CAPTCHA Techniques: Types, Benefits, and issues: A Review

Afnan Mousa Alammar, Btool Ahmed Al-Yousef, Imen Achour
af1nan@hotmail.com, Btool.8@hotmail.com, eman.a@mu.edu.sa
Department of Computer Science and Information, College of Science Al Zulfi, Majmaah University,
Al-Majmaah Kingdom of Saudi Arabia

1. Summary

CAPTCHA stands for a completely automated public Turing test designed to differentiate between machines and humans. Pronounced as (CAP-TCHA), CAPTCHA isn't the only way to block spammers, but it's still one of the most effective and widely used ways to do it. In light of the developments of our time, the Internet has become an integral part of our lives and everything we need is related to the Internet. In contrast, the percentage of electronic piracy has increased, so the use of CAPTCHA to enhance security in electronic systems has become very important to distinguish real people and stop electronic piracy. The main function of CAPTCHA is to prevent automated bots (spam) from proving the identity of users. Despite its importance, many studies on this topic have not been published. Our current paper aims to clarify the CAPTCHA schema and its purpose, review the different types, and attempt to compare them based on different criteria. Introduce various attack methods, design, discuss issues, and improve some kinds of problems at an advanced stage.

Key words:
CAPTCHA – SECURITY – DESIGN – TYPES – ATTACK

2. Introduction

Nowadays, nobody can deny the importance of the internet in our daily lives. Indeed, the availability of the large amount of free information has led to the increase of the internet users. Web developers are always challenged by security issues. Several methods have been developed by researchers to countersuch attacks. However, most of the methods are very expensive and require a lot of expertise. For instance, One-Time Passwords. CAPTCHA is one of the cheapest and most efficient methods. While many people may not know the termCAPTCHA, they use them quite frequently [12]. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) It's a program that can generate and grade tests that most humans canpass but also current computer programs can't. Basically, CAPTCHA is a software intended to distinguish human from machines typically as a way ofthwarting spam and automated extraction of data from websites. CAPTCHAs invented in 1997. In 2000 Researchers at CMU were informed by Yahoo about the "chat room problem" in which bots joined chat rooms and solicitedusers to click on advertisements. The CMU professors Manuel Blum, Luis von A, and John Langford have developed a GIMPY captcha which shows large English words as images, prompting the user to select the correct spelling. The term "CAPTCHA" was invented in2003. As of 2009, Google has deployed a new captcha technology called ReCAPTCHA. In past years, Google has used image-based captchas to identify objects, trees, street signs [6]. There are various types of CAPTCHA for instance Text-Based, Image-Based, Video-Based, Audio-Based, Puzzle- Based and Game-Based, Mouse-Based and Invisible-Based recently introduced by Google. These types maybe briefly described as following text-based it's a characters in a noisy background, image-based it's depending on image recognition according to a given hint, video-based watch the video then describes it in three words, audio- based listen to a sound with a blurry background, then identify the characters that are being spoken, in the puzzle-based the user is presented with pieces of images that need to be consolidated and the game-baseddepend on compact games to verify human interaction on websites. Each CAPTCHA type has its advantages and disadvantages. Therefore, we can't consider one CAPTCHA type is good or bad. For instance, some CAPTCHAs are suitable for blind where are others not. For instance, the audio-based captcha it's designed especially for blind individuals while the remain types are not suitable for blind people expect the new CAPTCHAMouse-Based. CAPTCHAs should be human friendly but should also be robust and resistant to computer program.

Contribution

In this current work we a have deeply reviewed the different types of Captcha Technique. Compared the results of each type using different criteria. Moreover, we have extracted the advantages and disadvantages and highlighted some CAPTCHA. Give due attention to Captcha issues. In particular security issues which represent the main challenges.

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.68

Paper organization

The remaining of this paper will be as follows. In section 2 we described how captcha works. in section 3 we are enumerating applications of captcha, we presented captcha types in section 4, we presented issues in captcha in section 5, in section 6 we offered advantages and disadvantages of captcha, and we presented a comparison between types of captcha in section 7, In section 8 attack models and breaking techniques.

3. How CAPTCHA works:

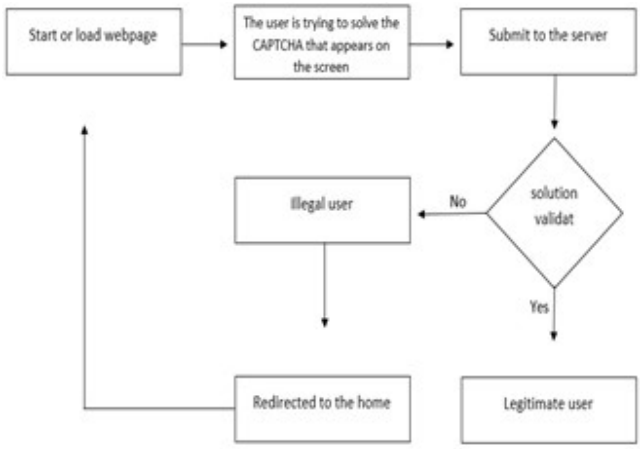

Figure 1 How CAPTCHA works

In this part we will give a brief description of the different steps followed by a captcha algorithm. First the user launch or load the web page, enter the CAPTCHA solution, send it to the server and verify the solution if it is correct, the user is legitimate, if it is incorrect, the user is illegal, and redirect to the home page.

4. Applications od CAPTCHA

There are several ways to utilize CAPTCHA for practical security, such as:

- Protecting Email Addresses from Scrapers: By using CAPTCHAs you can completely hide your email address from scrapers. To display an e-mail address, the user must solve a CAPTCHA [1].
- Online Polls: The CAPTCHA can also be used to restrict internet polls from being cast automatically by computer programs [12].
- Preventing Dictionary Attacks: According to an onlinearticle, a dictionary attack is a way to defeat an authentication system by attempting to guess its secretpassphrase or password [12].
- Worms and Spam: This protects against spam and worms that come from computer programs by only allowing mail to be received by humans and not by computer programs [1].

  Search Engine Bots: To prevent the web pages from being easily found, they should not be indexed. When an HTML tag is used, the bots cannot read the page. It only serves to say, "No bots please", but it is not guarantee [1].

5. CAPTCHA types

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 diagram shown in figure2.

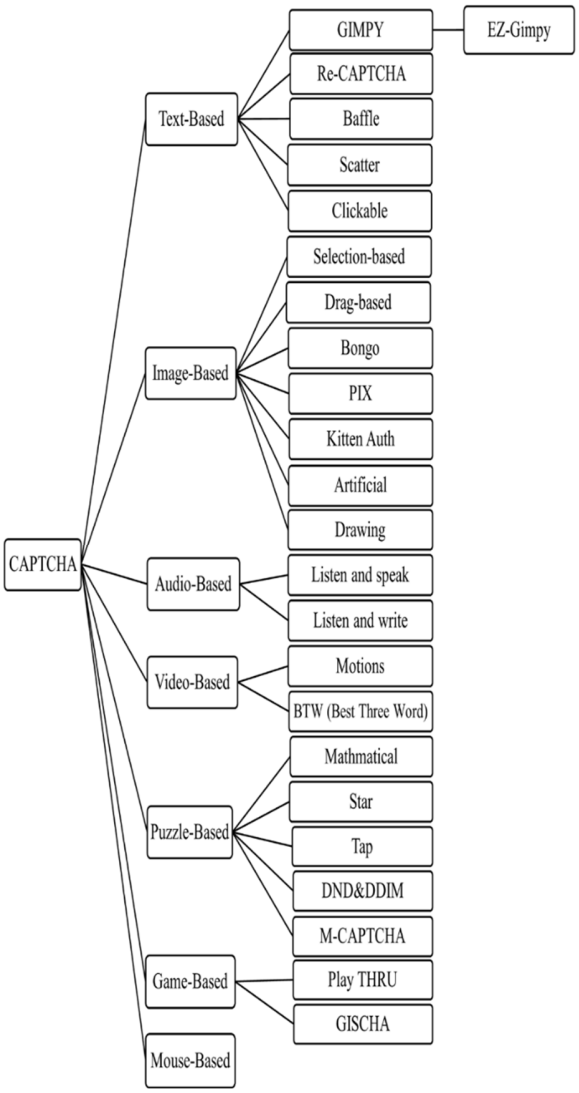

Figure 2 CAPTCHA Types

5.1. Text-Based: The most common type of CAPTCHA, Text-based captcha, is presented in a distorted form that contains letters and numbers which are case-insensitive. Furthermore, color blind people can easily solve them. and the texts are designed in an unrecognizable form (bycomputer programs) so that only humans can identify the characters embedded in the image. [1,8]

There are a variety types of text-based CAPTCHAs:

- **Gimpy:** In a gimpy CAPTCHA, the characters are displayed in a distorted, cluttered, overlapped, or corrupted image. Adding white and black lines,making non-linear changes, and asking the user to write the correct letter. This type of CAPTCHA was designed in cooperation with Yahoo! and it's the most common type [7] shown in figure3.

Figure 2 Gimpy

  - A simple type of Gimpy CAPTCHA developed from Carnegie Mellon University it's called **EZ- Gimpy** which mean (easy Gimpy) that uses differentfonts and distortions, making the characters easier to detect characters more than Gimpy as shown in figure4 It is used in chat rooms. [7]

Figure 3 EZ-GIMPY

- **Re-CAPTCHA**: Google's free service provides protection against spam and automated software on web pages shown in figure5.[7]

Figure 4 RE-CAPTCHA

- **Baffle:** It was developed at the Palo Alto Research Centre by Monica Chew (UC Berkeley) and Henry Baird (PARC). It is a CAPTCHA based on reading, using random masks as shown in figure6. The main idea of Baffle text is to reduce the problems in the dictionary. Nonsense that cannot be solved by using a computer program, but the user can use this reasoning to solve the problem. [7]

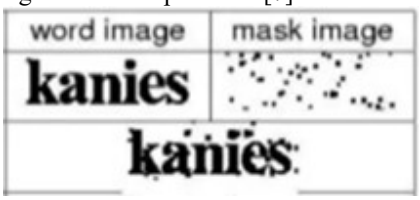

Figure 5 baffle

- **Scatter:** This type of CAPTCHA relies on segmentation characters. The characters cannot be easily broken because this method segments each character into multiple small pieces [7] shown in figure7.

Figure 6 Scatter

- **Clickable:** There are two defense mechanisms for this type: anti-detection and anti-recognition User, to passa test, the user must select three cells containing English words shown in figure8, otherwise, the test will fail. The user must be proficient in English. The software was created by Tencent. Semantic information and image interpretation are difficult for computers to comprehend. [7]

Figure 7 Clickable

5.2. Image-Based: This type of captcha displays an image to the user and relies on the user recognizing the imagefrom a group of images.

It is proposed using SVM (Support Vector Machine). In this method, the user the user is not demanded to type. It depends on image recognition to recognize an object or a particular idea from an image. It is also called Image Recognition CAPTCHA(IRC) [7,9].

There are a variety types under Image-Based CAPTCHA:

- **Selection-based:** The only requirement is to select the correct answer according to the hint.[8]
- **Click-based:** This type requires the users to click on characters that appear on a complicated background according to a short hint as shown in figure9, thereby simplifying the task, reducing the passing time and minimizing inconvenience to the users[8].

Figure 8 Click-based

- **Drag-based**: Drag-based CAPTCHAs determine whether the user is a human by analyzing the mouse's track, speed, and response time. They are simple to use.[8] Figure10.

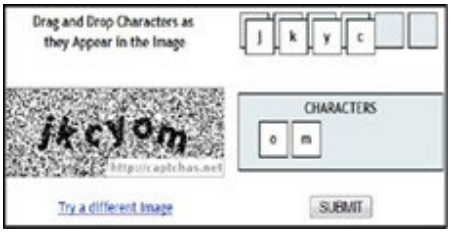

Figure 9 Drag-based

- **Bongo:** It requires the user to resolve the problem of visual pattern recognition. It appears as two blocks, one on each side as shown in figure11. A person must select thecorrect characteristic that differentiates the blocks appearing on the left from those appearing on the right. [7]

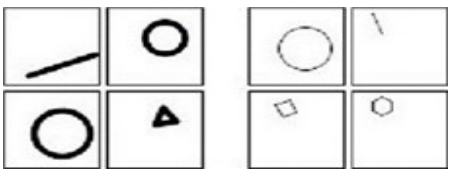

Figure 10 bongo

- **Pix:** It displays four different pictures of the same object and asks the user to write down the word that represents the object or the concept across the four pictures [7] shown in figure12.

Figure 11 Pix

- **KittenAuth:** The test consists of many pictures of different kinds of animals, and the user is supposed to click all the kitten pictures to pass [7] as shown in figure13.

Figure 12 KittenAUTH

- **Artificial:** This method exploited human abilities to recognize faces from displayed images through an automated reverse test called FACIAL [7] shown in figure14.

Figure 13 Artificial

- **Drawing:** It is used in PDA (Personal Digital Assistant).In a noisy background, many dots are displayed as shown in figure15, and the user is asked to connect them. [7]

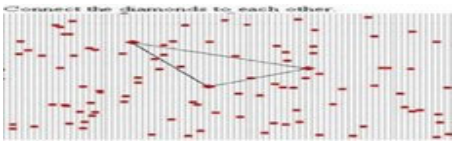

Figure 14 Drawing

5.3. Audio-Based: Users with visual impairments can use the audio-based CAPTCHA as it works using sound- based systems. Audio clips can be downloaded. Then, after listening the user submits the word. [1,2] Also, Audio-Based CAPTCHA has two different types: Listen and speak, Listen and write.

- **Listen and speak**: Using Text-To-Speech (TTS) technology, this system is designed to convert the selected word into speech, then play a sound clip and ask users to say it. [8] Shown in figure16.

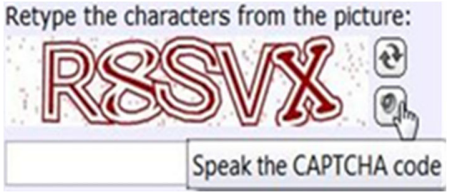

Figure 15 listen and speak

- **Listen and write:** Users must listen to noisy audio that is narrated by a voice that shows some characters. Those characters must be identified and submitted to servers to prove that the user is human. Artificially intelligent systems and AI attacks cannot identify the characters because the voice signal is distorted byadditional noise.[8] As shown in figure17.

Figure 16 listen and write

5.4. Video-Based: The user must provide three tags describing the video and a CAPTCHA engine separates the video clip into several segments after extracting a segment from a database. If there are any tags that match the ones on the video, the challenge passes. Videos CAPTCHAs are a recently developed technique. However, their bandwidth requirements and varying perception of the user pose challenges. [2] shown in figure18.

Figure 18 Video-Based

- **Motion-based:** Users are asked to choose the bestdescription of the person's motion in the video [7].
- **BTW (Best Three Word):** video-based CAPTCHAUsers are required to type three words describing avideo. [7]

5.5. Puzzle-Based: It asks the user to identify a particular image amongst lumps of images presented in an array of images or combine the pieces into a new image. For many users, this CAPTCHA is an interesting challenge. However, people Some people may have difficulty rearranging these segments if they have low cognitive abilities or low vision.[3,7]

Types of puzzle-based:

- **Mathematical:** this test requires an answer to a question in mathematics to pass these tests. [9]Shown in figure19.

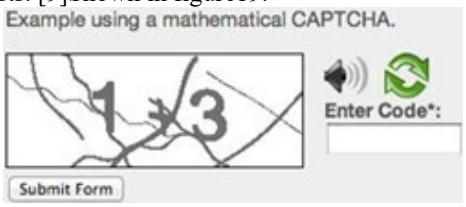

Figure 19 Mathematical

- **Star:** The application prompts the user to draw some stars into a square, based on cognitive abilities. The position of the star changes with themovement of the cursor. Users must move their cursor in the drawable space until the stars. As shown in figure20.

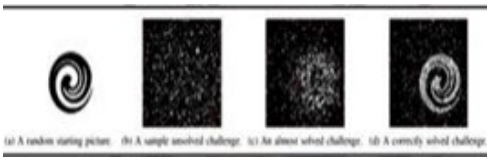

Figure 20 Star

- **DND&DDIM:** Drag and Drop CAPTCHA. DND is developed in [Desai 2009]. A specific word wasdistorted and each letter, separately, must be dragged and dropped into the appropriate position of this character. [7] Shown in figure21.

Figure 21 DND&DDIM

- **Tap:** The concept of design Tap CAPTCHA is built on a hybrid challenge that combines both textrecognition puzzles and shape recognition puzzles.[7] As in figure22.

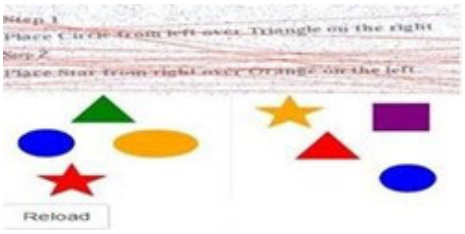

Figure 22 Tap

- **M-CAPTCHA:** Known as Mobile CAPTCHA, theHuman Interactive Proof (HIP) blocks bot attacksby requiring the user to draw a randomly generated pattern as in figure23. This technology was designedto use with touch screens such as smartphones and tablets. [7]

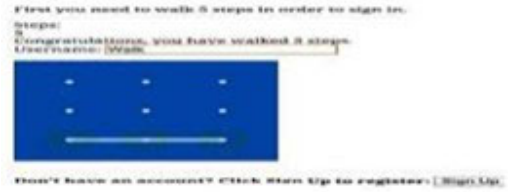

Figure 23 M-CAPTCHA

5.6. Game-based: Researcher who designs and develops intelligent CAPTCHA approaches, which rely on compact games to verify human interaction on websites.[7]

There are some types of game-based CAPTCHA:

- **Play thru:** Creating a new CAPTCHA that is simpler and more fun than other types of CAPTCHAs. It's called a dynamic cognitive game (DCG). A simple game piece appears through an image that requires the user to solve it. [7] as in figure24.

Figure 24 Play THRU

- **GISCHA:** It is possible to explain GISCHA with the use of a rolling ball rolling on a two-colored square surface and a target hall with different shapes. The user's ability to move the ball into thetarget hall is framed as a circle, but it is difficult for the computer program to understand and recognize the meaning of a rolling ball. [7]

5.7. Mouse-Based: Several years ago, Google developed a CAPTCHA that requires neither text, image, audio, nor video data to pass. By simply clicking the mouse, the computer can identify whether there is a person on the other side of the program. This feature is called reCAPTCHA. Users have to check a box to confirm they are not robots. Checkboxes aren't exactly boxes; they are virtual ones. An invisible text area isinserted in the form, which is filled with a value unique to theform. By examining this value, we can determine if a user isa bot or not. It can either be true or false. According to an online article, Google wasn't only dependent on check boxes but also relied on mouse movements to distinguish humans from programs. Furthermore, it analyzes the time visitors spend on the page, bot IP addresses, HTTP referrer, number of requests, and other factors. Google Analytics can also detect bots (to prevent them from increasing page views) andGoogle AdSense can block fraudulent clicks on ads (to prevent fraud). Google is keeping a lid on how the reCAPTCHA algorithm works, so it is difficult to know howit works. If reCAPTCHA is unsure about the user, a traditional image-based CAPTCHA is displayed. Therefore, according to Ahn et al., it is not a CAPTCHA since it is not public as CAPTCHA is defined. [12]

6. Pros and cons:

After a giving an extensive review of the different types of CAPTCHA we move now to discuss the pros and cons of the main based types in order to extract finally criteria based on which we will be able to compare them, and which is the main purpose of this work.

Table 1 pros and cons

CAPTCHA TYPES	PROS	CONS
Text-Based	- Text based CAPTCHAs are easy to build. [3] - Creation and recognition of content do not require a database,high internet bandwidth, or memorization of content phase. [3] - can increase security by using different fonts, lines, shapes, and different font sizes that can be recognized by humans but are hard for bots or computers to recognize. [3]	- Prone to OCR attacks. [1] - Susceptible to dictionary attacks when words are taken from the dictionary like Gimpy. [3] - Not suitable for visually impaired person [3] - Vulnerable to attacks by artificialintelligence tools CNN (Convolutional Neural Networks) and SVM (Support Vector Machine). [3] - Distorted signs: When signs are distorted, random sequences such as l and I, 5 and S, G and6, etc., lead to perceptual problems. [9]
Image-Based	- In the images- Based, they use animals, structures, vehicles, and other common objects. which are familiar to most people. [3] - It's not hard to recognize combinations of images when you're human, but it's hard for an automatic system to do so. [3] - A single task requires a large number of images, limiting the repetition of the same image in successive tasks. [9] - Simple click- based system so you do not have totype. [1] - Is easier to solve since there is no need to formulate a solution, only torecognize it.[3]	- Easily attacked by OCR attacks. [7] - Prone to artificial intelligence attacks. [3] - In comparison to text-based communication, the network bandwidth requirements are higher. [3] - Requires large database for storageof images. [9] - The attacker can identify it by using a random rate attack or by using a dictionary-based attack. [1] - People who are color blind have many problems.[1]
Video-Based	- Video based CAPTCHAs carry tags which make them easy to recognize. [3] - Humans can easily recognize the tags, but it's difficult for a bot.[3] - These techniques provide the user with a moving graphic that represents a particular visualization that can be expressed in one word.[9]	- A large database is needed to store video clips [3] - To load video, you need high bandwidth. [3] - Due to the large size of the files, users have difficulty downloading the video and passing the CAPTCHA test. [1] - Prone to OCR attacks. [3] - These videos cannot be solved by foreign users or non-native speakers. [9]
Audio-Based	- Audio-based CAPTCHAs are very useful for visually impaired people [1] - Humans can easily detect audio with noise, but it's difficult for a bot.[3] - The audio clip can be downloaded and listened to repeatedly at will. [3]	- Since the system isavailable in English,the end user should be familiar with the language. [1] - Characters with similar sounds are difficult for humans to recognize. [1] - User interaction takes more time higher bandwidth.[8]
Puzzle-Based	- Interesting to solve. [3] - It would be fun. [1] - It helps the user to monitor his brain. [1] - This captcha system is played like a game so that the user can interact with it more. [1] - Rearranging segments of an image is very difficult for a bot. [3]	- Requires much time to solve. [7] - Requires a lot of brain work, so it's hard to solve for people with low intelligence. [3] - The user cannot easily identify the puzzle. [1] - the defect lies in the limitation of the number of such questions which have a definite answer, are easily retrievable. [9]
Mouse-Based	You do not need to submit text, images, audio, or video to pass. A single mouse click is all you need.[12]	As a result of Mouse CAPTCHA failure, Invisible CAPTCHA is also rendered useless.[12]

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.68

7. Issues in CAPTCHA:

In this paper we will talk about issues may face CAPTCHA

a. Security issues
b. Usability issues

a. **Security issues:** Security issues: there are two ways to crack CAPTCHAs: challenge segmentation and character recognition. Since CAPTCHAs are no longer able to withstand attacks aimed at cracking the underlying protocols through man-in-the-middle or oracle attacks due to advances in OCR (optical character recognition) techniques, CAPTCHAs needed to be developed that are robust, secure, and usable. The success of a CAPTCHA technique depends on the accuracy achieved during segmentation. After this process, single character recognition techniques are applied at high speed. [1,10]

b. **Usability issues**: It is an important aspect of CAPTCHA and a measure of how effectively, efficiently, and satisfactorily users can achieve certain goals in each environment. The diverse backgrounds of users, such as differences in age, culture, and language, necessitate the consideration of two factors when designing a CAPTCHA system: visual perception and cognitive judgment. An important question is how to evaluate the usability of CAPTCHA. Using the following quality components, to define usability: [5,10]

- Memorability: if users return to the design after a period of disuse, how easily can they recover knowledge. [5]
- Satisfaction: How pleasant it is to use thedesign. [5]
- Accuracy: is a measure of the correctness with which users can respond to a CAPTCHA taskwithout making mistakes.[10]
- Response time: is the time it takes a user to respond to the CAPTCHA test. [10]
- Perceived difficulty: is the difficulty observed by users when solving CAPTCHA test. [10]

To make CAPTCHAs usable, high accuracy, low response time, and low perceived difficulty are desired. Biases are used in CAPTCHAs to improve security control. However,the use of excessive or uncontrolled bias levels and methods may not only render CAPTCHAs unusable, but also reduce security control, as the system would have to allow multiple attempts for failed tests.[10]

8. Attack models and breaking techniques:

Table 2 attacks model

Captcha type	Attack method	
Text-Based	Brute Force Attack	
	Smuggling	
	DE-CAPTCHA Pipeline	Pre-processing
		Segmentation
		Character structure
		Recognition
		post-segmentation
		post processing
		K-Nearest Neighbors (KNN)
		Support Vector Machines
		Convolutional Neural Networks(Deep Learning)CNN
	End to End	
	Teabag 3D attack	
Image-based	Single processing	
	Preprocessing	
	Vidoop	
	Database	
	brute force	
	Implementation	
Audio - based	single processing	

8.1. Attack for Text-Based CAPTCHA:

a. Brute Force Attacks: The sponge can use the sensitivityinformation to automatically attack CAPTCHA detailsby trying answers at random or according to a specifiedorder. This is typically used when the CAPTCHA test has a limited number of answers.

b. Smuggling Attack: The challenge is to automatically repeat the identifying online task. The attacker controls the attack behavior. At first, the script requires the user to perform an online task that the attacker wishes to postpone. When the malware gets to a victim's host, it intercepts the request and stores all information

locally.

c. DE-CAPTCHA Pipeline Attack: The attack consisted of five steps applied to a specific text CAPTCHA to break it. Attack methods in the second stage always involved segmentation and recognition. Before the segmentation stage, a few alternative preprocessing approaches are chosen. These preprocessing techniques focus on eliminating noise and highlighting the information.

There are some types under DE-CAPTCHA:

- Preprocessing: The image might be considered negligent if it is noise-free. By using different techniques, the background is removed, and the CAPTCHA is displayed in white and black and saved into the binary matrix. It is easier to implement the DE-CAPTCHA pipeline after a captcha is transformed into a binary matrix.
- Segmentation: Different segmentation methods are used to cut CAPTCHAs.
  - ❖ The following methods can be used to segment by single characters:
    - Uniform cutting: The method is suitable for CAPTCHAs whose characters are uniform in width and distribution. It is simple but limited.
    - Feature extraction: You can use this method for alphabetic characters and Arabic numerals. Certain character features are used, Forinstance, circles and dots. It will be possible todetect shapes in characters such as in "i" and "j", a loop effect in "a" and "b", a cross imagein "t" and "f," and so on.
    - Projection: For segmenting individual characters, the character projection histogram proves to be an effective method. This technique works well for non-overlapping characters. Projections can be horizontal or vertical, or a combination of the two.
    - CFS (color filling segmentation): Utilizing the CFS algorithm, each connected componentcan be detected using CFS. CFS identifies objects that are not segment able by projection and contributes to further segmentation. Based on a paint bucket flood filling algorithm. As CFS is a default segmentation method, it can segment CAPTCHA words regardless of whether they are tilted or overlapping.
  - ❖ Segmentation methods based on character components:
    - Filter: There are several types of text-based CAPTCHAs that can be processed using this method. By using filters of different orientations, it extracts the character components within a CAPTCHA Afterwards, each character is made up by combining adjacent elements in various ways
    - Character structure: The contour lines of characters constitute some close parts. The contour lines of characters constitute some close parts. After color filling and removing noise components, the strokes of the character are segmented along this close structure.
    - Recognition: After segmenting the CAPTCHA, the classifier can learn what a character looks like by using training mode. In the testing mode, each letter is detected individually with classifiers in predictive mode.
    - Post-Segmentation: Each segment that was produced in the previous step is individually processed to facilitate recognition. Normally, the magnitude of every segment is normalized.
    - Post-processing: The output of the classifier is getting better, and it can be enhanced by using spell-checking techniques to enhance its accuracy and regulation.

d. End-to-End attack: Researchers have rediscovered the methods of end-to-end attack because multistage processing is more complex and deep learning has powerful classification abilities. In addition to simplifying and accelerating the prediction process, it also reduces the prediction time greatly.

e. Teabag 3D attack: Its design is based on three- dimensional space. This type of 3D CAPTCHA ischaracterized by some of the following characteristics: The 3D-CAPTCHA is displayed as four letters in 3D space using only upper case and digits. The charactersare extremely close to each other and appear to be created from slightly different perspectives. The present challenges to Teabag 3DCAPTCHA can be divided into four phases based on differences in grid directions and shapes of background cells.

8.2. Attack for image-based CAPTCHA:

a. Signal processing attacks: common attacks in image and audio-based CAPTCHAs. The attacker can solve image CAPTCHAs by removing the noise and distortion with optical character recognition (OCR). Using chaos, noise, and distortion to confuse and

jumble image- and audio-based CAPTCHAs are possible tasks for machines. [7]

b. Preprocessing: the background is removed using various techniques and the CAPTCHA is rendered in white and black and stored in a binary matrix. [3,7]
c. Vidoop CAPTCHA attack: a special type of image- based CAPTCHA attack. It uses images of objects, landscapes, people, animals, instead of distorted text to distinguish people from a computer program. [7]
d. Database Attacks: The underlying database can be partially created to attack image-based CAPTCHAs. Challenges displayed on the website reveal a portion of the database, but is it economically viable to recreate the entire database? While this approach may be suitable for an image database with a few images, it is not feasible for a database with millions of images unless there are financial incentives. [4]
e. brute force attack: A brute force attack is the simplest and most common method to defeat image-based CAPTCHAs. This involves providing random solutions to challenges based on a limited number of solutions until final success is achieved. In summary, the system castigates IP addresses that typically receive many consecutive incorrect responses by requiring them to correctly answer two challenges within three attempts before receiving a ticket. Attackers receive one service ticket for every 5.6 million attempts. [4,7]
f. Implementation Attacks: In some cases, CAPTCHAs have weak implementations. Think about what would

happen if the same session ID was used repeatedly to gain access. Stateful implementations can be used to track user sessions and stateful forms, whereas stateless services can be used to eliminate these scenarios. [4]

8.3. Attack for Audio - based CAPTCHA:

a. single processing attack: common attacks in image and audio-based CAPTCHAs. The attacker can solve image CAPTCHAs by removing the distortion andnoise with optical character recognition (OCR). Usingnoise, chaos, and distortion to confuse and jumbleimage- and audio-based CAPTCHAs are possible tasksfor machines. [7]

9. Comparison between CAPTCHA types and analysis:

In this section we have chosen nine criteria that seems to be the most relevant ones to compare Text, Image, Video, Audio, Puzzle, Mouse based techniques.

The most important features that characterize the efficiency of CAPTCHA are security and usability.

The table below is shows that there are no CAPTCHA types that provide or combines these two features -security and usability -. Therefore, we try to enhance the best CAPTCHA type that we have concluded which is the Mouse-based CAPTCHA. As it is shown in the table 2, this type of CAPTCHA represents the highest usability feature in term of time of response, easiness, learnability, availability, however the weak point of the Mouse-based CAPTCHA is the security which proved to be in the middle level.

Table 3 comparison between captcha types

CAPTCHA TYPES	***Text-Based***	***Image-Based***	***Video-Based***	***Audio-Based***	***Puzzle-Based***	***Mouse-Based***
Security	Low	Middle	Middle	Middle	High	Middle
Free	Yes	Yes	Yes	Yes	Yes	Yes
Suitable for the visually impaired	No	No	No	Yes	No	Yes
Easy ordifficultto use	Easy	Easy	Hard	Hard	Hard	Easy
Susceptiblele to OCRattacks	Yes	Yes	Yes	No	No	No
Language dependence	Yes	No	Yes	Yes	Sometimes	No
Intelligent dependence	No	No	No	No	Yes	No
Photo's dependence	Low	High	Low	Low	Middle	Low
Successrate on first try	Middle	Middle	Middle	Middle	Low	High

In the below figure, an explanation of how the proposed captcha works, the way it works in general is similar to the rest of the types where the user downloads the page, then the user appears the proposed captcha test, then the user solves the test and sends the solution, the server receives the solution and verifies the solution, if the solution is immediately True, the user is legal and skips the page otherwise, the user is illegal and says re-test. in the following figure 25, a detailed explanation of the captcha.

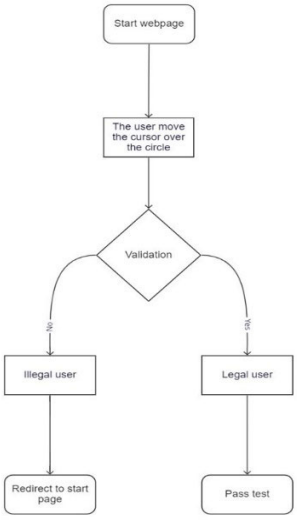

Figure 25

The proposed captcha test is a simple drawing in a circular shape with a very light line, and the user is asked to hover the mouse over the circular line in a circular motion, through this movement, the device recognizes the steps if it is a robot or a human as shown in figure 26, As we know that in general a robot is able to move in straightway not in curvilinear, so we have combine the two most important conditions for the captcha, which are high security and ease of use.

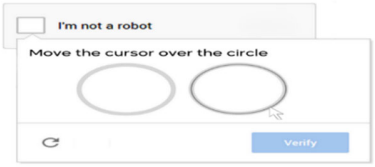

Figure 26

10. Conclusion:

Web applications use CAPTCHA to protect systems from malicious bot attacks and to distinguish humans from machines. In this paper, we present an extensive review of CAPTCHA. First, we start by explaining how the captcha works and some of the captcha applications, then we mentioned the types of captcha in an extensive manner with examples and mentioned the pros and cons of each type and made a comparison between the types based on specific parameters, in addition, we deeply studied the different issues that may a CAPTCHA technique suffer and highlighted the most important ones. at the end we have proposed a new model.

11. Acknowledgment:

The authors would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work.

References:

[1] Kaur, K., & Behal, S. (2014). CAPTCHA and its techniques: a review. International Journal of Computer Science and Information Technologies, 5(5), 6341-6344.

[2] Alqahtani, F. H., & Alsulaiman, F. A. (2020). Is image-based CAPTCHA secure against attacksbased on machine learning? An experimental study. Computers & Security, 88, 101635.

[3] Challa, R. K. (2020, December). CAPTCHA: A Systematic Review. In 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI) (pp. 1-8). IEEE.

[4] Singh, A., Tiwari, V., & Tentu, A. N. (2018, December). A Machine Vision Attack Model on Image Based CAPTCHAs Challenge: Large Scale Evaluation. In International Conference on Security,Privacy, and Applied Cryptography Engineering (pp.52-64). Springer, Cham.

[5] Ridzuan, F. R., Mahdin, H., Kasim, S., & Azmi, M.S. (2019). An Image-Based Captcha System Using Click. Acta Electronica Malaysia, 3(1), 23-25.

[6] Uma, P., Siddivinayak, K., & Ramachandra, P. (2019). Smart captcha to provide high security against bots. In Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering (pp. 3-5).

[7] Magdy, Menna, Medhat A. Tawfeek, and Hamdy M. Mousa. "A comprehensive Study for Different Types of CAPTCHA Methods and Various Attacks." (2021).

[8] Zhang, Yang, et al. "A survey of research on captchadesigning and breaking techniques." 2019 18th IEEEInternational Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE,2019.

[9] Thomas, Varun Ambrose, and Karanvir Kaur. "Cursor CAPTCHA-captcha mechanism using mouse cursor." International Journal of Computer Applications 67.22 (2013).

[10] Banday, M. Tariq, and Nisar A. Shah. "A study of captchas for securing web services." arXiv preprint arXiv:1112.5605 (2011).

[11] Bursztein, Elie, Matthieu Martin, and John Mitchell. "Text-based CAPTCHA strengths and weaknesses."Proceedings of the 18th ACM conference onComputer and communications security. 2011

[12] Kumar, Mohinder, M. K. Jindal, and Munish Kumar."A Systematic Survey on CAPTCHA Recognition: Types, Creation and Breaking Techniques." Archives of Computational Methods in Engineering(2021): 1-30.

[13] Gafni, R., & Nagar, I. (2016). CAPTCHA – Security affecting user experience. Issues in InformingScience and Information Technology, 13, 63-77

[14] Abdalla, K., & Kaya, M. (2017). An evaluation of different types of CAPTCHA: effectiveness, user- friendliness, and limitations. Int. J. Sci. Res. Inf. Syst.Eng, 2(3).

[15] Von Ahn, L., Blum, M., Hopper, N. J., & Langford,J. (2003, May). CAPTCHA: Using hard AI problems for security. In International conference on the theory and applications of cryptographic techniques(pp. 294-311). Springer, Berlin, Heidelberg.

[16] Yan, J., & El Ahmad, A. S. (2008, October). A Low- cost Attack on a Microsoft CAPTCHA. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 543- 554).

[17] Powell, B. M., Kumar, A., Thapar, J., Goswami, G., Vatsa, M., Singh, R., & Noore, A. (2016, September). A multibiometrics-based CAPTCHA for improved online security. In 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-8). IEEE.

[18] Goswami, Gaurav, et al. "FaceDCAPTCHA: Face detection-based color image CAPTCHA." Future Generation Computer Systems 31 (2014): 59-68

[19] PradeepKumar, S., R. Ramachandaran, and A. Saravanan. "Generation of Variant Random Order (VRO) in Text Graphics Color CAPTCHA for Enhancing Web Security Protection." Indian Journal of Science and Technology 9 (2016):10