxes when creating a user account. But usually these services do not query and confirm such information. They use CAPTCHA to prevent spammers from using email bots.

1.5.3 The role of CAPTCHA in rejecting shopping agent

CAPTCHA can be useful in online ticket sales sites. Without using any filter, it is possible for the broker to buy tickets using a robot in a fraction of a second instead of hundreds or thousands of people. Ordinary customers also become victims of this incident because the tickets are sold out only a few minutes after the start of the sale, and many interested people are deprived of buying tickets. The broker takes advantage of this feeling of enthusiasm and sells the purchased tickets at a high price and makes a huge profit. Although CAPTCHA applications do not prevent brokers and black markets, they prevent such purchases on a large scale and, as a result, prevent many people from buying tickets.

1.5.4 Preventing spam or fake feedbacks

Some web pages have notice boards or contact forms that allow visitors to write something on the site or send a message directly to the site administrators. In order to prevent the wealth of spam to the administrators user accounts, many of these sites have built in a CAPTCHA program to filter annoying messages. CAPTCHA cannot measure the content of the message and prevent receiving rude or immoral messages. But it can help to prevent automatic sending of repeated messages by robots [**13**].

1.5.5 Preventing fake or irrelevant comments on the site and blog

Most of the owners of blogs or sites are fully familiar with automatic online software (which publishes spam comments), which is usually used to increase the rank and improve the rank of the spammer's site. By using CAPTCHA, only real users will be able to publish comments in the blog section of the site, and thus, there will be no need to be a member of the site or blog in order to prevent spam comments [**13**].

1.5.6 The role of CAPTCHA in the site membership

There are many websites on the Internet for providing free services which require membership and creation of a user account from the users. Until recently and before the use of CAPTCHA, a major problem of these websites and service providers was the creation of a large number of accounts by robots that could create hundreds of fake accounts in a few minutes. The use of CAPTCHA system has provided the possibility that only real users are able to complete the form and final registration which has become a necessity of free service provider systems [**14**]. Figure (1.4) shows the CAPTCHAs used by famous websites .

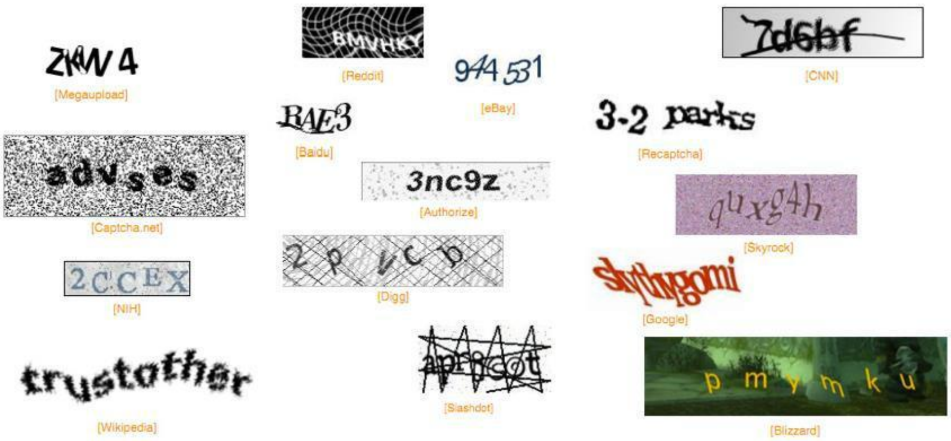


Figure 1.4: Some examples of CAPTCHA use by famous websites

1.5.7 CAPTCHA FOR ONLINE SURVEY

Today, conducting public survey on the Internet without using CAPTCHA is pointless and wrong. One of the most important factors in such sites to confirm the accuracy of the obtained results is that the participants in the survey are not robots. If it is ensured that no robot is able to participate in the survey, the obtained results will be completely valid and can be used in other occasions. The use of various CAPTCHAs is one of the important things that is considered in most of these sites. In survey forms, a field for CAPTCHA is considered to ensure that the user is human before sending the content [**15**].

1.5.8 Preventing the password from being broken

In the past and before the CAPTCHA system became widespread, one of the common methods for unauthorized access to user accounts and access to information was the trial and error of different passwords. In this method, by providing a dictionary containing thousands of words for a specific username it would be possible for the attacker to find the password (dictionary attack or comprehensive search attack). Today, with several wrong attempts in email systems, a CAPTCHA is shown to the user in order to deal with such attacks. After a fixed number of wrong attempts of password, an account gets locked, but it is not a better solution. Ahn et al. [**16**].

1.5.9 Using CAPTCHA in smartphones

Nowadays, mobile phones have become an integral part of modern human life. Due to the ever-increasing advancements of the capabilities of this equipment in various fields, almost all the daily and even personal activities of people have become dependent on these mobile phone. On the other hand, with their capabilities extending far beyond communication, these devices now serve as crucial edge systems within mobile IoT scenarios, help the collection and transmission of sensitive data linked to human activities, often potential forensic evidence. As a result, safeguarding these transactions against misuse and fraud stemming from automation techniques has emerged as a pressing concern.

1.6 Different Classes of CAPTCHA

It's essential to study the diverse range of CAPTCHA methods that are available. This work necessitates a comprehensive compilation of existing research, gathering a vast array of information on the various CAPTCHA techniques that currently exist. For clarity and ease of comprehension, we need to categorize existing variations of CAPTCHAs. Despite the absence of a clearly defined boundary for discerning distinct classes, a practical approach involves the general categorization of CAPTCHA types into well-established classes within the CAPTCH framework. This classification not only facilitates a more organized understanding of the landscape but also contributes to the development of comprehensive strategies for addressing challenges associated with diverse

CAPTCHA implementations. Consequently, to simplify matters, all the distinct types of CAPTCHA schemes are organized under the subsequent headings:

- Text-Based
- Image-Based
- Audio-Based
- Video-Based
- Game-Based
- Biometric-Based
- Social Network-Based
- Invisible CAPTCHA

1.7 Emergence of reCAPTCHA

The most common type of CAPTCHA requires the visitor to type a word or a set of letters and numbers that have been transformed by the program into an image of distorted letters in the corresponding box. Some CAPTCHA creators have suggested the approach of digitizing books for optimal use and creating added value.

A software package called reCAPTCHA has limited the CAPTCHA field to the content type of a scanned part of a part of the book. Computers are not always able to correctly recognize words from digital scans, and humans must type what they see on a scanned page.

Now, by using the words typed by the user and matching them with the corresponding scanned parts, the computer can prepare the entire text of the book digitally. The general method of this approach is as follows

1. reCAPTCHA program manager scans a book.
2. The reCAPTCHA program selects two words from a digital image (The program has already recognized one of the words).
3. If the visitor enters that word in a field correctly, the software assumes that the second word that the user enters is also typed correctly.
4. The second word is added to the set of words that the program will show to other users.

5. As each user types a word, the software compares this word with the original answer.
6. The software receives answers that are sufficient to confirm the word with a high degree of confidence.
7. The word can go to the set of words approved by the software.

This idea may seem time-consuming, but it should be noted that in this case CAPTCHA not only verifies the contents of a scanned book, but also verifies that the users who filled the form are human. On the other hand, those users who participated in this work will also reach their desired service.

Google has recently enhanced reCAPTCHA significantly, introducing an innovative concept named No CAPTCHA or Invisible reCAPTCHA. This novel CAPTCHA iteration eliminates the need for user engagement, rendering even the act of checking a box unnecessary. According to an article on developers.google.com, this CAPTCHA variant is triggered directly upon a user's interaction with an existing website button. Alternatively, it can be activated through a JavaScript API call.

reCAPTCHA Enterprise is developed over the existing reCAPTCH API and follows advanced techniques to analyze and determine whether the user is human. On the other hand, reCAPTCHA v3 calculates a score for every request the user makes.

In that research, they seek to extract parameters that are extracted from the movement of the user's mouse and can be used to determine a percentage of the user's humanness. The extracted percentage can be used in reCAPTCHA as a criterion for choosing CAPTCHA and its difficulty.

1.8 The summary of chapter one

Chapter 1 of the dissertation provides an overview of the rapidly advancing web technology and its integration into various aspects of human life. While the internet brings numerous benefits, security remains a significant challenge. The chapter introduces the CIA triad (Confidentiality, Integrity, and Availability) as fundamental aspects of web security. Security compromises can lead to irreparable damages, affecting users and service providers. Denial of Service attacks, especially through automated bots, poses a serious threat. The chapter highlights the role of CAPTCHA as a security mechanism to distinguish between humans and automated bots. This chapter explored various applications of CAPTCHA, such as protecting online polls, registration forms, and preventing spam. As mentioned, the concept of CAPTCHA is rooted in the Turing test, aiming to create challenges that humans can easily pass but machines find difficult. In this chapter, we introduced the emergence of reCAPTCHA, an advanced form that incorporates scanned book text and the evolution of CAPTCHA into an invisible form. The main objectives of the thesis include comprehensive study of existing human-robot detection methods, CAPTCHAs, to ensure efficiency and security against various types of robots in real-world.

2

Chapter 2

2.1 Introduction

As mentioned in the previous chapter, CAPTCHAs are considered as one of the most widely used ways to identify humans from robots in the Internet and web world and play a key role in preventing denial of service attacks on different servers.

In this chapter, in addition to providing a brief history of CAPTCHA types and introducing each of the proposed solutions based on CAPTCHA until now, the significant features of the existing CAPTCHA will be discussed. While acknowledging the abundant diversity in CAPTCHA variations, our focus lies in systematically addressing well-known and applicable versions for a more comprehensive study. Despite the continual emergence of numerous CAPTCHA techniques proposed by researchers, it is noteworthy that not all innovations find immediate integration into real-world applications. Therefore, our efforts are dedicated to studying and reviewing those techniques that have proven to be robust, reliable, and applicable in practical setting.

2.2 History Of CAPTCHA Evolution

The history of CAPTCHA is an evolution that mirrors the ongoing battle between advancing technology and the need for online security. CAPTCHAs emerged in the late 20th century as a response to the rise of automated bots, which were exploiting online platforms for various malicious purposes. The concept of CAPTCHA was introduced in 1997 by computer scientists Manuel Blum and Luis von Ahn. The idea was to create a test that humans could easily pass, but machines would struggle with. The first CAPTCHAs consisted of distorted text characters that users had to decipher and input, effectively proving their human identity. This simple yet effective method prevented automated bots from accessing sensitive areas like online forms and comments sections. However, as bots became more sophisticated, they began to find ways to bypass text-based CAPTCHAs. This prompted the development of more complex variations, such as image-based CAPTCHAs, where users were required to identify objects within images. Audio CAPTCHAs were introduced to ensure accessibility for visually impaired users, requiring them to transcribe spoken characters from audio challenges.

2.3 CAPTCHA Classes

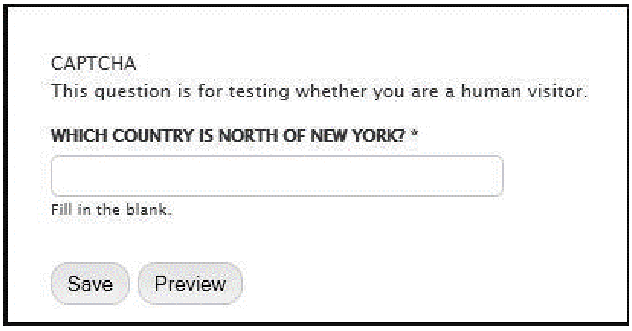
In this section we will give a detailed overview of the different CAPTCHA types, the main types and their variants which are the illustrated in the following sections:

2.4 CAPTCHA based on question and answer

In this type of CAPTCHA, a question is asked from the user and the user must enter the answer in the relevant text field to confirm his real identity system. A remarkable point in this category of CAPTCHAs is the type of question that is raised. The question asked should not be so easy that the robot is able to find the desired answer and pass the CAPTCHA barrier.

Also, the question should not be so complicated that real users are not able to answer. For example, in Figure (2.1) it is asked that "WHICH COUNTRY IS NORTH OF NEW YORK?" and the user should write the answer in the text field and send the form. If the answer matches the desired answer, the requester is recognized as human and approved for further procedures.

If the question asked is the same for all users, the robot can send the same request to the web server many times after manual adjustment and cause many problems. Therefore, it is necessary to have a large data set of questions in order



CAPTCHA

This question is for testing whether you are a human visitor.

WHICH COUNTRY IS NORTH OF NEW YORK? *

Fill in the blank.

Figure 2.1: An example of a question and answer CAPTCHA

to be able to ask a different question to each user [17].

Another problem with this type of CAPTCHA is the wide range of possible answers, which complicates the CAPTCHA verification process. In order to solve this problem, the solution of limiting the answers to predetermined options was suggested. Whenever the user needs a logical question, he can send a request to the CAPTCHA server. The server returns an XML response that contains a random question and answer. In order to prevent annoying users (robots), the answers are hashed using the MD5 encryption algorithm and allows the site server to hash the user's answer without knowing the answer and compare it with the original hash.

2.5 Text-Based CAPTCHAs

Text-based CAPTCHAs involve displaying distorted text that is easy for humans to recognize but difficult for bots and automated programs. They leverage differences between human and machine text processing abilities.

The most common form is Gimpy CAPTCHAs, which overlay randomly generated letters and numbers over a noisy colorful background [18]. The text is distorted through a variety of techniques including varying fonts, sizes, colors, orientations, overlapping characters, introducing arcs/lines, and more. This makes it hard for optical character recognition (OCR) algorithms to reliably segment and recognize each character. Simple segmentation techniques like projecting profiles or contours fail on such CAPTCHAs Figure(2.2). Humans utilize contextual clues and pattern recognition skills to identify obscured or overlapping characters.

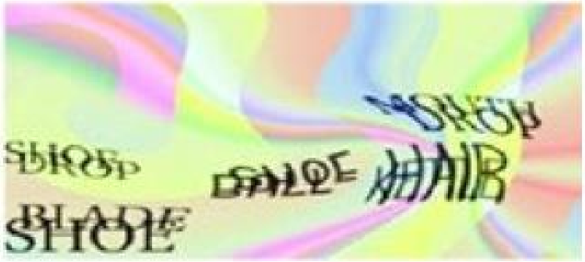


Figure 2.2: Gimpy CAPTCHA

EZ Gimpy CAPTCHAs are a simplified variant with clearly printed fonts and reduced overlaps and distortions. While easy for humans, EZ Gimpy's variable fonts and cluttered background still pose challenges for automated OCR attack tools Figure 2.3.

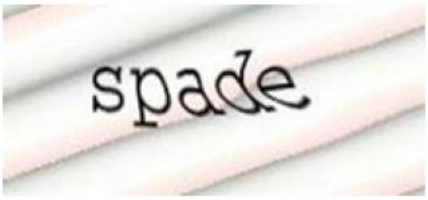


Figure 2.3: EZ Gimpy CAPTCHA

Baffle Text CAPTCHAs Figure (2.4) overlay visual noise and masks on random parts of displayed text - around 30-40% of characters are obscured. Humans can intuit and fill in the missing letters based on the surrounding visible letters and drawing on lexical knowledge. But bots cannot reconstruct masked text without wider contextual understanding.

In Scatter CAPTCHAs Figure (2.5) individual characters are broken into pixel fragments and scattered randomly across the image area. Humans can mentally reassemble and recognize characters from their constituent fragments.

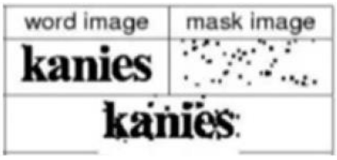


Figure 2.4: Baffle CAPTCHA

But machines cannot meaningfully reconnect the scattered pieces belonging to each character.

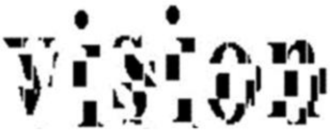


Figure 2.5: Scatter CAPTCHA

Creating secure and usable text CAPTCHAs requires carefully balancing distortion levels. Excessive noise risks making it unsolvable for humans, while too little allows bots to break the tests. Domain expertise in visual perception, cognitive psychology, and machine learning is needed to design robust text CAPTCHAs that remain ahead of adversary capabilities.

2.6 Image-Based CAPTCHAs

Image-based CAPTCHAs rely on visual imagery rather than text distortions to differentiate humans. They test user's ability to recognize images, identify objects, parse scenes, and perform other visual cognitive tasks that are easy for humans but difficult to automate.

In click-based CAPTCHAs, users are shown an image and asked to click on specific parts of the image mentioned in accompanying hint text. For example, the hint may say "Click on the dog's tail" on an image containing a dog Figure (2.6). This targets human visual parsing and comprehension skills [19].

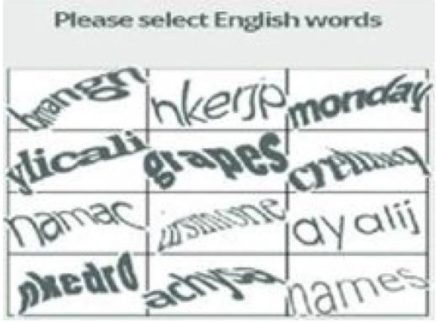


Figure 2.6: Click-based CAPTCHAs

Drag-based CAPTCHAs display icons that users need to drag from initial positions to target locations on the image grid. The trajectories and speed of dragging are analyzed to distinguish natural human mouse movements.

Bongo CAPTCHAs display two similar image blocks with some minor difference introduced in one of them. The user has to identify the altered image Figure (2.7). This difference detection leverages innate human perception skills [20].

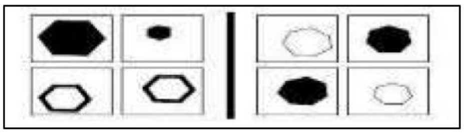


Figure 2.7: Bongo CAPTCHAs

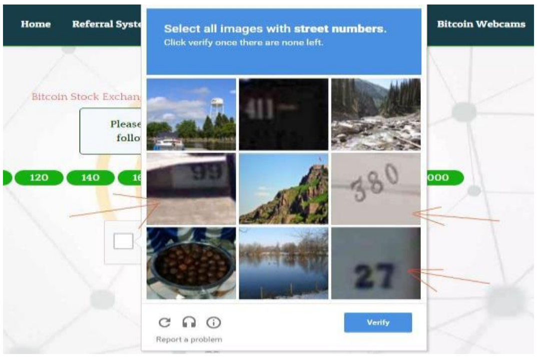
Pix CAPTCHAs show four random sample images belonging to a specific category like flowers, birds, trees, etc. The user enters the category name linking the images. It targets higher level human abilities of semantic classification and knowledge generalization [20].

Drawing CAPTCHAs display randomized dots which users have to connect by dragging their mouse to draw a specified shape or pattern. The generated drawing provides signals to classify whether it was produced by a human [21]. According to the studies conducted on this CAPTCHA, it has been determined that the accuracy of this CAPTCHA is around 96%-98% [22]. The technology used in these CAPTCHAs is similar to the technology used in the old Google

CAPTCHA, in which questions are asked from the user based on the displayed photos. If the user chooses the correct answer, he will be able to send the request.

The technology used in these CAPTCHAs is similar to the technology used in the old Google CAPTCHA, in which questions are asked from the user based on the displayed photos. If the user chooses the correct answer, he will be able to send the request.

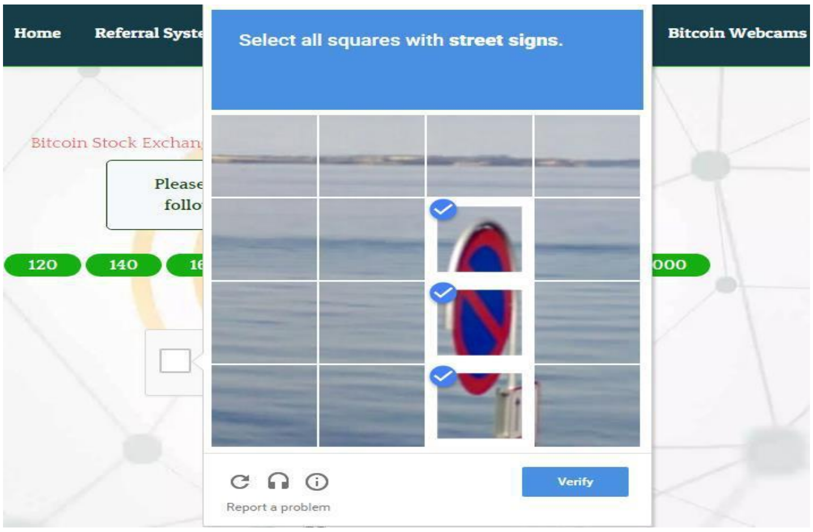
In Selection-based CAPTCHA type, tabular images are shown as in Figure (2.8) and the user is asked to click on some of the houses in the table during a question [23]. For example, in this form, the user is asked to click on the requested numbers.



Select all images with **street numbers**.
Click verify once there are none left.

Figure 2.8: A CAPTCHA for selecting images

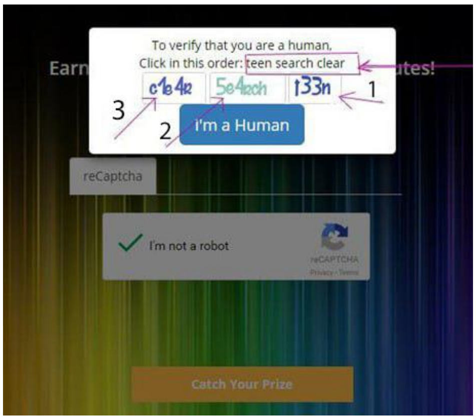
Or in Figure(2.9) users are asked to confirm their identity by clicking on the pictures containing the guide board.



Select all squares with **street signs**.

Figure 2.9: A CAPTCHA for selecting images

In another type of Selection-based CAPTCHA, as in Figure (2.10), several words are given and the user is asked to find them respectively among similar options using his intelligence to prove that he is a human and not a robot [**22**, **23**, **24**].



To verify that you are a human,
Click in this order: teen search clear

Figure 2.10: A CAPTCHA, based on choosing the correct order

A major challenge in designing robust image CAPTCHAs is creating diverse, high-quality image datasets. The larger and more real-world the training data, the better machine learning models become at developing automated attacks. CAPTCHA creators have to constantly expand databases and increase image difficulty to stay ahead of evolving AI capabilities.

Unlike text, image challenges cannot reuse assets as their security depends on novelty. So substantial ongoing effort is needed to rapidly generate fresh image CAPTCHA content. 3D graphics and simulations can help create large synthetic image datasets cheaply.

The choice of image categories also matters - everyday objects and scenes are more intuitive for humans than abstract shapes. Natural images with ambiguity and variability also resist automated reasoning better. Overall, image CAPTCHAs provide an alternative aesthetic and user experience to text while leveraging complementary human skills.

2.7 Game-Based CAPTCHAs:

Game CAPTCHAs incorporate interactive computational game environments which users have to successfully play through to prove their humanness. This builds upon the puzzle approach by testing skills like strategic thinking and hand-eye motor coordination in dynamic game contexts.

For example, one method generates platform game levels with moving obstacles, enemies and stairs which users have to navigate by controlling a character. Solving the game requires human abilities like planning sequences of jumps, real-time reactions, spatial memory, and learned gaming conventions [25].

Another scheme simulates a 2D physics environment with balls, ramps, obstacles where users have to visually estimate required velocities and angles to strike targets. This leverages human intuitive physics skills which are needed to succeed at the game challenge.

Such CAPTCHAs are usually not used in large sites with serious topics. Figure (2.11) shows an example of a fun CAPTCHA with a game theme. Also, in Figure (2.12) an example of an entertaining CAPTCHA with the topic of advertising is shown.

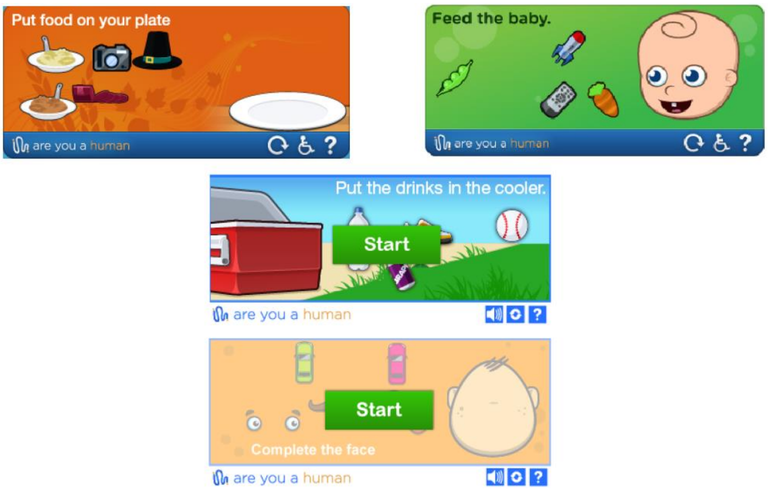


Figure 2.11: A fun CAPTCHA with a game theme

Unlike standard gameplay, game CAPTCHAs randomize and diversify scenarios to prevent easy pattern recognition. Sufficient gameplay data is analyzed to reliably assess if a human is controlling decisions. Short levels focusing on specific skills help minimize time commitment. However, games require exact mental modeling of their physics and constraints. Overly convoluted or unpredictable games may fail the task of separating humans and bots if neither can reasonably succeed. Long completion times also impact usability.

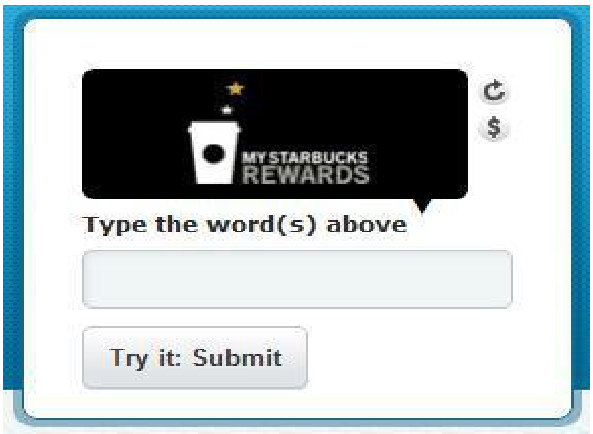


Figure 2.12: An entertaining CAPTCHA on advertising

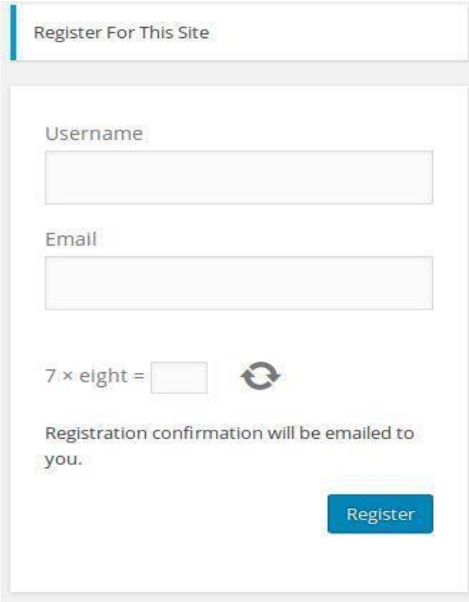
2.7.1 Puzzle-Based CAPTCHAs:

Unlike other CAPTCHAs relying on recognition, puzzle CAPTCHAs test a user's ability to actively solve a cognitive game or challenge. This taps into human problem-solving skills and intuitive reasoning which is difficult for machines.

For example, one method displays an incomplete mathematical expression and asks the user to enter the result, leveraging human arithmetic skills. In this type of CAPTCHA, the user must answer a mathematical question. The advantage of this method compared to the previous method is that the answers are limited in the range of numbers. That is, the user can only enter numbers and the answer is a specific number.

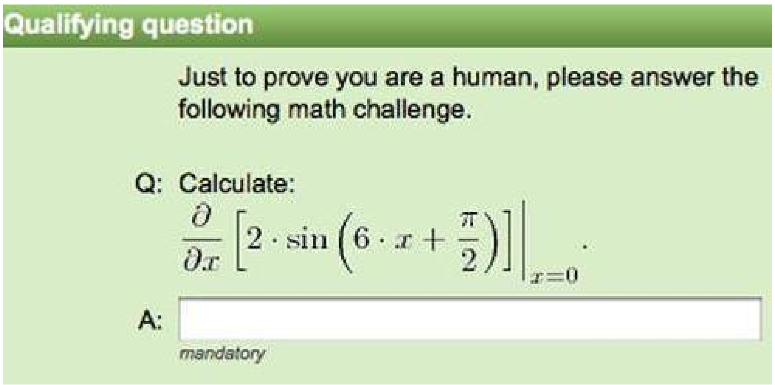
The drawback of this method is that increasing the difficulty percentage of the question depends on the level of mathematical knowledge of the user. In other words, a user who has a low level of mathematical knowledge cannot find the answer to the question, so he will not be able to complete the application process [26].

Figure (2.13) shows a simple example of CAPTCHA based on mathematical logic. But in Figure (2.14), a complex example of mathematical CAPTCHAs is shown. It is clear that such a complex mathematical operation to verify the user's authenticity is not very pleasant for real users and prevents them from continuing.



Registration confirmation will be emailed to you.

Figure 2.13: A simple example of CAPTCHA based on mathematics



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

Q: Calculate:

$$\frac{\partial}{\partial x}\left[2 \cdot \sin\left(6 \cdot x + \frac{\pi}{2}\right)\right]\bigg|_{x=0}.$$

A:

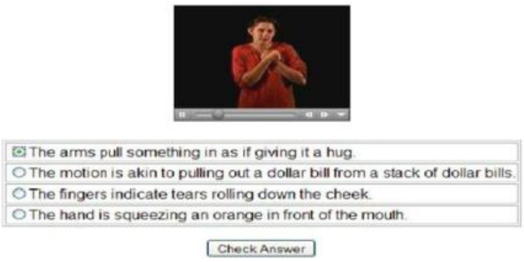
Figure 2.14: A more complicated example of math-based CAPTCHA

However, the open-ended nature of puzzles makes them harder to standardize and grade. Setting an appropriate difficulty level is also challenging - overly complex puzzles will stump legitimate users. There is also potential for usability issues around accessibility. Creative puzzle generation leveraging different aspects of cognition, from language to geometry to general knowledge, is an engaging research area. Puzzles around understanding absurdist humor, intuiting unstated assumptions, or exploring paradoxes appear potentially viable. Adaptively adjusting puzzle difficulty based on user performance could allow better balancing of security and usability.

2.8 Video-Based CAPTCHAs

Video CAPTCHAs rely on users watching a short video clip and then solving a visual comprehension task related to the clip. This aims to leverage the innate human ability to holistically parse and summarize visual dynamics, which remains challenging for machines. There are several forms of video-based CAPTCHA.

In Motion CAPTCHAs form, after watching a randomized video clip, the user has to select the correct text description corresponding to the events and actions depicted in the video from multiple choice options Figure (2.15). This targets the person's capability to accurately comprehend and map visuals to conceptual representations.



● The arms pull something in as if giving it a hug.

○ The motion is akin to pulling out a dollar bill from a stack of dollar bills.

○ The fingers indicate tears rolling down the cheek.

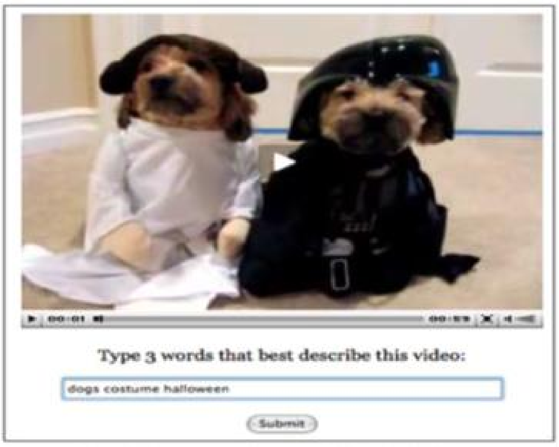
○ The hand is squeezing an orange in front of the mouth.

Figure 2.15: Motion CAPTCHAs

Another variant asks users to watch a short video and then type in three words that best summarize or describe the clip Figure (2.16). The entered words are checked for semantic relevance to the actual video content. This not only requires visual parsing, but also higher-level abstraction of the scene's salient elements.

Compared to images, short video clips can capture more complex appearances, motions, interactions and context. Interpreting these multifaceted visual dynamics and distilling the essence poses increased challenges for automated algorithms. Videos also have greater diversity - animations, simulations, game footage and real-world clips can all be used.

However, relative to text or images, video files have much larger data bandwidth requirements. Generating and storing large video databases can be expensive. Serving high-quality video also poses bandwidth costs for deployment. These constraints have limited widespread adoption of video CAPTCHAs thus far. Recent progress in computer vision, video analysis and scene understand-



Type 3 words that best describe this video:

dogs costume halloween

Figure 2.16: Described motion

ing powered by deep neural networks is rapidly improving machine capabilities. But human cognition still outperforms algorithms, especially on subjective qualities like expressing clip themes in few words.

As with other CAPTCHAs, the goal is a difficult but not impossible test. If the visual task is too confusing or abstract, humans will not be able to reasonably complete it either. Striking this balance along with engineering optimizations for serving video at scale remain key challenges. If these can be addressed, video CAPTCHAs provide an interactive and engaging alternative to static images. They open the door to cheaper crowdsourced annotation of massive video datasets as well. Overall, they demonstrate potentials of leveraging human visual intelligence in entirely new ways going forward.

2.9 Audio-Based CAPTCHAs

Audio-based CAPTCHAs rely on voice, speech and sound instead of visuals. They are designed to test a user's ability to interpret garbled audio clips that are easy for humans to recognize but difficult for machines.

In the listen and speak approach, random digits or characters are generated using text-to-speech synthesis. Various forms of background noise such as beeps, static, echoes etc. are then added to garble the audio. Users have to listen to these distorted audio samples and speak back the text they hear. Speech recognition is used to check if their input matches the original sample [27].

The listen and write method similarly adds heavy background noise to spoken text of random numbers/letters. But here the user has to manually type in the text heard in the garbled audio clip. This directly tests a person's capability to extract meaningful information from severely obfuscated audio [28].

Audio CAPTCHAs capitalize on the human auditory system's ability to focus on relevant sounds and filter out noise. Even faint speech buried under loud distortions can be recovered by the human brain. But for machines, separating the original speech from background noise without any context is an extremely challenging task.

Some key advantages of audio CAPTCHAs are accessibility for visually impaired users, and resistance to automated optical character recognition techniques. But human speech and hearing capabilities vary substantially across users. Also, audio poses language dependencies - native speakers will perform better at comprehending heavily accented speech. Designing the audio distortion and noise is a delicate balancing act. Excessive garbling risks making it uninterpretable even for humans. But minor effects may allow machines to clean up and recognize the spoken text. Selection of speaker voice, speaking pace, background sounds, and mixing process all affect difficulty.

With recent advances in deep learning for noise cancellation and speech analysis, machine capabilities on audio processing tasks are fast evolving. So audio CAPTCHAs require constant assessment and tweaking to provide robust security. But designed well, they provide a hands-free and language-agnostic alternative to conventional visual CAPTCHAs.

2.10 Social network based CAPTCHAs

In social networks or websites related to social networks, a type of CAPTCHA is used, in which questions are asked using the information stored in the user's account. In other words, the reference for CAPTCHA questions or identity verification is the stored information of the user or even his friends list. Facebook is one of the famous social networks that uses this type of CAPTCHA. In this process, the user is shown the photo of several users and asked, "Which one is your friend?" If the selected user is among the person's friends list, the process has been successfully completed [29].

2.11 Cognitive/Biometric-based CAPTCHAs

Traditional CAPTCHAs using distorted text and images are being replaced by more advanced CAPTCHAs that leverage human cognitive abilities and physical interactions. Cognitive CAPTCHAs target specific mental skills like knowledge, memory, problem solving, spatial reasoning etc. Biometric factors (fingerprint, face), device gestures (tilt, rotate), knowledge questions are also being incorporated. Biometrics has been one of the popular and famous options in the process of authenticating users in real and virtual environments. It is also possible to use this option to distinguish humans from robots. For example, to buy equipment or services, biometric parameters can be used to confirm that the user is not a robot [**30**]. Biometric CAPTCHAs use unique human biometric characteristics, such as fingerprint or facial recognition, to verify user identity [**31**].

2.11.1 Face Recognition CAPTCHAs

Face recognition CAPTCHAs leverage facial recognition technology to ascertain whether a user is human or a bot, serving as a barrier against automated spam and misuse. They compel users to discern and match human faces within a set of images [**31**]. Figure (2.17) shows an example of Face recognition CAPTCHAs. Various technologies are at the disposal of face recognition CAPTCHAs, including:

- Computer vision algorithms: These algorithms employ machine learning techniques to scrutinize facial attributes and identify faces. Training them on extensive human face datasets enhances their accuracy.
- Facial landmarks detection: This method entails pinpointing key facial features like eye corners, nose, and mouth to authenticate users. Combining it with other techniques, such as machine learning, improves accuracy.
- Live detection: Users are prompted to perform specific actions like blinking or smiling to affirm their human status.

Facial landmarks detection technology is frequently harnessed in face recognition systems, as it capitalizes on the unique nature of each individual's facial landmarks for identification. Compared to more general computer vision algorithms, it can be effectively paired with live detection to yield more precise and dependable outcomes. By focusing on crucial facial features rather than analyzing the entire image, it achieves greater accuracy.

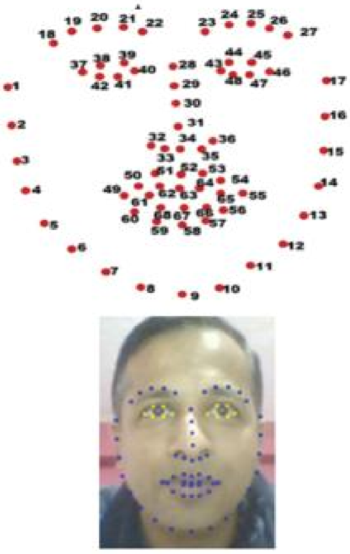


Figure 2.17: Face recognition CAPTCHAs

For instance, among the 68 facial landmarks, points 36 to 48 are employed for eye prediction, enabling the determination of whether human eyes are open or closed. This approach foils bot attempts to utilize still images or photographs to masquerade as human users and thwarts human relay attacks.

Employing computer vision algorithms, facial landmark detection, and live detection in face recognition CAPTCHAs proves to be highly effective in thwarting automated spam and misuse with the usage of B3DA algorithm.

2.11.2 Gestural CAPTCHA

Gestural CAPTCHA, referred to as GAPTCHA henceforth, presents users with a series of simple hand gestures and requests them to replicate these gestures in front of their camera. The core of this approach revolves around the recognition of these gestures, achieved through the computation of finger bend angles [**32**].

The method initiates by preprocessing and applying a skin filter to the 2D input image. An effective segmentation technique is employed to isolate the hand pose even in scenarios where the background features skin-colored objects. This segmentation approach concentrates exclusively on the areas of interest within the image, leading to swifter and more precise analysis.

Initially, the method identifies the fingertips and palm within the segmented image. Subsequently, it computes the distances between the palm's center and each fingertip. The bending angles of the fingers are determined based on these distances, allowing for the accurate detection of fingers, palm, and their corresponding angles without any errors.

2.11.3 BeCAPTCHA-Mouse

In 2020, Acien and colleagues [33] introduced BeCAPTCHA-Mouse, a system designed to discern humans from bots by scrutinizing mouse trajectories during the challenge. Similarly, Gametrics [34] distinguishes between humans and bots by capturing and analyzing the users' mouse movements during drag-and-drop operations within the context of solving a Dynamic Cognitive Game. Additionally, GEETest and Netease utilize similar techniques for user verification.

2.11.4 EYE-CAPTCHA

EYE-CAPTCHA is a unique CAPTCHA system. Unlike traditional methods, EYE-CAPTCHA requires users to solve math-based challenges using their eye movements. To succeed, users must identify the correct answer and navigate it to the center of the screen solely with their eyes, leveraging eye-tracking technology for verification. This approach represents a departure from text-based or image-centric CAPTCHAs, emphasizing users' eye control as a novel means of authentication. EYE-CAPTCHA has the potential to enhance digital security and accessibility by introducing innovative eye-based verification methods [35].

2.11.5 Sensor CAPTCHA

Users are tasked with executing intricate gestures using their mobile devices, such as actions like fishing, hammering, or drinking. Additionally, the authors introduced Pedometric CAPTCHA, a system that necessitates human users to take a minimum of five steps. As the user walks, the mobile device registers acceleration, thereby creating a challenge that is challenging for automated bots to overcome [36].

2.12 Popular Invisible CAPTCHAs

Invisible CAPTCHAs are all techniques that leverage micro-movements of a smartphone to transparently distinguish humans from bots. When a user taps the touchscreen, small accelerations perpendicular to the screen are generated as the finger makes contact. Though imperceptible to the user, these micro-motions can be measured using the accelerometer embedded in a phone's secure element. Unlike previous CAPTCHA methods that explicitly challenge users to tilt their device to a specific angle, Invisible CAPTCHA passively monitors tap micro-movements in the background without any added user burden. When a user submits data through a mobile browser or app, the secure element analyzes the tap acceleration patterns. If human-like micro-motions are detected, the input is authenticated as originating from a real user. Otherwise, it is flagged as potentially malicious automated input.

The rationale is that malware cannot physically move a device to replicate natural human tap motions and rhythms. To prove this, experiments demonstrated the reliability of classifying tap patterns as well as the inability of malware to simulate such micro-movements even using smartphone actuators like vibration motors. By leveraging tamper-resistant security hardware already present in many modern SIM cards, Invisible CAPTCHA achieves completely transparent bot discrimination without sending sensitive sensor data off-device. This avoids usability issues and privacy risks seen in some active CAPTCHA schemes.

Guerar et al (2016) presented BrightPass, an authentication mechanism that uses screen brightness as a communication channel to improve security in mobile social network access inaccessible to mobile malware. For each authentication attempt, BrightPass displays an alternating circular flash on the phone's screen to tell the user when to enter the correct PIN digit and when to enter a fake one. In this way, it prevents malware from successfully broadcasting the user's PIN, thereby preventing the possibility of unwanted access and/or taking certain actions without the user's knowledge. It also ensures short authentication time (i.e. 6.73 seconds) and low error rate (i.e. 1.81%). However, all these solutions require a specific additional activity to be performed by the user[**37**].

Conti et al (2011), presented a transparent method that uses the data measured by the accelerometer and the orientation sensor during call/answer as a biometric measure to authenticate the user and thus prevent unauthorized users from doing this.

Buriro et al (2017) proposed a motion-based touch typing biometric method to improve the security of an 8-digit PIN/password used for mobile banking applications. Their method is based on timing differences in keystrokes and phone movements during the PIN/password entry process measured from various 3D sensors (e.g., accelerometer, orientation, gravity sensor, magnetic) thereby authenticating the authorized user [**30**].

De Luca et al introduced a transparent authentication method to enhance the security of Android pattern lock. When performing a wipe gesture to draw a pattern, some biometric features including XY coordinates pressure, size, time and speed of touch are collected to validate the entered pattern Figure (2.18). Therefore, the smartphone will be unlocked only if the user draws the correct pattern and the way it is drawn matches the stored features [**38**].

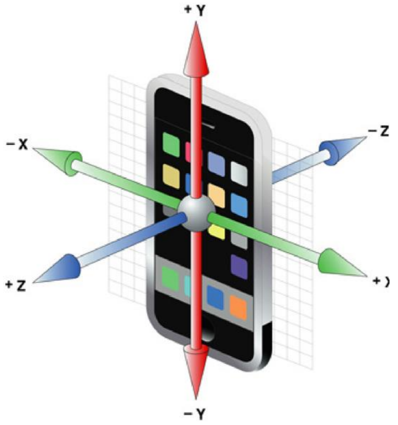


Figure 2.18: Design of accelerometer axes (2016)

Impact detection by accelerometer is not new and many researchers have proposed algorithms for impact detection for different purposes. Meanwhile Davarchi et al. suggested using accelerometer data to detect the impact and also determine whether it belongs to a child or an adult [**17**].

The vibration motor in any smartphone can be exploited by malicious programs to create a micro-device movement in an automation. Therefore, the difference between the micro-movement caused by real shocks and the movements caused by vibration should be shown. For this reason, a comparison has been made between accelerometer data collected during user impact and vibration from different smartphones, such as HTC DESIRE, GALAXY S ADVANCE, LG G4, OPPO F1 and ONEPLUS 5T. These devices represent a significant time span, as they are commercial smartphones marketed in 2010, 2012, 2015, 2016, and 2017, respectively 2018.

In order to implement invisible reCAPTCHA, an embedded secure element with a motion sensor such as SIMSense is required to ensure the security of sensed data, while an integrated hit detection algorithm analyzes this data to distinguish between humans and malware. Because the SIMsense secure element is available as a SIM card, it can be used inside any mobile device without the need for hardware modifications. In addition, communication between web/cloud applications and the secure element is done through a defined web API.

2.13 The summary of chapter Two

Chapter two of the document provides a comprehensive overview of the evolution of CAPTCHAs. It begins by emphasizing the role of CAPTCHAs in distinguishing humans from robots and preventing denial of service attacks on servers. The chapter delves into the history of CAPTCHA evolution, starting with its inception in 1997 by computer scientists Manuel Blum and Luis von Ahn.

The text explores various CAPTCHA classes, including question and answer-based CAPTCHAs, text-based CAPTCHAs (such as Gimpy, EZ Gimpy, Baffle, and Scatter), image-based CAPTCHAs (Click-based, Drag-based, Bongo, Pix, Drawing, Easy CAPTCHA, and Selection-based), puzzle-based CAPTCHAs, game-based CAPTCHAs, video-based CAPTCHAs, audio-based CAPTCHAs, social network-based CAPTCHAs, cognitive/biometric-based CAPTCHAs, face recognition CAPTCHAs, gestural CAPTCHAs, BeCAPTCHA-Mouse, EYE-CAPTCHA, and sensor CAPTCHA.

Furthermore, the document introduces the concept of "Invisible CAPTCHAs" which leverage micro-movements of smartphones to distinguish humans from bots without imposing explicit challenges on users. It discusses various forms of Invisible CAPTCHAs, including those based on tap micro-movements, screen brightness, accelerometer and orientation sensor data, and other biometric measures.

The text touches on the continuous challenge of developing CAPTCHAs that remain effective against evolving AI capabilities and concludes with a discussion on the role of AI in breaking CAPTCHAs and the need for innovative solutions to counter these AI-based threats.

3

Chapter 3

3.1 Introduction

It should be noted that artificial intelligence is the opposite of CAPTCHA; in other words, CAPTCHA tries to prevent artificial intelligence from running in different systems so that only humans can use the system. But with the progress of artificial intelligence, a solution has been found to bypass each CAPTCHA.

For example, for text CAPTCHA, CNN algorithm is used to convert image text to input text. Later, the researchers invented a system called RCN, according to which the text CAPTCHA image is converted into the input text with a high percentage of accuracy.

This method is quite different from other artificial intelligence methods that use CNN algorithm. Researchers have come to the conclusion that RCN is better than CNN because it needs less learning. The proof of this is that a system based on RCN only needs 5 image samples to convert each letter from image to text with an accuracy of 66.6% for learning, while the advanced CNN example usually needs over 50,000 similar images similar to CAPTCHA images for training the model in order to convert the CAPTCHA image into text with an acceptable percentage of accuracy [**39**].

Different methods have been proposed to break different CAPTCHAs, each of which can make that CAPTCHA ineffective. The question that arises is how to tackle with these methods and what is the new CAPTCHA solution?

3.2 reCAPTCHA, a powerful variation of CAPTCHA

According to research, the statistics of the number of times that all Internet users answer CAPTCHA questions is something around 200 million times a day which according to the high number, time equivalent to 150,000 working hours per day is wasted answering CAPTCHA questions. But what is the method to prevent the wasting of a part of Internet users' time that can be efficiently used?

This was the question that Google raised after examining the statistics of the time taken from users and tried to provide a new method to solve this problem, which after some time presented very creative and useful ideas called reCAPTCHA .Figure (3.1) shows an example of reCAPTCHA in the Google account login form.

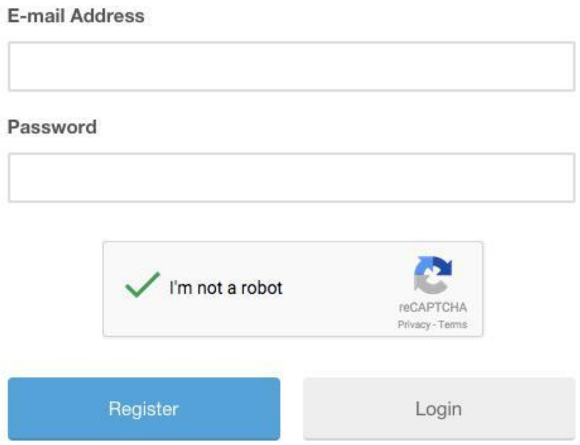


Figure 3.1: Use of reCAPTCHA in the user login form

3.3 How does reCAPTCHA work

There are many methods for creating digital copies of books or newspapers that have been printed and are not digital, the most widely used being OCR which is a computer scanning method that scans the pages of newspapers and printed books.

Then it converts the scanned image into text. An interesting point is that the conversion of image to text significantly reduces the size of a digital book for storage, and as a result, its download speed increases, but the problem in the OCR method is that some words are found in books and newspapers whose ink has spread and after scanning and turning into a photo, OCR is not able to read and recognize them in order to convert the photo into digital text (Figure (3.2)) .

reCAPTCHA is a creative idea which has solved the problem of using OCR. The words that are not recognized by OCR are given to reCAPTCHA and reCAPTCHA sends these words as CAPTCHA when the user is asked to recognize the word and enter it in the box. Then, the words that could not be recognized by OCR are recognized by the user and sent to OCR. In fact, reCAPTCHA carries two things in one fell swoop: first, it reduces to some extent the time spent by Internet users to answer CAPTCHA questions, and of course, it makes useful and beneficial use of the time users spend answering so that the process of creating digital books and newspapers by converting photos to text in the OCR system proceeds without any problems and even faster [39].

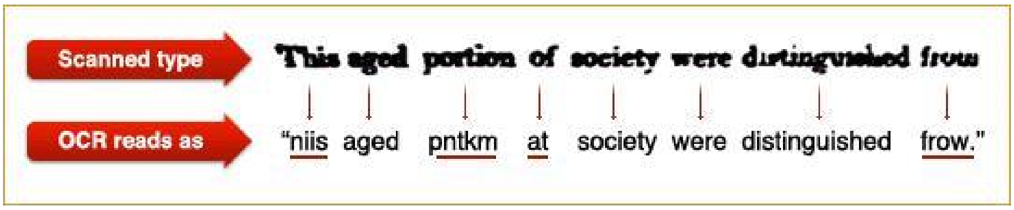

Scanned type
This aged portion of society were distinguished from
OCR reads as
"niis aged pntkm at society were distinguished frow."

Figure 3.2: OCR system's inability to recognize words

3.4 Comparison between CAPTCHA and reCAPTCHA

One of the main methods used to create and access digital version of documents is by scanning the book pages and character recognition, or OCR. The main problem arises when the accuracy of OCR systems is not perfect, and as shown in Figure (3.2), it will always be accompanied by errors in character recognition. reCAPTCHA has shown its efficiency at this stage and has proven to be instrumental.

reCAPTCHA simplifies the process of creating digital copies and sends words as CAPTCHAs to Internet users. In this method, only the words that cannot be recognized by the OCR system are sent to the users which generally include things such as printing ink spread or folds in the pages.

The main question is if the computer is not able to recognize these images how it can ensure the correctness of the information entered by the user for a reCAPTCHA. To solve this problem, every word that is sent from the OCR system is shown to the user along with other words that are generated by the reCAPTCHA system and the correct answer is known.

If the first word is answered correctly, the chances of the second word sent through OCR being correct will also be very high.

For the final confirmation of reCAPTCHA answers, each word is sent to several different users, so that if the answers are the same, they will be sent to the OCR system as the main answer [**32**]. As a result, if the user gives a correct answer to the first word and a wrong answer to the second word in a reCAPTCHA question, he will still have access to the next stage of registration, because only the first word is used as a criterion to distinguish humans from robots, and the second word is used as cooperation in a free and international project.

3.5 The structure of reCAPTCHA

Several parameters are studied and used in the reCAPTCHA structure such as the number of incorrect CAPTCHA entries, the IP of the user who sends a request to the system, the time the user is active in the system, the time a request is made, and many others. Here, as an example, a brief explanation about the IP parameter is given. IP address actually an abbreviation of Internet Protocol address or Internet protocol addresses (worldwide network) is a series of numbers with a rule, to any device (including computer, mobile phone, printer, etc.) assigned to connect to the web network, IP is actually a unique identification number for a network connection with which different computers (or different servers) in the wide web network in this way, the user's geographic location, network connection information, etc. can be identified and tracked. Of course, it should be noted that most home users use the IP assigned by their ISP or Internet service provider so their IP is a number assigned by the

Internet service provider which usually has a certain number and series of IPs for connection so IP may change every time the user is connected to the Internet however, the country, name and location of the service provider will be the same as the ISP because one of the channels and connection numbers of that company is used.

Each user of the system has his own IP ID so it is possible to determine how many requests each IP sends to the system in a certain period of time (for example, one minute). According to the studies conducted on human behavior when visiting a website, usually people spend some time reading the content of the page and then send another request to the server. Therefore, the lower the number of requests for each IP at a certain time, the higher the probability that the agent is human. On the other hand, it has been proven that humans usually do not follow a specific rule in sending requests but robots usually send a regular and predetermined number of requests to the server per unit of time. Therefore, by examining the process of sending site user requests, a solution can be found to determine whether the user is human.

In order to reach more users and use free human resources on the Internet reCAPTCHA needs the cooperation of webmasters. This project, which is currently managed by Google has provided facilities for installing the reCAPTCHA system for free on Internet sites.

If the user owns a site and has a problem with spammers, he can fight against spammers on his site and participate in this project by putting a reCAPTCHA on the site. Google has released free plugins for widely used content management systems such as WordPress so that people without the need for coding knowledge can use reCAPTCHA.

3.5.1 Invisible reCAPTCHA

reCAPTCHA v3 is a newer version of reCAPTCHA developed by Google that uses machine learning to analyze the user's behavior on the website to determine if the user is a human or a bot. reCAPTCHA v3 is invisible to users, so it does not interrupt the user experience. Google has not disclosed the details on how exactly the algorithm works.

In [**40**], an examination of Google reCAPTCHA systems' accessibility is conducted to gauge their efficacy in providing secure yet user-friendly website interactions. The investigation likely scrutinizes various iterations of reCAPTCHA, including the classic checkbox confirming the user is not a robot, tasks involving identifying images, and the more modern, unobtrusive reCAPTCHA. Elements such as the duration required to solve the CAPTCHA, the system's precision in differentiating between human users and automated bots, and the end-user experience may be evaluated. The inclusivity of these systems for individuals with disabilities, determining how well reCAPTCHA caters to those with visual, hearing, or motor challenges, may also be a focal point of the study. The objective of the research is to comprehend how Google's reCAPTCHA strikes a harmony between ensuring security and offering accessibility.

TAPCHA [**41**] is a groundbreaking CAPTCHA system specifically designed for touch-enabled devices. It acknowledges and addresses the challenges that traditional text-based CAPTCHAs present on mobile interfaces, often leading to user frustration. Capitalizing on context effects, TAPCHA has been engineered to be "invisible" to automated bots while remaining intuitive and user-friendly for human users. The system introduces several design variations to cater to different user preferences and device capabilities. One notable method is the "Shape & Shade" approach, where users are prompted to move specific objects on the screen based on detailed shape and shade instructions. Another intriguing version is the "Multi" design, which incorporates challenges that require users to swipe in specific patterns or directions. These innovative interaction methods not only aim to offer a seamless and engaging user experience but also ensure robust security measures against increasingly sophisticated automated bot attacks.

In [**42**], it is proposed a reCAPTCHA solver that leverages a custom deep learning solution using YOLOv3 object-detection and Google's Cloud Vision API. YOLOv3 is an efficient CNN-based object-detection method, while Google's Cloud Vision provides a pre-trained model accessible via a REST API. ReCAPTCHA v2 presents image challenges where users must identify images containing a given clue, which could be text or an image. The challenges can be categorized into three types:

- Type 1 (3x3): Users are presented with a 3x3 grid of distinct images. After selecting a correct image, it may be replaced by a new one. About twelve possible clues are used for this type.
- Type 2 (4x4): Users see a single image divided into a 4x4 grid. The same clue set as Type 1 is used, but no new images are added after a selection.
- Type 3 (4x2): Users get a 4x2 grid of distinct images with a unique set of

clues. Like Type 1, new images might replace selected ones.

Types 1 and 3 can have static images or new images replacing old ones. After completing a challenge, users may receive additional challenges based on reCAPTCHA's risk assessment. Riskier users may face more challenges and noisier images. Most users are verified after 1 or 2 challenges.

The proposed solution in [42] aims to solve reCAPTCHA's image challenges by combining human-like mouse movements and deep learning object-detection. The process is as follows:

Human-Like Mouse Movements: The mouse is moved along a Bezier curve with randomly selected points on the web page to mimic human behavior. This is done to receive a better risk analysis score from reCAPTCHA, resulting in image challenges with less noise.

Image Challenge: The text clue from the image challenge is extracted. The set of images presented in the challenge is screenshotted, cropped, and spliced as needed.

For type 1 and type 3 challenges, the 9 and 8 distinct images respectively are processed by the object-detection method according to the clue. Images containing the clue label are selected in reCAPTCHA. If new images are added after a selection, the process continues until no new images contain the clue label.

For type 2 challenges, the original image is reconstructed by removing gridlines, sent through the object-detector, and then split back into 4 by 4 sections. Sections containing the clue label are selected.

Object-Detection: Two custom YOLOv3 models are created using different training sets: one from ImageNet and additional Google image searches, and the other from images taken directly from Google reCAPTCHA v2 challenges. Each dataset uses 300 images for training and 200 for testing. Transfer learning is used with pre-trained weights from a YOLOv3 model trained on Google's Open Images dataset.

After submitting a challenge, the solution waits to see if reCAPTCHA verifies or sends another challenge. If not verified, the process is repeated until verification is received.

3.6 Weaknesses and problems of CAPTCHA

Definitely CAPTCHA is a efficient tool that helps to distinguish between human or robots. But, even though it's useful, it also has some drawbacks.

Sometimes the tests are too hard, and some people can't do them, which can be frustrating. Also, some smart computers can trick CAPTCHA tests, making them less effective. Plus, it costs money to use CAPTCHA on websites, and it might not work well for everyone. There are some key weaknesses of CAPTCHA:

- Usability Challenges: CAPTCHA challenges often involve tasks that can be difficult for some users to complete, especially those with visual impairments, cognitive disabilities, or those using mobile devices. This can result in frustration and exclusion of certain user groups.

- Accessibility Issues: Many CAPTCHAs rely heavily on visual recognition, making them inaccessible to users who are blind or visually impaired. While audio alternatives exist, they may not always provide a clear or effective experience.

- Sophisticated Bots: As bots become more advanced, some can simulate human-like behavior and successfully solve CAPTCHA challenges, undermining the effectiveness of CAPTCHA as a bot-detection mechanism.

- Maintenance and Cost: Implementing and maintaining CAPTCHA systems can be resource-intensive for website operators. It might involve coding changes, updates, and sometimes costs if third-party CAPTCHA services are used.

- Negative User Experience: Complex or confusing CAPTCHA challenges can discourage users from completing tasks on a website. If challenges are too difficult to solve, users might abandon the process, leading to decreased engagement and conversions.

- Privacy Concerns: CAPTCHA solutions provided by third-party services could potentially collect user data, raising privacy and security concerns if data is misused or mishandled.

- Circumvention: Some CAPTCHAs are easier to circumvent than others. If attackers find a vulnerability in the CAPTCHA implementation, they can exploit it to automate bot activity.

- Language and Cultural Barriers: CAPTCHAs that rely on language-specific questions or cultural references might be confusing or irrelevant to users from different linguistic or cultural backgrounds.

- Ineffectiveness for New Threats: CAPTCHAs are designed to combat specific types of bots and attacks. New, innovative bot techniques might evade existing CAPTCHA methods.

- Environmental Concerns: Certain types of CAPTCHAs, like those that require solving resource-intensive puzzles, can contribute to higher energy consumption, potentially impacting the environment.

- Social Engineering: CAPTCHA challenges that require users to perform specific actions could potentially be manipulated by attackers who deceive users into solving them, thereby bypassing the security measure.

3.7 Popular methods to break CAPTCHA

There are three main and popular CAPTCHA solving methods available for attackers to solve the CAPTCHA.

1. OCR (Optical Character Recognition) enabled bots: Optical Character Recognition (OCR) is a technique used to recognize and extract text from images. In this CAPTCHA solving method, automated bots utilize OCR technology to automatically identify and interpret the characters in the CAPTCHA image. Tools like Ocrad and Tesseract are OCR engines that can be employed for this purpose. However, the accuracy of OCR-based CAPTCHA solving can be relatively low, especially when CAPTCHAs are designed to be challenging for OCR engines to decipher.

2. Machine Learning: Machine learning involves training algorithms to perform specific tasks by learning from data. In the context of CAPTCHA solving, machine learning techniques are used to recognize patterns and features in CAPTCHA images. Convolutional Neural Networks (CNNs) are particularly effective in image recognition tasks. Python frameworks and libraries like Keras and TensorFlow provide the tools to develop and train deep CNN models. By training these models on a dataset of CAPTCHA images, the models can learn to identify the letters and digits within the CAPTCHA and subsequently solve them.

3. Online CAPTCHA-solving services: Online CAPTCHA-solving services operate by employing human workers who are available to solve CAPTCHAs in real time. When a user submits a CAPTCHA-solving request, the service forwards the CAPTCHA to these human solvers. The human solvers manually interpret the CAPTCHA and provide the correct solution, which is then sent back to the user. This method relies on human intelligence to solve CAPTCHAs that automated algorithms struggle with. While effective, it may not be as instantaneous as other methods and might involve associated costs [43].

3.8 CAPTCHA and artificial intelligence, concerns and considerations

CAPTCHA is considered a serious obstacle for the attackers to achieve their goals, they must spend a lot of time and energy to break it. The success of the attackers means that the methods adopted by them become more complicated. In other words, it is possible to attack CAPTCHA leveraging artificial intelligence.

As attackers are trying to find new ways to bypass CAPTCHAs, computer network security researchers are also trying to design advanced CAPTCHAs that challenge other fields of artificial intelligence. CAPTCHA failure means a step forward to advance the goals of artificial intelligence. But website managers are not satisfied with this issue because the main harm is towards them. From their point of view, it is still necessary to deal with a big problem such as spammers and hackers. People who run websites or have online polls should be aware that some examples of CAPTCHA system are no longer effective and therefore they should refrain from using it.

Before choosing any CAPTCHA system, a little research should be done on CAPTCHA applications that are still reliable. Of course, keeping information up-to-date about verified or hacked CAPTCHAs is also very important. As soon as the failure of a CAPTCHA system is observed, the manager is obliged to make an appropriate decision about the security method used (such as replacing the CAPTCHA method) in his website .

CAPTCHA designers should move in a clear direction. As computers are progressing and becoming more complex day by day, the methods of testing with CAPTCHA must also evolve. On the other hand, if the CAPTCHA evolves and reaches a point where even a human cannot pass it with a reasonable success rate, the whole system will be considered failed and ineffective.

Maybe the evolution of distorted text is not the final solution. Users can be asked to solve a math equation or answer questions about a short story. While such tests are becoming more complex day by day, there is also a risk of losing the user's interest in continuing the way.

How many users would be willing to write a forum post or post a comment if they were asked to solve a quadratic equation first? On the other hand, it is possible to reach a point where computers and humans understand a puzzle in the same way.

Such an event will cause the loss of the ability to use CAPTCHAs. Until then users just have to open their eyes (or listen carefully) to find the correct CAPTCHA code and enter it in the box.

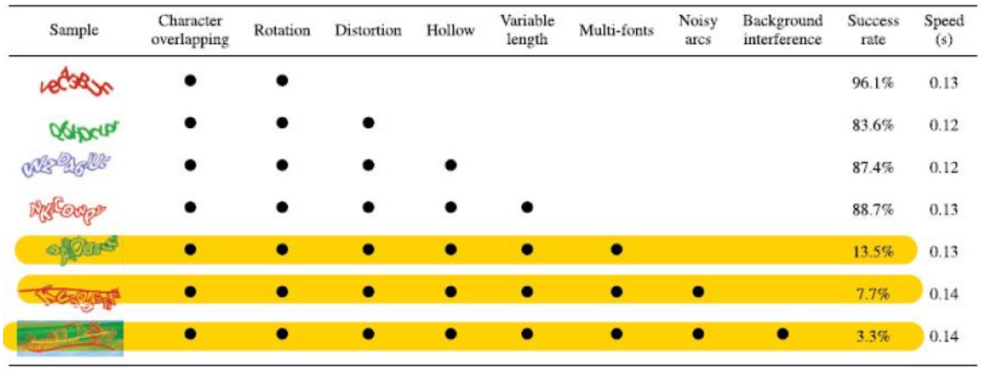
3.9 CAPTCHA's vulnerabilities in real world

Researchers have identified the weakness of computer security codes and to prove this, they have successfully neutralized the security code of famous websites such as Visa, CNN, and eBay. CAPTCHA is a security system and the process of evaluating the authenticity of service requesters, which is used to prevent some malicious attacks (such as Denial of Service attacks) by Internet robots. This process can determine whether the visitors to a site or other online services are real users or computers.

Eli Burzestan et al. succeeded in breaking these codes [28]. The automatic tool known as DeCAPTCHA includes the removal of noise and broken text strings of the background image as single characters for easier identification of the code. The researchers used this tool on several selected sites, among which the Visa site's Authorize.net payment gateway was broken in 66% of cases, eBay site's CAPTCHA in 43% of cases, and in a lower percentage in other sites such as Wikipedia, Digg and CNN. Only Google that uses reCAPTCHA resisted these attacks. Interestingly, reCAPTCHA also originated from Carnegie Mellon University and it is used by Google since 2002 [7].

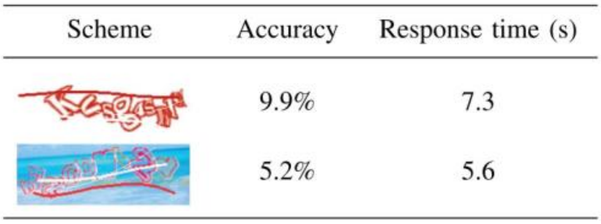
3.10 CAPTCHAs becoming more difficult

Every user may have encountered such a problem that the displayed word was so complicated and difficult that he could not recognize and type it easily. With the advancement of computer programs, it becomes more difficult to design a suitable CAPTCHA. A recent study suggests that most of existing methods are not easy for human users to interpret [44]. As an illustration, the success rates of the most robust text CAPTCHA systems, as depicted in Figure(3.3), stood at merely 7.7% and 3.3% correspondingly. However, these two applications had unfriendly interfaces and were not visible to the general public. As indicated in Figure (3.4), the user accuracy for these programs was 9.9% and 5.2%, highlighting their inefficacy for practical use [45].



Sample	Character overlapping	Rotation	Distortion	Hollow	Variable length	Multi-fonts	Noisy arcs	Background interference	Success rate	Speed (s)
	●	●							96.1%	0.13
	●	●	●						83.6%	0.12
	●	●	●	●					87.4%	0.12
	●	●	●	●	●				88.7%	0.13
	●	●	●	●	●	●			13.5%	0.13
	●	●	●	●	●	●	●		7.7%	0.14
	●	●	●	●	●	●	●	●	3.3%	0.14

Figure 3.3: Attack results on complex text CAPTCHAs



Scheme	Accuracy	Response time (s)
	9.9%	7.3
	5.2%	5.6

Figure 3.4: Human readability analysis of two complex CAPTCHA's Accuracy & Response time

4

Summary and Conclusion

4.1 Summary

The first chapter of this thesis lays a foundation by presenting a comprehensive overview of the ever-advancing landscape of web technology and its pervasive integration into daily life. While the internet offers myriad advantages, the chapter underscores the persistent challenge of security, introducing the crucial CIA triad (Confidentiality, Integrity, and Availability). The discussion gravitates towards the potent threat of Denial of Service attacks, particularly those orchestrated by automated bots. A key focus is directed at CAPTCHA's role as a security mechanism, stemming from the Turing test concept, with an exploration of its applications in safeguarding online polls, registration forms, and mitigating spam. The emergence of reCAPTCHA, a more advanced iteration, is introduced, incorporating scanned book text and progressing towards an invisible form. The overarching objectives of the thesis are set: a comprehensive examination of existing human-robot detection methods, specifically CAPTCHAs, to ensure efficiency and security against a diverse array of robots in real-world scenarios.

The second chapter embarks on a thorough exploration of the evolutionary journey of CAPTCHAs. It commences with a reminder of CAPTCHA's pivotal role in distinguishing humans from robots and preventing service attacks. Delving into its history, the chapter traces the evolution from its inception in 1997, examining various CAPTCHA classes. These include question and answer-based, text-based, image-based, puzzle-based, game-based, video-based, audio-based, social network-based, cognitive/biometric-based, and gestural CAPTCHAs. The chapter also introduces the intriguing concept of "Invisible CAPTCHAs" designed to leverage subtle smartphone micro-movements for human-bot discrimination without explicit challenges. It concludes with reflections on the perpetual challenge of developing CAPTCHAs resilient against advancing AI capabilities and the indispensable role of innovative solutions to counteract emerging AI-based threats.

Chapter three builds on the foundations laid in the previous chapters, delving into the evolution and challenges of CAPTCHAs and introducing a notable solution (reCAPTCHA). The narrative emphasizes the ongoing battle between artificial intelligence and CAPTCHA, with a particular focus on methods, such as the RCN algorithm, designed to efficiently bypass text-based CAPTCHAs. The inefficiencies of traditional CAPTCHAs set the stage for the introduction of reCAPTCHA by Google as a creative solution that engages users in the recognition process to overcome OCR limitations. The chapter highlights the structural aspects of reCAPTCHA, incorporating user parameters like incorrect entries, IP addresses, and active time to enhance its efficacy in distinguishing humans from bots. However, the chapter concludes by acknowledging the weaknesses of CAPTCHA, encompassing usability challenges, accessibility issues, susceptibility to advanced bots, maintenance costs, negative user experiences, privacy concerns, circumvention possibilities, and language and cultural barriers. The introduction of Invisible reCAPTCHA is also discussed, along with proposed research solutions aimed at fortifying reCAPTCHA's security against automated bot attacks.

References

[1] U. Cisco, "Cisco annual internet report (2018–2023) white paper," Cisco: San Jose, CA, USA, vol. 10, nr. 1, s. 1-35, 2020.

[2] L. Abusalah, A. Khokhar og M. Guizani, "A survey of secure mobile ad hoc routing protocols," IEEE communications surveys & tutorials, vol. 10, nr. 4, s. 78-93, 2008.

[3] M. Moradi og M. Keyvanpour, "CAPTCHA and its alternatives: A review," Security and Communication Networks, vol. 8, nr. 12, s. 2135-2156, 2015.

[4] S. Sivakorn, J. Polakis og A. D. Keromytis, "I'm not a human: Breaking the google reCAPTCHA," Black Hat, vol. 14, s. 1-12, 2016.

[5] D. Brodić, A. Amelio og R. Janković, "Exploring the influence of CAPTCHA types to the users response time by statistical analysis," Multimedia Tools and Applications, vol. 77, s. 12293-12329, 2018.

[6] D. Doran og S. S. Gokhale, "Web robot detection techniques: Overview and limitations," Data Mining and Knowledge Discovery, vol. 22, s. 183-210, 2011.

[7] A. M. Turing, Computing machinery and intelligence. Springer, 2009.

[8] Pinar Saygin, Ayse, Ilyas Cicekli, and Varol Akman. "Turing test: 50 years later." Minds and machines 10, no. 4: 463-518, 2000.

[9] A. Haleem, M. Javaid og R. P. Singh, "An era of chatgpt as a significant futuristic support tool: A study on features, abilities, and challenges," BenchCouncil transactions on benchmarks, standards and evaluations, vol. 2, nr. 4, s. 100089, 2022.

[10] I'm not a human: Breaking the Google reCAPTCHA S Sivakorn, J Polakis, AD Keromytis - Black Hat, 2016

[11] A. M. Alammar, B. A. Al-Yousef og I. Achour, "CAPTCHA techniques: Types, benefits, and issues: A review," IJCSNS, vol. 22, nr. 5, s. 485, 2022.

[12] C. Pope og K. Kaur, "Is it human or computer? Defending e-commerce with CAPTCHAs," IT professional, vol. 7, nr. 2, s. 43-49, 2005.

[13] A. O. Adesina, P. S. Ayobioloja, I. C. Obagbuwa, T. J. Odule, A. A. Afolorunso og S. A. Ajagbe, "An improved text-based and image-based CAPTCHA based on solving and response time," CMC-COMPUTERS MATERIALS & CONTINUA, vol. 74, nr. 2, s. 2661-2675, 2023.

[14] Gotta CAPTCHA'Em all: a survey of 20 Years of the human-or-computer Dilemma M Guerar, L Verderame, M Migliardi, F Palmieri, A Merlo ACM Computing Surveys (CSUR), 2021•dl.acm.org

[15] Z. Zhang, S. Zhu, J. Mink, A. Xiong, L. Song og G. Wang, "Beyond bot detection: Combating fraudulent online survey takers," i Proceedings of the ACM Web Conference 2022, 2022, s. 699-709.

[16] M. Kumar, M. Jindal og M. Kumar, "A systematic survey on CAPTCHA recognition: Types, creation and breaking techniques," Archives of Computational Methods in Engineering, vol. 29, nr. 2, s. 1107-1136, 2022.

[17] G. An og W. Yu, "CAPTCHA recognition algorithm based on the relative shape context and point pattern matching," i 2017 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 2017, s. 168-172: IEEE.

[18] M. Magdy, M. A. Tawfeek og H. M. Mousa, "A comprehensive study for different types of CAPTCHA methods and various attacks," 2021.

[19] D. Lorenzi, E. Uzun, J. Vaidya, S. Sural og V. Atluri, "Towards designing robust CAPTCHAs," Journal of computer security, vol. 26, nr. 6, s. 731-760, 2018.

[20] R. ur Rahman, D. S. Tomar og S. Das, "Dynamic image based CAPTCHA," i 2012 International Conference on Communication Systems and Network Technologies, 2012, s. 90-94: IEEE.

[21] D. Brodić, A. Amelio, D. Brodić og A. Amelio, "Direction of CAPTCHA," The CAPTCHA: Perspectives and Challenges: Perspectives and Challenges in Artificial Intelligence, s. 33-53, 2020.

[22] Guerar, Meriem, Luca Verderame, Mauro Migliardi, Francesco Palmieri, and Alessio Merlo. "Gotta CAPTCHA'Em all: a survey of 20 Years of the human-or-computer Dilemma." ACM Computing Surveys (CSUR) 54, no. 9 (2021): 1-33.

[23] Y. Zhang, H. Gao, G. Pei, S. Luo, G. Chang og N. Cheng, "A survey of research on CAPTCHA designing and breaking techniques," i 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2019, s. 75-84: IEEE.

[24] M. Khan, T. Shah og S. I. Batool, "A new implementation of chaotic s-boxes in CAPTCHA," Signal, Image and Video Processing, vol. 10, s. 293-300, 2016.

[25] M. Greene, Large scale CAPTCHA survey. University of Delaware, 2018.

[26] Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study. Author links open overlay panel by CJ Hernandez-Castro · 2010 · Cited by 79

[27] S. Shirali-Shahreza, H. Abolhassani, H. Sameti og M. Hassan, "Spoken CAPTCHA: A CAPTCHA system for blind users," i 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, 2009, vol. 1, s. 221-224: IEEE.

[28] E. Bursztein, R. Beauxis, H. Paskov, D. Perito, C. Fabry og J. Mitchell, "The failure of noise-based non-continuous audio CAPTCHAs," i 2011 IEEE symposium on security and privacy, 2011, s. 19-31: IEEE.

[29] K. Bock, D. Patel, G. Hughey og D. Levin, "unCAPTCHA: A low-resource defeat of reCAPTCHA's audio challenge," i 11th USENIX Workshop on Offensive Technologies (WOOT 17), 2017.

[30] D. Brodić, S. Petrovska, M. Jevtić og Z. Milivojević, "The influence of the CAPTCHA types to its solving times," i 2016 39th International Convention

on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016, s. 1274-1277: IEEE.

[31] N. P. Bora og D. C. Jain, "A web authentication biometric 3d animated CAPTCHA system using artificial intelligence and machine learning approach," Journal of Artificial Intelligence and Technology, vol. 3, nr. 3, s. 126-133, 2023.

[32] S. Shojae Chaeikar, F. Mirzaei Asl, S. Yazdanpanah, M. Zamani, A. A. Manaf og T. Khodadadi, "Secure CAPTCHA by genetic algorithm (ga) and multilayer perceptron (mlp)," Electronics, vol. 12, nr. 19, s. 4084, 2023.

[33] A. Acien, A. Morales, J. Fierrez og R. Vera-Rodriguez, "BeCAPTCHA-mouse: Synthetic mouse trajectories and improved bot detection," Pattern Recognition, vol. 127, s. 108643, 2022.

[34] M. Mohamed og N. Saxena, "Gametrics: Towards attack-resilient behavioral authentication with simple cognitive games," i Proceedings of the 32nd Annual Conference on Computer Security Applications, 2016, s. 277-288.

[35] A. Siripitakchai, S. Phimoltares og A. Mahaweerawat, "Eye-CAPTCHA: An enhanced CAPTCHA using eye movement," i 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, s. 2120-2126: IEEE.

[36] T. Hupperich, K. Krombholz og T. Holz, "Sensor CAPTCHAs: On the usability of instrumenting hardware sensors to prove liveliness," i Trust and Trustworthy Computing: 9th International Conference, TRUST 2016, Vienna, Austria, August 29-30, 2016, Proceedings 9, 2016, s. 40-59: Springer.

[37] X. Wang et al., “Robustness of text-based completely automated public turing test to tell computers and humans apart,” IET Inf. Secur., vol. 10, no. 1, pp. 45–52, 2016.

[38] S. Kwon og S. Cha, "A paradigm shift for the CAPTCHA race: Adding uncertainty to the process," IEEE Software, vol. 33, nr. 6, s. 80-85, 2016.

[39] H. Abubaker, K. Salah, H. Al-Muhairi og A. Bentiba, "Architectural design of a cloud-based reCAPTCHA service," i 2016 12th International Conference on Innovations in Information Technology (IIT), 2016, s. 1-6: IEEE.

[40] D. George et al., "A generative vision model that trains with high data efficiency and breaks text-based CAPTCHAs," Science, vol. 358, nr. 6368, s. eaag2612, 2017.

[41] O. Gaggi, "A study on accessibility of google reCAPTCHA systems," i Open challenges in online social networks, 2022, s. 25-30.

[42] N. Jiang og H. Dogan, "Tapcha–an 'invisible'CAPTCHA scheme," i Proceedings of the 32nd International BCS Human Computer Interaction Conference 32, 2018, s. 1-4.

[43] Wang, Dylan, Melody Moh, and Teng-Sheng Moh. "Using deep learning to solve google recaptcha v2's image challenges." In 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), pp. 1-5. IEEE, 2020.

[44] H Weng, B Zhao, S Ji, J Chen, T Wang, Q He, R Beyah Big Data Mining and Analytics,"Towards understanding the security of modern image captchas and underground captcha-solving services", IEEE, 2019

[45] Y. Zi, H. Gao, Z. Cheng og Y. Liu, "An end-to-end attack on text CAPTCHAs," IEEE Transactions on Information Forensics and Security, vol. 15, s. 753-766, 2019.

[46] Y. Raut, S. Pote, H. Boricha og P. Gunjgur, "A robust CAPTCHA scheme for web security," i 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA, 2022, s. 1-6: IEEE).