A comprehensive Study for Different Types of CAPTCHA Methods and Various Attacks

Menna M.Elbalky, Medhat A. Tawfeek and Hamdy M. Mousa

Computer Science Department, Faculty of Computers and Information,
Menoufia University, Shebin Elkom 32511, Egypt,

Abstract **–**Due to the growth of the internet in our life and its importance in all our everyday activities , including occupational and educational ones .We should also keep in mind that it harbours a negative aspect , as it brings security problems. Hence CAPTCHAs are used for making systems more secure. The major role of CAPTCHA is to prevent robotic bot (spam) form surrender or prove user personality. Using a pattern-matching algorithm is necessary for the user for comparison by receiving signs founded in similar matches. This method makes it difficult to get a forbidden access to data, since malicious bot is to spy out signs in the image. This mechanism implements actions on the attitude of user gesticulation which makes it distinguishable and secure. Human-Computer Interaction i.e. interaction between computer and individual is made to make it easy in understand human language .On other words, Human-computer Interaction focuses on the study of interfaces between computer and human. This paper presents a comprehensive study of various different types of CAPTCHA, the ones good in securing webpages. It also discusses the strengths and weaknesses of each one. Moreover, its importance in discerning the user’s individuality, the behavior of humans, and bots and the paper will illustrate some CAPTCHAs mechaniits and impairments which allows hackers to break .In addition, is necessary to take into consideration the approaches of building a good CAPTCHA.

Keywords -*CAPTCHA , Bot programs, Hackers, spammer, Scrapers, online social network.*

I.**I**NTRODUCTION

CAPTCHA is fundamentally used for security purposes.It is a mechanism that is used on webpages to be assured these rejoinder come from forbidden person. CAPTCHAs are mostly used to block spams.Spamming is accomplished at various public email supplier places and various forums, besieds blogs too. However, there are several types of CAPTCHA .CAPTCHA [1] mechanism is used to secure online services and resources against bad bots. CAPTCHAs have been integrated. Many are based on (OCR) Optical Character Recognition [3]. For example, CAPTCHA based on text, whereas others are based on (Non-OCR) Non-Optical Character Recognition [4] which uses multimedia, for example, video and voice. Some CAPTCHA types have been suspended by bots. This paper will analyse the different types of CAPTCHAs approach in recently published papers, discuss the classifications, contrasting between CAPTCHA from their impairment and strength. The challenge is presented through an interface which asks the party who aims to access a specific resource or service to solve the CAPTCHA test to be an authorized party. CAPTCHA nature and design are established on the appreciated intelligence cavity between philanthropic and machinability with respect to some problem, which is easy to solve for humans but not yet solvable by computers. There are several steps of working CAPTCHA as illustrated in figure 1.

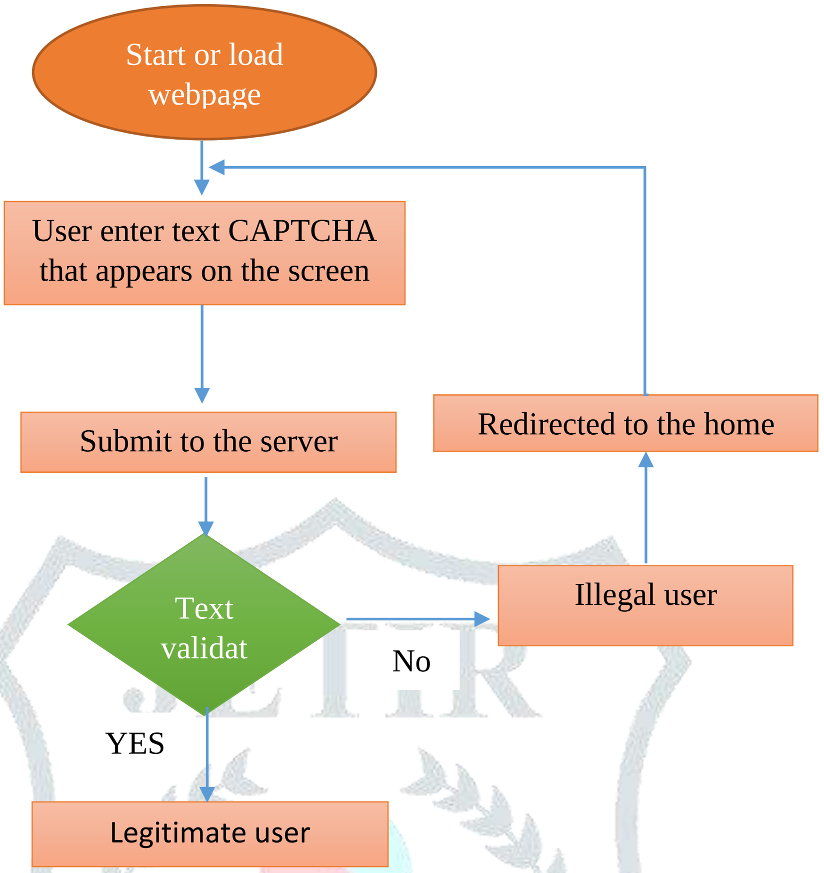


Figure 1: steps of working CAPTCHA

II. Classification of CAPTCHAs

There are several types of CAPTCHA, list as follows :

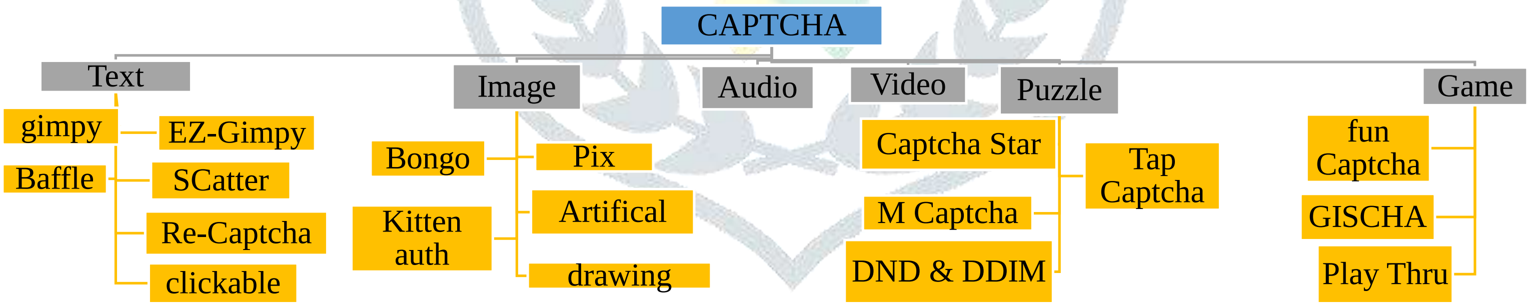


Figure 2: CAPTCHA types

A. *CAPTCHA based on the text*: This type is easy to execute a group of digits or letters appear to the users and asks users to recognize group of letters with lower & upper case or digit the designer make noise that can be classified into anti- segmentation (hollow schema : contour lines apply to form each letter as the connected letter are hard to segment but are easily seen by human but it is not secure as human expected [35] , CCT : crowing character together complicate segmention however it reduce readability for users and Overlapping try to make segmentation more difficult by using squeezing letter to gether but reduce user friendliness[36] , noise: it hide the position of letters , complex background to confuse solver [37] ,two layer structure : vertical combination of two horrizantal captches which complicates the segmentation of image[38]) ,and anti-recognition technique by adding (Multiple Fonts, Wave Motion, rotating or rendering letters in the shape of three dimension)this three designed to increase the diversityof each letter a few alterations to the letters for example scattering, , Blurred Letters, ,Collapsing(removing space between characters to avoid segmentation by bots) this changes preventing bots from pursuing the real character [38]. It consists of several types.

1) *Gimpy CAPTCHA*: Most common CAPTCHAs which are firstly based on sequence of character displayed in form of a distorted , clutter ,overlapped or corrupted image as illustrated in figure (3) by adding white and black lines, doing non-linear modification and asking user to write the correct letter. This CAPTCHA was developed in cooperation with Yahoo for preventing chat rooms from bots and to disable them from writing post or classified ads and written carbons to generate free e-mail addresses [5, 6].

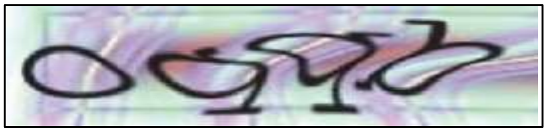
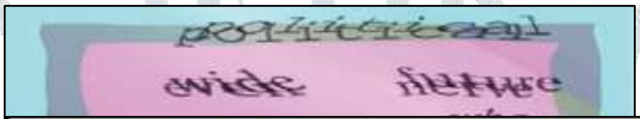
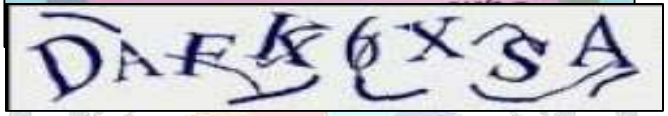


Figure 3: Gimpy CAPTCHA

2) *EZ-Gimpy CAPTCHA*: A Simple type of gimpy CAPTCHA developed from Carnegie Mellon University, it's a chosen word from the dictionary of words. Next, the word appears into image using different fonts; and various style of distortions which is easy to detect character more than gimpy [6,7] . It is used in chat rooms as illustrated in figure (4) broken by dictionary attacks and by Mori et al[11].

Figure 4: EZ-Gimpy CAPTCHA





3) *Baffle text*: It has been developed by Monica Chew (UC Berkeley) and Henry Baird (PARC) at the Palo Alto Research Centre. It’s a reading-based CAPTCHA that uses a random masking to degrade images or non-English pronounceable character strings and asks the user to recognize the masked words as displayed in Figure (3), for example printing and scanning it or applying the threshold technique on picture [8, 9] which transform picture from color to white and black and back it again. Adding noise and changing the gray level random to the image. The main idea of Baffle text is to reduce problem in the dictionary. By using nonsense words where computer programs cannot solve it but the user can use this inference to solving the problem [5, 6]. It is llustrated in figure (5).

Figure 5: Baffle CAPTCHA

4) *Scatter Type Method*: This kind of CAPTCHA depends on segmentation of characters. Characters are revised by severing each word into dislodge pieces. These technique for the realization of characters cannot break characters easily because every character in this method is segmented into multiple small pieces. Although, the characters are randomly selected so vocabulary can’t be used to expect the correct term. Figure (6) is an example of Scatter type method [8, 9].

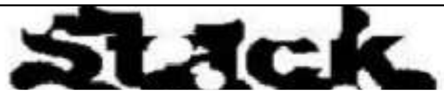


Figure 6: Scatter CAPTCHA

5) *Clickable CAPTCHA*: this type has two defense mechanisms: anti-detection and anti-recognition User should press on the three cells which include English words to pass the test but if the user pressed on words that are not in the English vocabloury, the answer will be incorrect as illustrated in figure (7). It depends on the perfection of the user in english language [10]. Recently, a novel of clickable CAPTCHA

named VTT was developed by Tencent .The computer cannot understand the semantic information and analyze the image like human shown in figure(8).

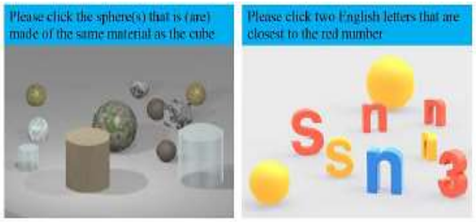

Please click the sphere(s) that is (are) made of the same material as the cube
Please click two English letters that are closest to the red number

Figure 8: VTT Clickable

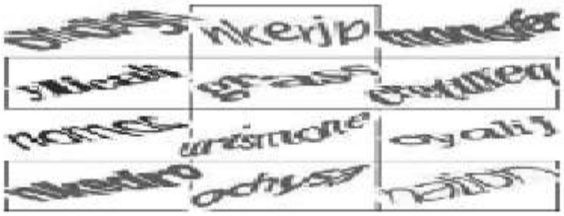
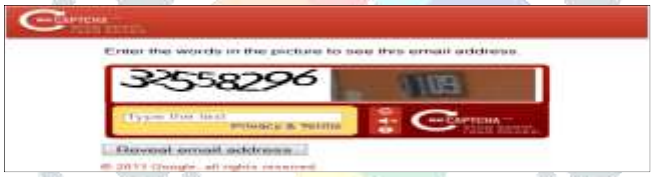


Figure 7: Clickable CAPTCHA

6) *Re-CAPTCHA*: Is a free service provided by Google that protects webpages from automated software, spam. The Most recent sensibility of Re-CAPTCHAs is that their captchas passed by attackers who used goggle's web tools as illustrated in figure (9), this was fixed in the latest update to re-Captcha v3. The other sensibility includes machine learning algorithms, brute force attacks, optical character recognition, and third-party attacks.Hotmail or MSN CAPTCHAs [12]: used in registeration in Hotmail emailing service , choose eight English letters (upper case letters and digits); then, applying dark blue color on a light gray background on the characters. Next, three types of arch are randomly added for making difficult segmentation.Yahoo! CAPTCHA (Yahoo version 2): Yahoo introduced its second-generation CAPTCHA.Their specification perform by using a string of characters without using the English words, using letters and digits black and white colors, and having linked lines and arcs as clutter. Google/Gmail: The characteristic of this CAPTCHA, is used by Gmail.com, using only warping image for character distortion, only having two colors. Two emergent techniques that can break reCAPTCHA illustrated as follows Shape recognition-based algorithm (Baecher et al., 2011), and image segmentation-based algorithm (Cruz- Perez et al., 2012).



Enter the words in the picture to see this email address

Figure 9:Re- CAPTCHA

A. *CAPTCHAs based on image*: This type shows an image appears to the user and depends on recognizing image from a group of images, once are blended with some terms [11]. It proposed using SVM (support vector machine) The user does not require to enter or read any text it depends on image recognition in order to recognize object or specific idea from image[16] .Using different design considerations. for example different patterns, algorithms of image generation, different size, and several dimensions. In addition, making it more secure requires various transformations applied on the objects for example color quantization, dithering and adding noisy ,rotation, transparency, scaling , and adding noisy [Raj et al 2012]So that it happens to be troublesome for spam projects to recognize designs and where users can pass the test there are many types of these methods as follows;

1) *Bongo*: It requires the user to resolve the problem of visual pattern recognition. Two blocks appear: one on right and one on left. The blocks appearing on the left are different from the blocks appearing on the right, and the person must select correct characteristic that sets to the two series apart shown in figure (10) [12, 13].

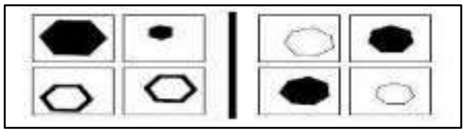


Figure 10: Bongo CAPTCHA

2) *Pix*: A huge database of pictures and moving picture of any objects for example cats, lions, dogs, flowers. As illustrated in figure (11) four different pictures of the same object appear to the user and user requires to write the word that marks the object or the concept that belongs to these images ask the user to type a word that indicates the object [13].

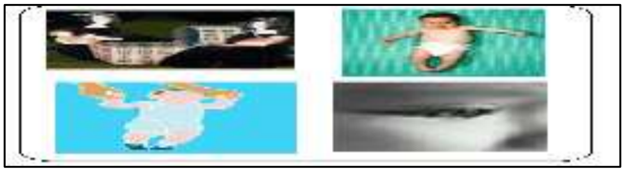
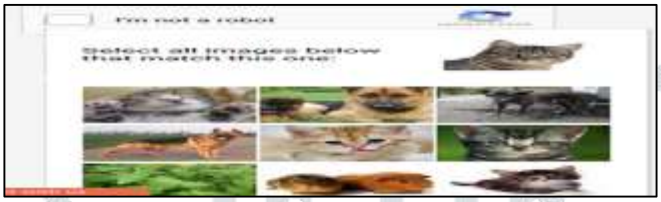


Figure 11: Pix CAPTCHA

3) *KittenAuth CAPTCHA*: Several pictures are displayed to the user with many different species of animals, as illustrated in Figure (12) and the user must click all the kitten pictures to pass the test [14].



I'm not a robot

Select all images below that match this one:

Figure 12: KittenAuth CAPTCHA

4) *Artificial CAPTCHA*: Automated Reverse test using features called FACIAL. It used to exploitability of the human to realize human faces from displayed images shown in figure (13) [15].

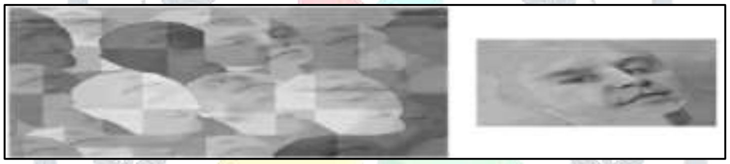
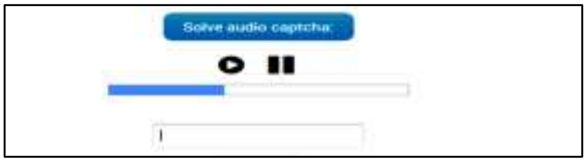


Figure 13: Artificial CAPTCHA

5) *Drawing CAPTCHA Method*: It is used in PDA (Personal Digital Assistance). A noisy background is displayed many dots and asked the user to connect dots with each other [16].

B. *CAPTCHAs based on audio*: This mechanism is known as visual CAPTCHAs in case of visually impaired users. Another type of audio captcha in which users aren't required only to listen but to preonounce a sound captcha in which a user should hear the secntence selected randomly . Here, it is beceessary to take into consideration computers' disability to recognize sound in noise distortion. It depicted in presenting acquainting words to the client appearing in voice sound, so the client is asked to write what he/she has heard for solving the CAPTCHA. The characteristics of this kind is that it can be utilized for the users they have hard problem in hearing. The test challenges the user to write letters of a word in an audio clip as illustrated in figure (14). Both male and female voices are used in common audio CAPTCHAs [17].

Figure 14: Audio CAPTCHA



C. *CAPTCHA based on the video*: A short motion video contains an individual speaking to some sort of activity and the client must choose the correct depiction from the rundown. This proposed video based on advertisement. The extent of the video in this technique is huge so the clients will confront the problem when vide are downloading it from website. This issue can lead client to exit the movie clip.A short movie clip displays a person doing some actions to the user shown in figure(15), then a group of sentences describe different actions shown to the user.

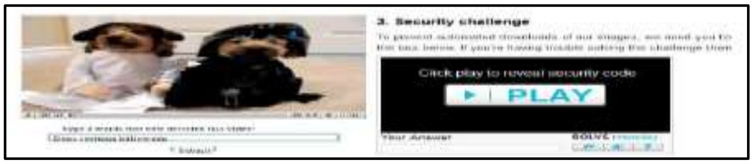


Figure15: Video CAPTCHA

D.CAPTCHA based on a puzzle: The client must solve a conundrum that depicts on presenting lumps of images and requesting that the user consolidates the pieces or recognize a particular piece of the picture shown in figure (16), [20]. It consists of several types:-

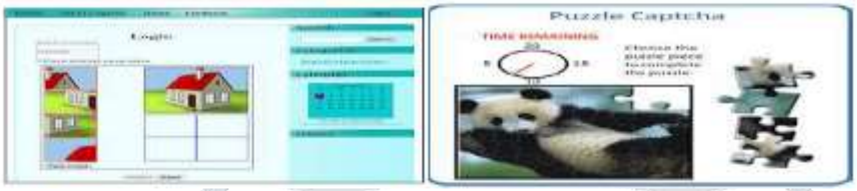


Figure 16: Puzzle CAPTCHA

1) *CAPTCHA Star*: Based on human cognitive ability to recognize specific shapes, it prompts the user with some stars into a square. The star's position changes according to the position of the cursor. The user must move the cursor in the drawable space until the shapes are recognized by the aggregated stars. Shown in figure (17).

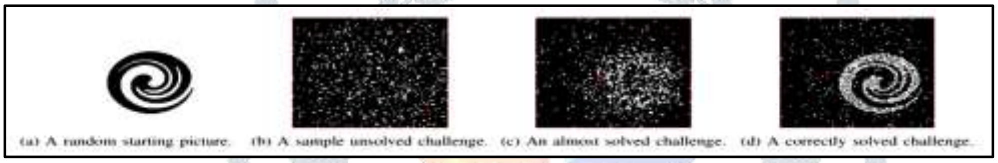
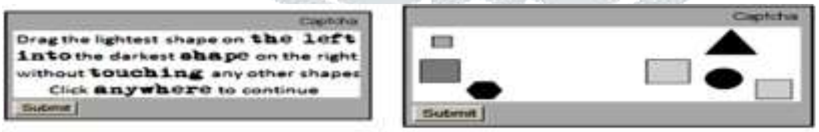

(a) A random starting picture. (b) A sample unsolved challenge. (c) An almost solved challenge. (d) A correctly solved challenge.

Figure 17: CAPTCHA Star

2) *DND & DDIM CAPTCHA*: Drag and Drop CAPTCHA. DND is developed in [Desai 2009]. The User is asked to drag every letter of a specific word that was displayed in distorted nature and drop it in the right position of this character.

3) *Tap CAPTCHA*: The main idea of design Tap CAPTCHA is structured based on a hybrid challenge that merges two puzzles shown in figure (18): text recognition puzzle and shape motion puzzle [21].

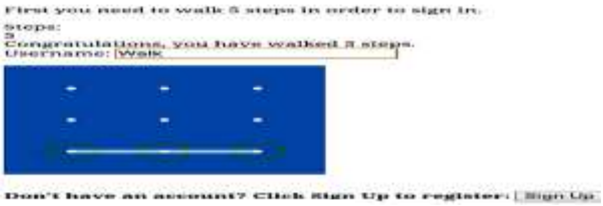


Drag the lightest shape on the left into the darkest shape on the right without touching any other shapes Click anywhere to continue

(a) TapCHA Instruction (Phase 1) (b) TapCHA Motion (Phase 2)

Figure 18: Tap CAPTCHA

4) *M CAPTCHA*: Known as Mobile CAPTCHA a new Human Interactive Proof approach (HIP) blocks Bot by asking the user to draw a randomly generated pattern as a graph as illustrated in figure (19). It developed to use in touch screens such as smart mobile phones or tablets [22].


First you need to walk 5 steps in order to sign in.

Steps:
5
Congratulations, you have walked 5 steps.
Username: Walk

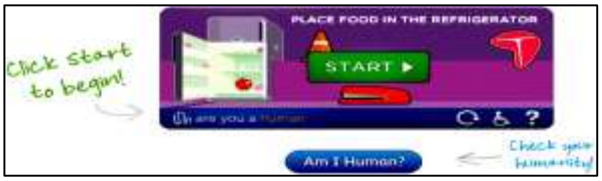
Don't have an account? Click Sign Up to register: Sign Up

Figure 19: M CAPTCHA

D. *CAPTCHA based on game:* Researcher Design and develop a novel CAPTCHA approaches that depend on compact games to verify human interaction on web sites. Consist of several types including the following:

1) *Play Thru CAPTCHAs*: Designing a new CAPTCHA to be simpler and more fun rather than any type of CAPTCHA. It's called Dynamic cognitive game (DCG) as illustrated in figure (20). It challenges the user to solve a simple piece of the game that appear through an image [23].

Figure 20: Play Thu CAPTCHA



2) *Fun CAPTCAs*: It's called Tick Tack. The test appears to the user as a set of arrangement and he asked to get the number of x in a row on each one of the presented arrangements as illustrated in figure (21). His selection is sent to the server and verified to ensure the submitted solution is from human or bot [23].

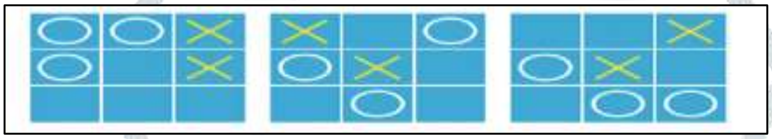


Figure 21: Fun CAPTCHA

3) *GISCHA*: Based on semantic CAPTCHA which is designed for portable and handset devices [Yang et al 2013]. The method of GISCHA can be discussed through using a rolling ball that moves on a two colored squared Surface, and a destination hall with different shapes as illustrated in figure (22). The user's ability for moving the ball to the destination slot framed as a circle although it's so difficult for the computer program to solve and recognize the meaning of rolling ball [24].

III. Compering between different CAPTCHA types

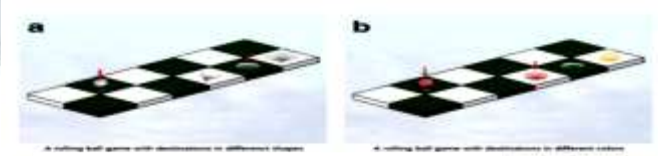


Figure 22: GISCHA CAPTCHA

Most common CAPTCHAS use on character acknowledgments that means it is based on text. However, CAPTCHA based on the text has low security comparing with different types of other CAPTCHAs. Comparison between different CAPTCHA in Table 1.

TABLE 1 : COMPARISON BETWEEN DIFFERENT CAPTCHA

Criteria Type	security	usability
CAPTCHA Based on text	low	Middle
CAPTCHA Based on image	High	High
CAPTCHA Based on audio / video	Middle	Middle

- CAPTCHA based on text: Some difficulty appear to the user for entering the correct character. Some reasons that lead the client to distinguish the correct character include using different lines, shapes, various fonts, font size variation.
- CAPTCHA based on image: OCR techniques used to broken it. The users that have color blindness will face some trouble.
- CAPTCHA based on video: The content of files is very huge , the speed of displaying video, etc.

- CAPTCHA based on audio: The availability of this system only in English. Hence it doesn't work for a deaf person or a foreign language speaker.
- CAPTCHA based on puzzle: The client cannot easily understand the puzzle. It is considered as a waste of time.

IV. Attack Models and Breaking Techniques

Attack methods: Different attack methods for various CAPTCHAs have various strategies as illustrated in figure 23.

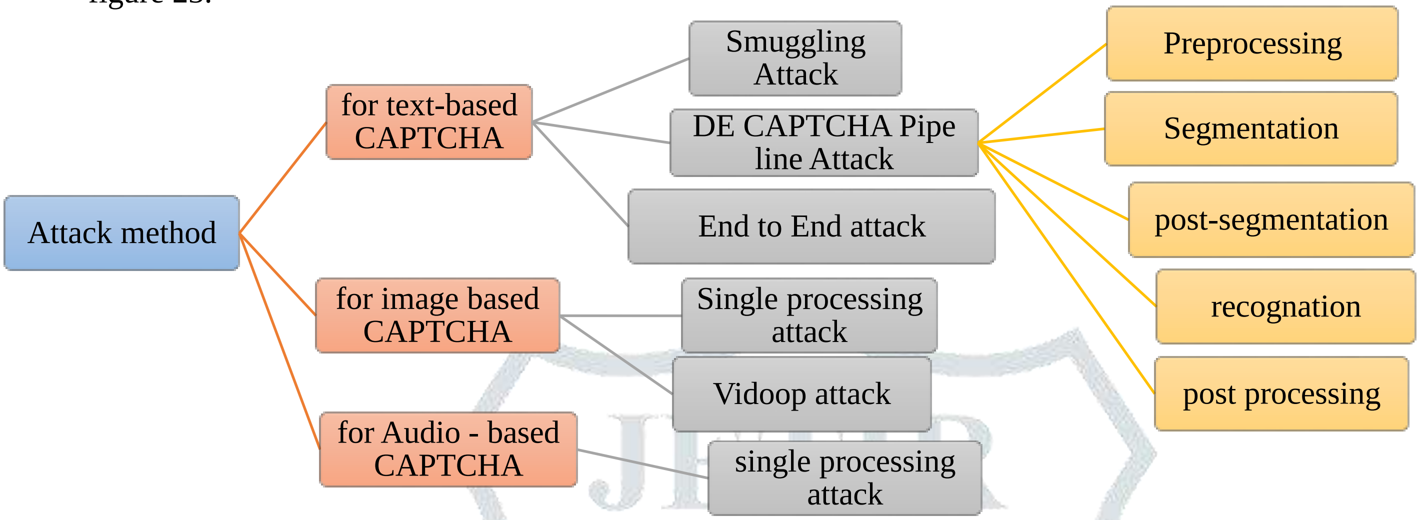


Figure 23: framework of breaking CAPTCHA

1) *Brute Force Attacks*: The Common attack used when the CAPTCHA test based on a limited number of solutions, then, the sponge can use the sensitivity information to automatically attack CAPTCHA details by trying answers at random or according to a selected sequence [25].
2) *Signal Processing Attacks:* Common attacks in the image and audio-based CAPTCHAs. Using chaos, noise and disruption that are used to fuzzy and disorganize captcha based on image and sound are possible tasks For machines to do, but the attacker can solve Image CAPTCHAs by removing the noise and distortion using Optical Character Recognition (OCR) technique or via mathematical heuristics and machine learning algorithms also besides, he/she can break Audio CAPTCHA using some machine learning algorithms, for example, Ada Boost, Supporting for Vector Machine/, and (K-NN) which mean K-Nearest Neighbor [26] to recognize the pronounced characters within noisy voice Environment [27].
3) *Smuggling Attack*: it is used when the attacker injects mocked CAPTCHA the Challenges are replaying an identifying online task automatically for example mail registration, Login Social Application such as Facebook applications, commenting on or sending message/photo or Sending friend requests. The behavior of this attack is controlled by the attacker. The script starts by the user performs an online task at first that the attacker wishes to postpone the mal-ware on the victim's host intercepts the request and locally stores all information [25].
4) *DE-CAPTCHA Pipeline Attack*: it is used to break text-based CAPTCHA [28, 29] and consists of five stages that are performed on a specific text CAPTCHA to solve it.

4.1 Preprocessing: It can be negligent if the image is noise-free. Removing background by using different technique and CAPTCHA is appeared in white and black and saved in binary matrix. The transformation of captcha into binary matrix makes the DE CAPTCHA pipeline easier for implementation. As shown in figure (21), [27, 28].

4.2 Segmentation: cutting of CAPTCHAs by using different segmentation method, such as CFS (Color Filling Segmentation) which based on a paint bucket flood filling algorithm in its work . CFS is a default segmentation method so it allows to segment of the CAPTCHA words however they are tilted and over-lapped [28, 30].

4.3 Post-Segmentation: The segments that are resulted in the previous stage are processed individually for making the recognition easier. The segments magnitude are always normalized [28, 31].

4.4 *Recognition*: By using training mode to learn the classifier what the character like after the CAPTCHA has been segmented. In the testing mode, using classifiers in predictive mode to detect each letters individually [31].

4.5 *Post-processing*:The classifier's output is getbetter and enhancing potentially by using spell checking techniques to raise the accuracy and regulation of the Output.

5) *Vidoop CAPTCHA Attack*: Special kind of image-based CAPTCHA attack. It uses images of objects, animals, people or landscapes, instead of distorted text, to differentiate humans from a computer program. The challenge of an image that consists of several pictures representing different categories. Every picture associated with a letter that is established in it. To pass the challenge, asking the user to report the letters corresponding to a list of required categories [32].

6) *Teabag 3D Attack*: Its design is based on three-dimension space such type of 3D CAPTCHA is characterized with some properties: The 3D-CAPTCHA test displayed on a grid in 3D space as depicted presented as four letters using Only Upper case and digits .Characters are very close to each other Appears to be produced from slightly various viewpoints. There are small difference in grid direction and the shape of background cells between the presented challenges to the attack model for breaking Teabag 3D-CAPTCHA can be described into four phases [33].

IV. **C**aptchas' strength and usability

CAPTCHA should be designed according to a set of robustness and security considerations.To design a strong and secure text and image-based CAPTCHA system, you must be very tough against segmentation algorithms and recognition algorithms. Clarification is given by randomlly the length of CAPTCHA: Don't use fixed-length while designing the CAPTCHA test. Randomize character/image size: a good approach to design difficult CAPTCHA. In-text CAPTCHA, you must use several font types and several font sizes for reducing classifier learnability and accuracy. For Image CAPTCHA, you must use several colors, several confused and distorted pictures, and several pictures size randomly for misleading the classifier algorithm.Waving of the CAPTCHA: Waving CAPTCHA improvement the difficulty of finding segment points in case of collapsing and helps to relive the dangers of the spammer to remove the added lines. Complex Background: using a complex background that contains dots, shapes and lines confuse the actual text and block the spammer from segment characters. Never Use Complex Charset: using a larger charset somewhat effect the classifier's learnability and accuracy, but, the charset of CAPTCHA.Adding Noise: Mechanism used to confuse the segmentation attacks by adding random noise on the image or text CAPTCHA. Large cross streaks: Using streaks that are not wide as the character segments give an attacker a robust discriminator and make the streak. Collapsing: Using by deleting the space between characters or by tilting them is a recommended principle to prevent the segmentation attack. Curser, Clicking, Dragging and Dropping techniques: Solving CAPTCHA especially Cognitive Puzzle-based CAPTCHA using curser Motion, clicking and Dragging and drop or move objects or is an easy and Usable task for a human, but designing CAPTCHAs using these techniques Makes breaking CAPTCHA is a very difficult problem for the bot attacks such As ad hoc attacks.Simple Game: Designing CAPTCHA based on playing funny Simple game is a useful technique to make the CAPTCHA Test more resistant against automated attacks.

V. Conclusion

This paper has introduced the conception and history of CAPTCHAs, CAPTCHA applications and describing the various CAPTCHA approaches based on text, images, voice, video, and puzzle. Although besides, discussing the strength, weakness of each category the most important features for analysis and the study of the test, which are usability. In addition, it discuss of the varition between the various schemes. Moreover, meaningful suggestions are proposed for designers. The CAPTCHA technology works on the various algorithms for the enhancement and also working on the above-mentioned issues over time. As a final point, the paper conducts a comprehensive survey of different existing techniques of CAPTCHA systems and how they are used for providing authentication.

References

[1] http://www.captcha.net/ visited 20 july2020

[2] M.Chew and J.DTygar,”Image Recognition CAPTCHAS”,In Proceeding of the 7 international information security conference(2004), Springer

[3] C. E. Dunn and , P. S. P. Wang, “Character segmentation techniques for handwritten text-a survey,” In Pattern Recognition, 1992. Vol. II. Conference B: Pattern Recognition Methodology and Systems, Proceedings., 11th IAPR International Conference , pp. 577-580.

[4] Chen, Jun, et al. "A Survey on Breaking Technique of Text-Based CAPTCHA. " *Security and Communication Networks* 2017 (2017).

[5] Usmani, Atiya, et al. "New Text-Based User Authentication Scheme Using CAPTCHA." Information and Communication Technology for Competitive Strategies. Springer, Singapore, 2019. 313-322.

[6] Moy, Gabriel, et al. "Distortion estimation techniques in solving visual CAPTCHAs." Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. CVPR 2004.. Vol. 2. IEEE, 2004.

[7] Bansal, A., Garg, D., Gupta, A., & Gupta, A. (2008). Breaking a Visual CAPTCHA: A Novel Approach using HMM..

[8] Al-Sudani, Wesam, et al. "Protection through multimedia CAPTCHAs." Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia. ACM, 2010.

[9] Chow, Richard, et al. "Making captchas clickable." Proceedings of the 9th workshop on Mobile computing systems and applications. ACM, 2008.

[10] Lorenzi, David, et al. "Towards designing robust CAPTCHAs." Journal of Computer Security Preprint (2018): 1-30.

[11] Anju Bala and Baljit Singh Saini, “A Review of Bot Protection using CAPTCHA for Web Security,”(IOSR-JCE) IOSR Journal of Computer Engineering, Volume 8, Issue 6 (Jan. - Feb. 2013), 36- 42.

[12] R. ur Rahman, D. S. Tomar, and S. Das, “Dynamic image based CAPTCHA,” in Proceedings of the International conference on Communication System and Network (CSNT), Rajkot, India, 2012, pp. 90 – 94.

[13] D. Lorenzi, J. Vaidya, E. Uzun, S. Sural, and V. Atluri, “Attacking image besed CAPTCHAs using image recognition recognition techniques,” in Proceeding of the 8th International Conference on Information Systems Security (ICISS), Guwahati, India, 2012, pp. 327-342.

[14] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

[15] Gao, H., Lei, L., Zhou, X., Li, J., & Liu, X. (2015, October). The robustness of face-based CAPTCHAs. In Computer and Information
Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on (pp. 2248-2255). IEEE.

[16] Brodić, Darko, and Alessia Amelio. "Direction of CAPTCHA." *The CAPTCHA: Perspectives and Challenges*. Springer, Cham, 2020. 33-53

[17] Usuzaki, Shotaro, et al. "Interactive Video CAPTCHA for Better Resistance to Automated Attack." 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2018.

[18] Choi, Jusop, et al. "POSTER: I Can't Hear This Because I Am Human: A Novel Design of Audio CAPTCHA System." Proceedings of the 2018 on Asia Conference on Computer and Communications Security. ACM, 2018.

[19]Shirali-shahreza, M. & Shirali-shahreza, S. (2008), "Motion CAPTCHA", Human System Interactions, 2008 Conference on, Krakow, 2008, vol., no. pp. 142-1044.

[20] Siripitakchai, Apichai, Suphakant Phimoltares, and Atchara Mahaweerawat. "EYE-CAPTCHA: An enhanced CAPTCHA using eye movement." 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017.

[21] Agrawal, Vani, et al. "Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication." *OTP and User Behaviour Authentication (January 6, 2019)* (2019).

[22] Kaur, Kulwinder, and David M. Cook. "Haptic Alternatives for Mobile Device Authentication by Older Technology Users." International Conference on Computing and Information Technology. Springer, Cham, 2018.

[23] Greene, Mecheal. Large scale captcha survey. Diss. University of Delaware, 2018.

[24] Chow, Yang-Wai, Willy Susilo, and Pairat Thorncharoensri. "CAPTCHA Design and Security Issues." *Advances in Cyber Security: Principles, Techniques, and Applications*. Springer, Singapore, 2019. 69-92.

[25] Doshi, Y., Sangani, A., Kanani, P., & Padole, M. An insight into CAPTCHA. 2017

[26] R. Hussain, H. Gao, and R. A. Shaikh, "Segmentation of connected characters in text-based CAPTCHAs for intelligent character recognition," Multimedia Tools and Applications, pp. 1–15, 2016.

[27] Gao, Haichang, et al. "Research on the security of microsoft's two-layer captcha." IEEE Transactions on Information Forensics and Security 12.7 (2017): 1671 1685.

[28] Rathour, Navjot, et al. "A Cross Correlation Approach for Breaking of Text CAPTCHA." 2018 International Conference on Intelligent Circuits and Systems (ICICS). IEEE, 2018.

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

[30] Zhou, Yuan, et al. "Breaking google reCaptcha V2." Journal of Computing Sciences in Colleges 34.1 (2018): 126-136.

[31] Zhang, Lili, et al. "Captcha automatic segmentation and recognition based on improved vertical projection." 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). IEEE, 2017.

[32] Michele,M, and Jacob, J, 2009, . "Breaking an Image based CAPTCHA." Technical Paper submitted to the Department of Computer Science, Columbia University, USA, Springer term, Available at www. cs. columbia. edu/ mmerler/project/FinalReport. Pdf

[33] Nguyen,V, D, Chow,T,W and Susilo,W, 2012, "Breaking a 3D-based CAPTCHA scheme. In the proceedings of the international Conference in Information Security and Cryptology-ICISC 2011, pp. 391-405). Springer

[34] Raman, Jayalakshmi, Karthikeyan Umapathy, and Haiyan Huang. "SECURITY AND USER EXPERIENCE: A HOLISTIC MODEL FOR CAPTCHA USABILITY ISSUES." (2018).

[35] Gao, H., Wang, W., Qi, J., Wang, X., Liu, X., & Yan, J. (2013,November). The robustness of hollow CAPTCHAs. In Proceedings of
the 2013 ACM SIGSAC conference on Computer & communications security (pp. 1075-1086). ACM.

[36] A. S. E. Ahmad, J. Yan, and M. Tayara. The robustness of google captchas. Technical report, Newcastle University, 2011.

[37] Gao, H., Tang, M., Liu, Y., Zhang, P., & Liu, X. (2017). Research on the Security of Microsoft's Two-Layer Captcha. IEEE Transactions on Information Forensics and Security, 12(7), 1671-1685

[38] J.malik and G.mori, "Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA, "Conference on Computer Vision and Pattern Recognition, vol-1,134-141, June 2003.