

A Brief Review on Text and Image CAPTCHA

Mahuya Sasmal¹, Palash Ray¹, Mrinmoy Sen¹, Rajesh Mukherjee¹, Shaon Bandyopadhyay¹

1(Computer Science & Engineering, Haldia Institute of Technology, India)

ABSTRACT

Nowadays, security is a major concern and has garnered foremost attention in recent years as a result of the Internet's evident impact on all facets of human life. To provide an appropriate level of security, the Completely Automated Public Turing Test to Tell Computer and Human Apart, or simply CAPTCHA, has been designed for circumstances when bots must be prevented from performing a specific action, such as signing up and downloading. At the same time, it should be designed in such a way that people can execute the same action. Despite its many benefits, there are several major concerns about security, usability, and accessibility that make its use contentious. In this work, we attempted to provide a comprehensive analysis of many features and the state-of-the-art of CAPTCHA in general, as well as its alternatives in particular, to assist researchers in focusing on specific concerns to propose new solutions and ideas. With the advancement of CAPTCHA development, various schemes of text-based and image-based CAPTCHAs have been described and compared. Furthermore, numerous proposed methods are used to classify and evaluate various sorts of CAPTCHA alternatives. This analysis could be useful in future studies aimed at developing new strategies for addressing current flaws.

Keywords –BOT, CAPTCHA, Security, Usability, Attack

I. INTRODUCTION

Using the Internet for various purposes has become a daily activity for practically all individuals all over the world, who use it to research, shop, use programs, and do a variety of other things. Because there are many unfair users like attackers, hackers, and spammers who intend to have unauthorized access to these applications (information), spam, hack accounts, and do other abuses, the importance of maintaining security attracts more attention as the amount of information and applications grows exponentially. As a result, the crucial importance of (information) security in securing applications and their most valuable assets, namely their private information, has been highlighted more than ever before [1]. The security domain is quite vast, and it should be able to control access, protect programs, detect intrusions, restore damage, and block unauthorized users, among other things. Several policies, processes, and instruments have been proposed to deal with the growing number of security threats [2]. The Completely Automatic Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), which was first introduced more than a decade ago, is now widely recognized as a useful security technique [3]. Several distinct variants of CAPTCHA have been proposed and used for diverse applications in the years since its development. On the other hand, because of the issues and shortcomings of CAPTCHAs, efforts have been made to provide alternate ways.

The four key characteristics [4] that every CAPTCHA system must have are:

1. Secure: The tests generated by the program must be difficult to solve by machines using any algorithm.
2. Automated: The software (computer programs) must be able to create and grade the test.
3. Open: The underlying algorithms and databases must be made public.
4. Usable: These tests should be able to be completed by humans in a reasonable amount of time.

Von et al. [3, 5] proposed various effective CAPTCHA techniques based on hard Artificial Intelligence (AI) issues i.e., challenges that most humans can readily answer but that computer programs cannot. The majority of CAPTCHA techniques proposed in the literature take this approach, utilizing various features such as character recognition,

image understanding, and speech recognition to generate challenges that effectively stop automated bots. However, thanks to recent advances in artificial intelligence (AI) in general and computer vision (CV) in particular, automated systems are now substantially better at performing such challenges. As a result, as shown in References, practically all previous CAPTCHA systems have been broken [6, 7, 8]. Furthermore, contrary to Von et al. assumptions, not all proposed attacks in the literature seek to address the underlying AI problem that these CAPTCHAs are founded on to defeat them. Instead, some of them try to get around the AI problem by exploiting flaws in the architecture of a particular CAPTCHA technique [9, 10]; these are named Side-channel attacks. Designing successful and user-friendly CAPTCHA methods based on difficult AI challenges has become increasingly difficult over time. As a result, a new generation of systems based on behavioral analysis and sensor readings has emerged.

In 2014, Google revealed that today's Artificial Intelligence technology can resolve even the most challenging variety of distorted text with 99.8% accuracy [11], and switched to a behavioral analysis-based CAPTCHA system, which is now the market's main CAPTCHA method. Even though many scholarly publications have demonstrated the vulnerability of classic CAPTCHA schemes, many researchers continue to focus on breaking traditional CAPTCHA schemes and evaluating their security and usability [12, 13, 14], while disregarding emerging CAPTCHA methods that have yet to be cracked. Recent publications in the literature, however, do not include these new CAPTCHA systems in their reviews or security assessments [15, 16, 17].

Motivation and Contribution: Unlike previous CAPTCHA surveys [16, 18, 19], we give an up-to-date comprehensive CAPTCHA survey in this paper, which includes both traditional and newer CAPTCHA schemes, such as those based on neural style transfer technique. We have made a detail analysis of test-based and image-based CAPTCHA schemes. In addition, we review and analyze all of the literature on the security evaluation of existing CAPTCHA systems and proposed strategies to break them, highlighting the flaws of various CAPTCHA schemes. This work also allows us to create a security chronology for 25 CAPTCHA schemes, which shows the invention and breaking year, as well as the breaking percentage. This timeline not only shows the progress of CAPTCHA over two decades, but also shows which CAPTCHA mechanisms are broken and which ones should be investigated further. It also explains the latest design trends in CAPTCHA schemes. The main contribution of this article is to review, classify, and compare various forms of text-based and image-based CAPTCHAs and their alternatives to create a overview for future research. This study sought to serve as a reference point for studies on CAPTCHA and alternative solutions that have been undertaken thus far, to lead future research activities toward developing more efficient and applicable cases.

Structure: The remainder of this article is structured in the following manner. In Section 2, we categorize conventional and recently created CAPTCHA approaches in depth. Section 3 goes through the main attacks on the CAPTCHA systems discussed in Section 2. Section 4 focuses on unresolved issues, roadblocks, and future work opportunities. Finally, based on all of the analysis and comparisons in Section 5, we draw some conclusions.

II. CAPTCHA CLASSIFICATION AND SURVEY

Till now text-based, image-based, audio-based, video-based, math-based, and game-based CAPTCHA are the six types of CAPTCHA that have been traditionally classified in the literature. However, we believe that this categorization is insufficient because it excludes the newer CAPTCHA algorithms. The most extensively used CAPTCHA systems today, for example, do not fit under this category (e.g., reCAPTCHA V2, V3, and Geetest).

Even the most recent literature reviews and evaluations use this imperfect categorization to examine and evaluate the security of existing CAPTCHA solutions. We proposed a more comprehensive taxonomy capable of capturing the new emergent CAPTCHA methods as a result of the disparity between the relevant literature and the real state-of-the-art. We have proposed that recent CAPTCHA schemes may be split into 10 categories like text-based, image-based, audio-based, video-based, game-based, slider-based, behavior-based, sensor-based, and CAPTCHAs for liveliness detection in authentication systems.

A. Text-based CAPTCHAs

The most common type of CAPTCHA is text-based. In these systems, a text (for example, a series of random letters or phrases) is distorted and shown to the user as an image. Language dependence is a key shortcoming of this type of CAPTCHA technique when words are employed. The user is next asked to enter the text that appears in the image in order to pass the exam. The basic idea is that humans can readily understand the deformed text, while bots utilizing OCR algorithms have a difficult time doing so. We categorized the variety of text-based CAPTCHAs according to the varied representations of the challenge text because the interaction necessary to solve the CAPTCHA (i.e., the input of a text) is the same in practically all text-based CAPTCHAs. As a result, three sub-categories were identified: (1) 2D text-based, (2) 3D text-based and (3) Animated text-based. Table-1 lists all of the text-based CAPTCHA methods that were investigated, as well as a relevant graphical representation and a thorough explanation of the challenge.

i. 2D Text-based CAPTCHA: Andrei Broder and his colleagues at the DEC Systems Research Center created the 2D text-based CAPTCHA method in 1997. The AltaVista website employed a similar strategy to prohibit bots attempting to affect the ranking of a group of sites on the AltaVista search engine in the same year [20].

In 2000, Von Ahn and Blum created Gimpy CAPTCHA and EZ-Gimpy [21] in conjunction with Yahoo to prevent spammers from placing dangerous adverts in chat rooms and to ensure that free accounts were only given to actual people. Gimpy works by taking a few words from the dictionary and misshaping, corrupting, or disfiguring them. To gain access to the secured services, the user must pass the gimpy test. Dictionary attacks using a restricted number of words have broken the Gimpy CAPTCHA challenge. The Gimpy CAPTCHA technique requires users to type properly at least three out of seven words chosen at random from a dictionary. EZ-Gimpy is a condensed version of Gimpy that displays only one random word from the dictionary. However, numerous fonts, backdrop grids, and gradients are used to transform the word into an image. Additionally, blurring, noise, and distortion effects on letters are used to change the image.

Monica Chew (UC Berkeley) and Henry Baird (PARC) of the Palo Alto Research Centre created the Baffle text [22]. Words that are not part of the British vocabulary are presented to the user in this sort of CAPTCHA. These words are converted to their image by printing out the image and scanning it back in, or by using the threshold approach to convert the image from color to black and white and back again. This modifies the grayscale and adds noise to the picture at random. Baffle text's goal is to reduce the tiny dictionary problem by employing nonsensical words that a person can answer using intuition but that computer programs or bot can't.

Yahoo! debuted their second generation CAPTCHA in August 2004. Its distinguishing features include the use of a string of characters rather than English words, the use of solely black and white hues, the use of both letters and numerals, and the presence of linked lines and arcs as clutter. Just image warping for character distortion, having only two colors (one for foreground and the other for background), positioning characters near to each other, and following a curved baseline are included in CAPTCHA, which is utilized by Gmail.com [24]. Chow et al. proposed the concept of clickable CAPTCHA [23] to increase the usability of text-based CAPTCHAs. Multiple textual CAPTCHA challenges are combined into a grid of clickable CAPTCHAs in their method (e.g., a 3×4 grid). The user must select the grid components that correspond to the challenge's requirements. The detection of English terms amid non-English words in the grid, for example, can be a difficult task. Such a task has linguistic ramifications.

Megaupload.com, a major website for downloading and uploading files, developed a CAPTCHA system in 2010 that was based on a new segmentation-resistant technology that differed from Microsoft, Google, or Yahoo. This novel technique works by combining overlapping characters with the "Gestalt Perception" concept, which hides some of the information of the characters where they intersect. According to the Gestalt Perception principle, humans can mentally rebuild individual characters, but computer algorithms struggle with this job.

ReCAPTCHA chooses its words from old printed materials or scanned text that OCR algorithms can't read. This method not only improves the security of the CAPTCHA but also allows human users' solutions to be utilized to interpret the non-digital text. This CAPTCHA presents the user with two words: one with an unknown response and another 'control' word with a known answer. If the user successfully inputs the control word, she is presumed to be

human, and her response to the other word is regarded as accurate. A control word is created when a certain amount of users' replies to an unknown word match.

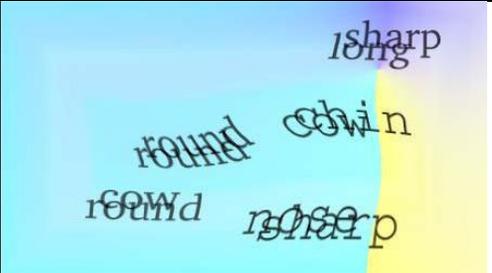
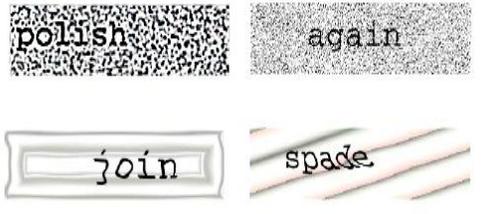
ii. 3D Text-based CAPTCHA:3D text-based CAPTCHA schemes make use of the fact that humans can readily detect sequences of 3D characters but computer programs or bots can't; as a result, they're a step up over 2D text-based CAPTCHA methods. The Teabag-3D, built by the OCR Research Team to discover the flaws in 2D text-based CAPTCHA methods and suggest a fresh and more secure CAPTCHA scheme, is one of the initial ideas. The picture Teabag-3D is made up of a 3D design with textual characters. The scientists proved that humans could easily detect the 3D text using the new CAPTCHA approach, but automated systems failed to do so. Super CAPTCHA [27] and 3DCAPTCHA [28], for example, are 3D text-based CAPTCHA methods based on the same assumptions and utilized on a variety of websites. Super CAPTCHA, for example, has been accessible as a WordPress.org plug-in since 2013. Imsamai and Phimoltares designed a new 3D CAPTCHA strategy [29] that entices automated recognition systems by presenting a sequence of 3D alphanumeric characters and adding a variety of effects. Text rotation, text overlapping, noise addition, scaling, font variation, special characters, and various backdrop textures are among the effects available.

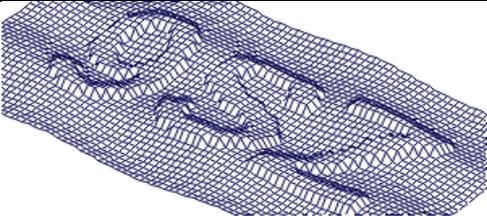
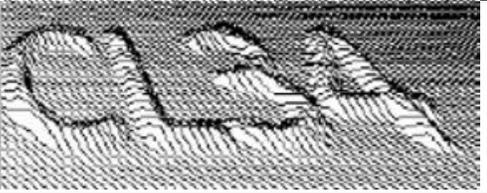
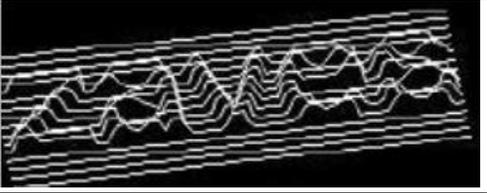
iii. Animated Text-based CAPTCHA:Text-based schemes are enhanced by the addition of a temporal dimension in animated-CAPTCHAs. In detail, various CAPTCHA approaches animate the challenge's textual content in a brief clip, making automated system extraction more difficult. In 2006, Fischer and Herfet proposed one of the first animated CAPTCHA concepts [30]. The idea behind their CAPTCHA method is to project the text into a deforming dynamic surface. Naumann et al. proposed an animated CAPTCHA in 2009 [31], based on the belief that the human visual system likes to group moving items. As a result, the scientists devised a novel CAPTCHA technique in which letters are placed on a noisy background. When the letters move, the users can tell the difference between the text and the backdrop.

Cui et al. suggested an animated CAPTCHA [32] in which the user may only see the correct characters in the animation while they move. They also created the "zero-knowledge per frame" idea, which assures that no information is leaked in each frame of the animation to solve the CAPTCHA challenge. In 2010, the Creo Group released HelloCAPTCHA, [33] an animated CAPTCHA that can be downloaded for free from the creators' website. The HelloCAPTCHA challenge is made up of a series of six characters displayed in an animated GIF image. The figures change position and orientation in certain problems, and they are not all visible at the same time in others. The objective behind such a system is to disperse the data across numerous animation frames to avoid a single-frame OCR attack.

Another animated CAPTCHA method is NuCaptcha [34]. The challenge comprises a movie with white text scrolling on a dynamic background, followed by three random red characters moving across it. To solve the CAPTCHA, the user must input the moving red characters. CAPTCHAs with the name "Dracon" are animated visual Flash CAPTCHAs [35]. The task is recognizing five characters that are shown in fixed positions but have been randomly changed using fade and blur effects. Random falling bars in the front or little text characters in the background add noise to the animation.

Scheme	Year	Type	Database	Sample	Description
--------	------	------	----------	--------	-------------

GIMPY [21]	2000	2D	561 words		Recognize three of seven words chosen at random from a dictionary.
EZ-GIMPY [21]	2000	2D	411 words		In a distorted picture, recognize one English word.
Baffle Text [22]	2003	2D	26^8 words		With different masking applied, identifying a comprehensible string of characters.
Google [24]	2006	2D	4 to 15 letters (a-z, A-Z,0-9), 52^6 words		Recognize characters that are squeezed into a little space.
Clickable CAPTCHA [23]	2008	2D	Infinite		To find the English words in the grid and amid the non-English terms.
Yahoo [24]	2004	2D	25^4 to 52^6 words		Find the characters with arbitrary lines.
ReCAPTCHA A [25]	2008	2D	Infinite		To find the distorted text scanned from old books

Teabag-3D[26]	2006	3D	24^5 to 62^6 words		To find characters from a 3D grid.
3D-CAPTCHA [28]	2006	3D	Alphanumeric		To find sequence of 3D characters.
Super CAPTCHA [27]	2013	3D	Alphanumeric		To find sequence of 3D characters.
Dracon CAPTCHA [35]	2006	Animated	(a-z,A_Z)		Recognize bur and faded animated characters
HelloCAPTCHA [33]	2010	Animated	Alphanumeric		To find an arrangement of characters
NuCAPTCHA[34]	2010	Animated	(a-z,A_Z)		Insert last colored characters

B. Image-based CAPTCHAs:In the machine learning and the deep learning era, a huge number of textCAPTCHAs were effectively cracked. Therefore, researchers made a decent attempt to design hard AI problems that are much tougher than optical characterrecognition. By using the concept of object detection, target recognition, andscene understanding image-based CAPTCHA's are used to distinguish humanand malicious bots. Most image CAPTCHAs needn't bother with text inputs;consequently, they are appropriate to execute on various touch devices with better convenience [36].

In 1970, Bongardfirst introduce a concept of image CAPTCHA namedBongo, which is based on visual pattern recognition problems. Some geometric shapes are displayed equally in two blocks are placed on both the right andleft sides of the screen. The properties of two blocks can differ in size, line thickness, etc. Next another four shapes are displayed and the user is asked to selectthe correct suitable block from the left side or right side. The user passes thetest if they correctly determine the side to which all four shapes belong.Chew and Tygar [37] proposed “The naming CAPTCHA”, “Distinguishing CAPTCHA” and “Anomaly CAPTCHA” which are the initial attempts

of image-based CAPTCHA techniques. In these proposed methods, users are asked to find the similarity or the dissimilarity from a set of images collected from a Google image search. The user needs to submit the correct label of the image to pass the challenge. These schemes suffer from misspelling, mislabeling from users, synonym words, and polysemy words. Baird and Bentley proposed Implicit CAPTCHA [38] in 2005, where the user has asked to click on the desired position or a specific word on an image. In 2007, Shirali-Shahreza proposed Collage CAPTCHA [39], where various object images are merged into a single image, and the user has asked to select certain objects. Collage CAPTCHA requires a database of labeled object images, which are scattered and rotated randomly on the background image. Object segmentation and recognition based attacks are common in case of Collage CAPTCHA.

To design an image-based CAPTCHA, Rui et al. have used a complex 2D face model which has human face recognition abilities named ARTIFACIAL [40]. A human face along with face-like noises is imposed on a cluttered background and the user has asked to search the human face and other facial feature points. ARTIFACIAL is successfully cracked by Zhu et al. [41] with a success rate of 18.0% and an average time of 1.47 sec. Another famous CAPTCHA named ASSIRA [42] was proposed in 2007, where the user needs to recognize and select the images of cats and from an image grid, which contains images of cats and dogs. Instead of labeling the images, and maintaining the database's scalability and dynamic updating, ASSIRA leverages image data from Petfinder's website. ASSIRA employs multiple choice questions to broaden the solution space and thus improve security. Golle et al. [16] use image recognition technology to perform an attack on ASSIRA, which can distinguish cat and dog images in ASSIRA by just integrating color and textural features with a recognition rate of 10.3%. Datta et al. [43] proposed the "IMAGINATION" system, which is an image-based CAPTCHA creation method. The goal of the CAPTCHA system is to exploit people's imaginations by allowing them to interpret images among distortion and clutter background. The system posed a challenge that consisted of two processes: a click and an annotation procedure. The user has provided a composite image made up of eight tiled images during the click process. To annotate an image, the user has to click towards the geometric center of the image. The user has presented with a selection of word options after the selected image was distorted in a controlled manner. Next, the user has to choose the best word to describe the deformed image. IMAGINATION is a language-dependent CAPTCHA, and Zhu et al. [41] successfully attacked it with a success rate of 4.95 percent.

The core content of image semantics is an object's directionality. Based on the visual direction of an object, Gossweiler et al. [45] developed a CAPTCHA scheme named What's-Up CAPTCHA. The user has to determine the object's direction in the randomly rotated test image and then use the scroll bar to rotate the image object vertically. Banday et al. [54] further enhance What's Up CAPTCHA, by adding interference noise in the image and suggests the image-Flip CAPTCHA. SEMAGE [46] is a type of image CAPTCHA that works by matching semantic content of the object images. The user must first comprehend the content of each image before locating and selecting semantically related objects. Basso et al. [47] proposed "MosaHIP," in a mosaic-based technique of human computer interaction, to reduce text box input and increase CAPTCHA usability. Objects are scattered randomly in different positions of Mosaic images and overlaid with other image objects in "MosaHIP." The descriptive characters must be dragged and dropped onto the correct image objects by the users. reCAPTCHA, introduced by Google in 2007 [48], is a CAPTCHA technology that allows web hosts to differentiate between humans and bots for accessing the websites. It requires no text, image, audio, or video data to pass. It only takes one mouse click to tell the computer whether there is a human on the other end of the line. It's called reCAPTCHA. A checkbox is shown to the user, and he is instructed to simply click on it. The checkbox is a virtual checkbox, not just a regular checkbox. Google adds an invisible text space to the form and fills it with a one-of-a-kind value. This value serves as a check to see if the user is a bot or not. For the test, the value can be true or false. Furthermore, the latest version of Google's No CAPTCHA reCAPTCHA [49] increases the usability of image CAPTCHAs even further.

Though, developing image recognition technology [50] poses a threat to the security of an image CAPTCHA that is based on semantic content interpretation. For example, Sivakorn et al. [51] defeated Google's version of No CAPTCHA reCAPTCHA using deep learning technology, which has become popular in recent years. To enhance the security of CAPTCHA, Polakis et al. [52] developed an image selection and transformation method based on Facebook's social authentication to generate image CAPTCHAs [53]. In this scheme, human face images, which are

unclear, blocked, or from the back, are utilized as features to safeguard against image recognition attempts by bot programs. Based on existing knowledge, users can recognize their friends from these avatars.

To enhance image CAPTCHA security, new complex hard AI image processing challenges must be created. Osadchy also suggested an image-based CAPTCHA scheme named DeepCAPTCHA [55] based on adversarial noise, considering that deep learning technology has difficulties detecting adversarial examples. Adversarial noise offers strong security since it can successfully defend against frequently used image processing attacks. As a result, the adversarial examples with adversarial noise are nearly identical to the original image, implying that DeepCAPTCHA will be more usable than the current CAPTCHA with interfering noise.

Several Captchas based on human faces have also been tested. D'Souza et al. came up with the Avatar Captcha [56], which requires users to identify avatar faces from a series of 12 photos that include both human and avatar faces.

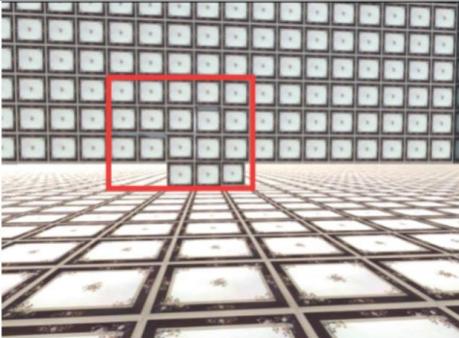
These images are taken from a database of human and avatar faces, and they are all transformed to gray-scale to prevent bots from using the color spectrum disparities between human and avatar images to crack the CAPTCHA. Cheung et al. [57] use Convolution Neural Network to break Avatar CAPTCHA effectively with a 99% success rate.

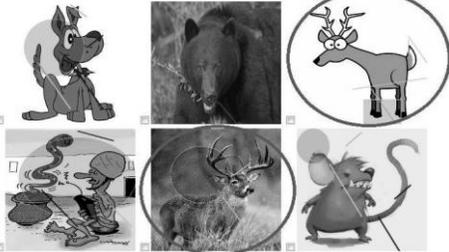
More face-based CAPTCHA schemes like FR-CAPTCHA [58] and FaceDCAPTCHA [59] are proposed by Goswami et al. In FR-CAPTCHA users must discover matching faces from a group of face images. The face images are blended over a complex background followed by rotation and noises. In FaceDCAPTCHA users must discern between genuine human faces and animated human faces from a group of human face images and animated face images. The human face pictures in FR-CAPTCHA and FaceDCAPTCHA are rotated, deformed, and blended with a cluttered background. Gao et al. have performed an attack on FR-CAPTCHA and FaceDCAPTCHA and achieved success rates of 23% and 48% respectively. Ray et al. [60] proposed FP-CAPTCHA (Face Point Captcha), which requires users to click on human face points such as the eye, nose, and mouth. A cluttered background is used to embed a group of eight real and fake face images, with adequate noises and patterns. The Captcha challenge will be solved if the users click on the proper face points (up to a specific tolerance level), otherwise discarded and a new CAPTCHA challenge will be generated.

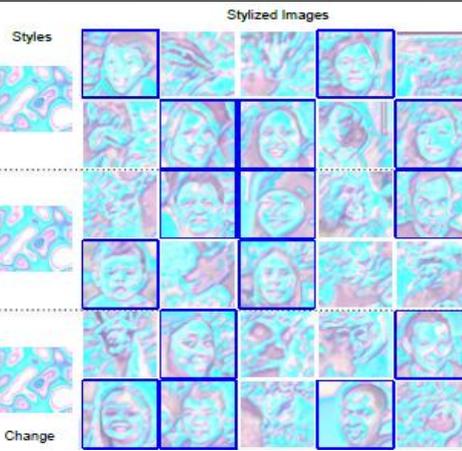
In 2017, Zhang et al. proposed CONSCHEME [61], where users are asked to count the number of cubes in order to pass the Captcha challenge. It is an interactive three-dimensional Captcha system that consists of a large number of cubes stacked in a three-dimensional space with the same stickers on the walls, ceiling, and floor. Zhang et al. also proposed DeRection [61] scheme, where visitors are requested to discover all the warped and distorted regions from a particular GIF image. Users can also request that the frame or image be changed as needed. In 2018, Bera et al. proposed a novel image-based CAPTCHA technique named HandCAPTCHA [62]. This CAPTCHA verification technique is based on hand pictures of humans. It allows a person to answer a CAPTCHA based on various images of hands that are automatically generated using a randomized combination of two actual and other fake hand photos. It also determines if the user is a human or a bot. Further, Bera et al. have improved HandCAPTCHA technique by a two-stage verification scheme [63]. The scheme performs human verification in two phases. Stage-1 determines whether a human or bot solves an IH-CAPTCHA. If the responder is a human, then stage-2 recognizes the real hand of a person who claims to have a valid identity using geometric features of the four fingers, except the thumb.

Tang et al. proposed SACaptcha [64] which is based on the neural style transfer technique. SACaptcha displays a synthetic image with a resolution of 560 x 320 pixels, in which some sections of varying shapes are transferred using a variety of styles. It instructs users to click foreground style-transferred regions in accordance with a brief explanation that specifies which shapes should be selected. Cheng et al. [65] proposed two CAPTCHA schemes named Grid-CAPTCHA and Font-CAPTCHA, based on neural style transfer techniques. The procedure investigates an upright design concept for an image-based CAPTCHA that can improve its security by matching the text description. In Grid-CAPTCHA, users are asked to select one among nine stylized images to match a short scene description. Also, the CAPTCHA scheme uses the same style to transfer all their images to stylized images. Font-CAPTCHA uses neural style transfer to embed Chinese characters in an image and asks users to click the Chinese characters in the correct order according to the description. To exploit the basic weaknesses of current Deep

Convolutional Network Chenet al. proposed a new CAPTCHA system named StyleCAPTCHA [66]. It employs neural style transfer (NST) to blend human face images with reference style images. Each face image has been painted with a style image to produce a stylized face image. In each CAPTCHA task, the user must classify ten stylized images into one of two categories: human face or animal face.

Type	Scheme	Year	Sample	Description
Click	Implicit CAPTCHA [38]	2005		Click on a particular point on an image.
Click	FP-CAPTCHA [60]	2019		Click on a particular face-point on human face.
Click	SACAPTCHA [64]	2018	<p>Please click the <i>circle</i>, <i>heart</i> and <i>pentagram</i> regions with different styles:</p> 	Click on a particular shape in an image.
Selection	CONSCHEME [61]	2017		Click on the squares in junction.

<p>Click</p>	<p>DeRection [61]</p>	<p>2017</p>	<p>Click all of the deformed regions below:</p> 	<p>Click on all deformed regions.</p>
<p>Selection</p>	<p>ASSIRA [42]</p>	<p>2007</p>	<p>Image from Petfinder.com</p> <p>Please select all the cat photos:</p> 	<p>Click all cat images, not the dog.</p>
<p>Selection</p>	<p>SEMAGE [46]</p>	<p>2011</p>	<p>Choose images of the same animal (one may be real picture and the other a cartoon image !!)</p> 	<p>Select semantically similar images.</p>
<p>Selection</p>	<p>Avatar Captcha [56]</p>	<p>2012</p>	<p>Select all the Avatar (artificial) faces. Push Submit to validate the test. Refresh for a new set of images</p> 	<p>Select avatar faces not human faces.</p>

<p>Selection</p>	<p>HandCAPTCHA [63].</p>	<p>2017</p>		<p>Select two hand image of a person.</p>
<p>Selection</p>	<p>Stylecaptcha [66]</p>	<p>2020</p>		<p>Select human faces only from stylized image grid.</p>

III. VARIOUS ATTACKS ON CAPTCHA SCHEMES

The objective of CAPTCHA schemes is mainly to distinguish between human and computer systems. Instead, the attacker's objective is to break the CAPTCHA scheme, that is, to solve the presented challenge using an automated system while still being identified as a human. Pre-processing, segmentation, and recognition are the three phases in the typical process of overcoming classic CAPTCHAs. Before the segmentation and recognition phases, pre-processing techniques (such as picture binarization, image thinning, and noise reduction) are typically employed to remove background patterns, separate the foreground from the background, and eliminate noise [67].

In certain circumstances, extraction techniques such as PixelDelay Map (PDM), Catching Line, and Frame Selection are utilized before pre-processing. To aid recognition, segmentation algorithms are employed to separate the CAPTCHA picture into segments that include specific items. Vertical histogram, color-filling, snake segmentation, and JSEG are all well-known approaches for hacking CAPTCHAs [67]. In recent years, the scientific community has spent a lot of work on overcoming the various CAPTCHAs. To accomplish so, the attackers might employ a variety of methods, which are listed below.

1. **Object Recognition Attacks:** Object recognition, pixel count, dictionary, and database attacks are examples of this kind of attack. Pattern matching (e.g., shape context matching [68], correlation algorithm [69]), OCR recognition, Scale-Invariant Feature Transform (SIFT), and, more recently, deep learning is all prevalent approaches for object recognition. CNN, RNN, and LSTM-RNN are the most often utilized deep learning models for CAPTCHA recognition [70, 71, 72].

2. **Random Guess Attacks:** Attackers attempt to bypass the CAPTCHA method by guessing the right answer in this sort of attack. As a result, CAPTCHAs with a limited number of challenges are susceptible to this technique.
3. **Human Solver Relay Attacks:** The bot sends the CAPTCHA challenges to a distant human who, in exchange for a modest fee, solves the CAPTCHAs. The human completes the tests and submits the appropriate replies to the bot, which may then solve the CAPTCHA.

A. Attacks on Text CAPTCHA: Several researchers have proposed strategies for breaking the various types of text-based CAPTCHAs. Mori and Malik proposed a technique [68] based on shape context matching in 2003 that successfully broke both Gimpy and EZ-Gimpy CAPTCHAs [21] with 33% and 92% accuracy, respectively. Moy and Jones [69] used a correlation algorithm and a direct distortion estimation technique to break EZ-Gimpy with a success rate of 99 percent. Yan and El Ahmad demonstrated in 2008 that some segmentation-resistant CAPTCHAs, such as those used by Microsoft, Google, and Yahoo, [73, 24] could be cracked. Later, other researchers like Gao et al. [75] attempted to attack these CAPTCHA techniques, and their success rates were greater. With a success rate of 78%, El Ahmad and Yan [76] were able to crack Megaupload-CAPTCHA. Google researchers used neural networks to break the toughest category of ReCAPTCHA in 2014, with an accuracy of 99.8% [8]. Even without using OCR systems, Nguyen et al. [93] developed a set of methods against 3D CAPTCHAs. They were able to extract a collection of pixels from the characters of numerous 3D CAPTCHA systems (such as Teabag 3D, 3dcaptcha, and Super CAPTCHA) that may be utilized for automated challenge recognition. The authors were successful in breaching Teabag 3D, 3dcaptcha, and Super CAPTCHA with success rates of 31%, 58 percent, and 27%, respectively. Furthermore, using the side surface information included in the 3D text objects, Nguyen et al. [78] were able to crack Teabag 3D with a greater success rate, 76%. Nguyen et al. [79] demonstrated that the information over several animation frames in animated CAPTCHA schemes may be easily retrieved using basic approaches such as the PDM (Pixel Delay Map) or CL (Catching Line) methods. They successfully defeated various animated CAPTCHAs, including iCAPTCHA, Atlantis, KillBot Professional, and Dracon CAPTCHA, using these tactics. Due to their vulnerability against segmentation attacks, the same approaches have been used to overcome several types of HelloCAPTCHA systems with a success rate ranging from 16% to 100% [77]. NuCaptcha, unlike HelloCAPTCHA, is an animated CAPTCHA that is segmentation resistant. The PDM and CL approach used to bypass HelloCAPTCHA are ineffective in separating the characters since they are overlapping and packed together. NuCaptcha, on the other hand, has been cracked using more advanced methods [80, 81].

B. Attacks on Image CAPTCHA: Several techniques have been proposed in the literature to bypass various types of image-based CAPTCHAs. With a success rate of 10.3%, Golle [23] was able to discern the Asirra scheme. To accomplish so, he employed a variety of variables to train an SVM (Support Vector Machine) classifier that correctly identified cats and dogs with an accuracy of 82.7% (i.e., accuracy for a single image). With a 92% success rate, Hernandez-Castro et al. [10] developed a side-channel approach that evaded the Human Authentication barrier. With success rates of 70.78% and 83.5%, Sivakorn et al. [82] have effectively attacked both Google and Facebook image-based CAPTCHA. Zhao et al. [83] cracked both the new and old versions of reCAPTCHA V2 with success rates of 79% and 88% respectively. They also cracked the Facebook picture CAPTCHA and the China Railway CAPTCHA, with success rates of 86% and 90%, respectively. Cheung et al. [84] used Convolutional Neural Networks (CNN) to effectively break Avatar CAPTCHA, with a success rate of 99%. With success rates of 23% and 48%, Gao et al. [85] cracked both FR-CAPTCHA and Face-DCAPTCHA.

Andrews et al. [86] exploited the idea of Sobel operators and the length of the image's edges to break the Minteye CAPTCHA technique. The concept behind this approach is based on the fact that when a picture is twisted more, the image's edges get longer. As a result, the breaking techniques entail adding the lengths of the image's edges and then selecting the image with the smallest total of edges as the correct solution. Zhao et al. [83] cracked several image-based CAPTCHA methods, including the Tencent CAPTCHA. In particular, even throughout the motion of the sliding puzzle to the target place, their idea was 100% successful. Hernandez et al. presented a low-cost technique that employs JPEG to evaluate image continuity rather than attempting to tackle image recognition or form

recognition difficulties. They were able to overcome the most popular sliding-based CAPTCHAs using this side-channel technique. They were able to overcome Copy CAPTCHA with a 65.1% success rate, and they were also able to crack KeyCAPTCHA and Garb CAPTCHA with success rates of 20% and 98.1%, respectively, with minimal adjustments. Conti et al. [87] found out that Gao's Jigsaw CAPTCHA [88] is subject to relay and random guess attacks, with a 6.66% success rate. Lin et al. [89] cracked Drawing CAPTCHA with a 75% accuracy rate. Based on their observations of the difference in size between the diamond-shaped dots and the dots utilized in the background as noise, they presented an effective erosion-based breaking method.

IV. OPEN ISSUES, CHALLENGES, AND OPPORTUNITIES

In this research, we have identified the unresolved difficulties in building robust and useful CAPTCHA schemes, as well as the major obstacles that a CAPTCHA designer may face for research prospects. When the automated attack success rate is less than 0.01% and the scheme is resistant to human solver relay attacks, then the CAPTCHA is considered highly secure [60, 90, 84]. Unfortunately, most research on CAPTCHA scheme design in the literature focus solely on automated attacks, with just a few taking into account the susceptibility against human solver relay attacks. As a result, it's critical to shift away from schemes based on hard AI problems and toward other techniques that are less sensitive to learning-based attacks [91] while designing the next generation of CAPTCHA schemes. Big firms like Google, Alibaba, and Tencent have recently shifted to behavior-based CAPTCHA schemes, and a startup named Brave is working on implementing a sensor-based CAPTCHA scheme that employs the same core principle as Invisible CAPTCHA [92].

CAPTCHA methods are well-known for causing consumers aggravation. This is because, in most cases, designers attempting to make the system more secure also make the issue more difficult for humans. It's critical to lessen overall stiffness as well as the cognitive overload caused by the CAPTCHA challenges. However, creating user-friendly CAPTCHAs is not always simple, and there is often a trade-off between security and usability. Some CAPTCHA solutions, such as invisible reCAPTCHA and invisible CAPTCHA, provide perfect transparency to users, removing all cognitive hurdles.

Based on the foregoing observations, we have highlighted the following unresolved issues that need to be investigated further in order to create robust and useful CAPTCHA schemes: It is essential to analyze (1) the resilience of currently unbroken behavior-based CAPTCHAs against fourth-generation bots; (2) the security strength must be increased for the CAPTCHA schemes against replay attacks and human solver relay attacks; and (3) the security of CAPTCHA schemes that perform validation at the client-side, either with or without secure hardware, as they are vulnerable to hacking.

V. CONCLUSION

As a technique for preventing web bots and scripts from impersonating human activities, the CAPTCHA has a variety of uses, including safeguarding online voting, Ecommerce, and sign up/login. CAPTCHAs come in a variety of forms, including text-based and image-based, and may be used in a variety of scenarios. Apart from the inherent difficulties in establishing and securing CAPTCHAs, usability and accessibility concerns are key roadblocks to their adoption. Several solutions have been offered to address these major issues that might jeopardise the effectiveness of CAPTCHAs. Even though present options are functional and valuable, some of them have issues owing to increased implementation costs. Furthermore, in certain circumstances, usability and accessibility issues with these alternatives have remained unaddressed. Overall, a hybrid protection strategy, including CAPTCHA and its variants, is assessed wherever necessary to acquire better security. In order to address the aforementioned concerns, this article examines text-based and image-based CAPTCHAs, as well as alternate solutions, advancements, and issues are assessed using a set of criteria. The major goal of this article is to give a reference point for future research on existing studies and trends.

REFERENCES

- [1] Von Solms B. Information security—a multidimensional discipline. *Computers & Security* 2001; 20(6):504–508.
- [2] Verwoerd T, Hunt R. Intrusion detection techniques and approaches. *Computer Communications* 2002;25(15):1356–1365.
- [3] Von Ahn L, Blum M, Langford J. Telling humans and computers apart automatically. *Communications of the ACM* 2004; 47(2):56–60.
- [4] Mehrnejad, M., Bafghi, A. G., Harati, A., & Toreini, E. SEIMCHA: A New Semantic Image CAPTCHA Using Geometric Transformations. *International Journal of Information Security*, 63 - 76.
- [5] Luis Von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford. 2003. CAPTCHA: Using hard AI problems for security. In *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 294–311.
- [6] Kumar Chellapilla and Patrice Y. Simard. 2004. Using machine learning to break visual human interaction proofs (HIPs). In *17th International Conference on Neural Information Processing Systems (NIPS'04)*. The MIT Press, Cambridge, MA, 265–272.
- [7] H. Gao, J. Yan, Fang Cao, Zhengya Zhang, Lei Lei, Mengyun Tang, P. Zhang, X. Zhou, Xuqin Wang, and J. Li. 2016. A simple generic attack on text captchas. In *Network and Distributed System Security Symposium*.
- [8] Ian J. Goodfellow, Yaroslav Bulatov, Julian Ibarz, Sacha Arnoud, and Vinay D. Shet. 2014. Multi-digit number recognition from street view imagery using deep convolutional neural networks. *CoRR abs/1312.6082* (2014).
- [9] Christoph Fritsch, Michael Netter, Andreas Reisser, and Günther Pernul. 2010. Attacking image recognition Captchas. In *Trust, Privacy and Security in Digital Business*, Sokratis Katsikas, Javier Lopez, and Miguel Soriano (Eds.). Springer Berlin, 13–25.
- [10] C. J. Hernandez-Castro, A. Ribagorda, and Y. Saez. 2010. Side-channel attack on the HumanAuth CAPTCHA. In *International Conference on Security and Cryptography (SECRYPT'10)*. 1–7.
- [11] Vinay Shet. 2014. Are you a robot? Introducing “No CAPTCHA reCAPTCHA.” Retrieved from <https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html>.
- [12] Darko Brodic and Alessia Amelio. 2019. Exploring the usability of the text-based CAPTCHA on tablet computers. *Connect. Sci.* 31, 4 (2019), 430–444.
- [13] Diogo Daniel Ferreira, Luís Leira, Petya Mihaylova, and Petia Georgieva. 2019. Breaking text-based CAPTCHA with sparse convolutional neural networks. In *Pattern Recognition and Image Analysis*, Aythami Morales, Julian Fierrez, José Salvador Sánchez, and Bernardete Ribeiro (Eds.). Springer International Publishing, Cham, 404–415.
- [14] P. Wang, H. Gao, Z. Shi, Z. Yuan, and J. Hu. 2020. Simple and easy: Transfer learning-based attacks to text CAPTCHA. *IEEE Access* 8 (2020), 59044–59058.
- [15] Yang-Wai Chow, Willy Susilo, and Pairat Thorncharoensri. 2019. CAPTCHA Design and Security Issues. Springer Singapore, 69–92.
- [16] Xin Xu, Lei Liu, and Bo Li. 2020. A survey of CAPTCHA technologies to distinguish between human and computer. *Neurocomputing* (2020).
- [17] Y. Zhang, H. Gao, G. Pei, S. Luo, G. Chang, and N. Cheng. 2019. A survey of research on CAPTCHA designing and breaking techniques. In *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'19)*. 75–84. DOI: <https://doi.org/10.1109/TrustCom/BigDataSE.2019.00020>
- [18] J. Chen, Xiangyang Luo, Yanqing Guo, Y. Zhang, and Daofu Gong. 2017. A survey on breaking technique of text-based CAPTCHA. *Secur. Commun. Netw.* 2017 (2017), 6898617:1–6898617:15.
- [19] Ved Prakash Singh and Preet Pal. 2014. Survey of different types of CAPTCHA. *Int. J. Comput. Sci. Inf. Technol.* 5, 2(2014), 2242–2245.
- [20] M. Tariq Banday and Nisar A. Shah. 2011. A study of CAPTCHAs for securing web services. *arXiv preprint arXiv:1112.5605* (2011).

- [21] Luis von Ahn, Manuel Blum, Nick Hopper, John Langford, and Udi Manber. 2000. GIMPY. Retrieved from <http://www.captcha.net/captchas/gimpy/>.
- [22] Monica Chew and Henry S. Baird. 2003. BaffleText: a human interactive proof. In Document Recognition and RetrievalX, Tapas Kanungo, Elisa H. Barney Smith, Jianying Hu, and Paul B. Kantor (Eds.), Vol. 5010. International Society for Optics and Photonics, SPIE, 305–316.
- [23] Richard Chow, Philippe Golle, Markus Jakobsson, Lusha Wang, and XiaoFeng Wang. 2008. Making CAPTCHAclickable. In 9th Workshop on Mobile Computing Systems and Applications (HotMobile'08). Association for Computing Machinery, New York, NY, 91–94.
- [24] Jeff Yan and Ahmad Salah El Ahmad. 2008. A low-cost attack on a Microsoft Captcha. In 15th ACM Conference on Computer and Communications Security (CCS'08). Association for Computing Machinery, New York, NY, 543–554.
- [25] Luis von Ahn, Benjamin Maurer, Colin McMillen, David Abraham, and Manuel Blum. 2008. reCAPTCHA: Humanbased character recognition via web security measures. *Science* 321, 5895 (2008), 1465–1468.
- [26] OCR Research Team. 2006. Teabag 3D evolution. Retrieved from <https://ocr-research.org.ua/teabag.html>.
- [27] Michael L. Wells. 2003. Exciting Features in Super CAPTCHA. Retrieved from <https://goldsborowebdevelopment.com/2013/06/exciting-features-in-super-captcha/>.
- [28] Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo. 2014. On the security of text-based 3D CAPTCHAs. *Comput.Secur.* 45 (2014), 84–99. DOI:<https://doi.org/10.1016/j.cose.2014.05.004>
- [29] M. Imsamai and S. Phimoltares. 2010. 3D CAPTCHA: A next generation of the CAPTCHA. In International Conference on Information Science and Applications. 1–8.
- [30] I. Fischer and T. Herfet. 2006. Visual CAPTCHAs for document authentication. In IEEE Workshop on Multimedia Signal Processing. 471–474.
- [31] Anja B. Naumann, Thomas Franke, and Christian Bauckhage. 2009. Investigating CAPTCHAs based on visual phenomena. In Human-Computer Interaction–INTERACT 2009, Tom Gross, Jan Gulliksen, Paula Kotzé, Lars Oestreicher, Philippe Palanque, Raquel Oliveira Prates, and Marco Winckler (Eds.). Springer Berlin, 745–748.
- [32] J. Cui, J. Mei, X. Wang, D. Zhang, and W. Zhang. 2009. A CAPTCHA implementation based on 3D animation. In International Conference on Multimedia Information Networking and Security. 179–182.
- [33] Program Product. 2010. HelloCAPTCHA. Retrieved from <http://www.hellocaptcha.com/>.
- [34] NuCaptcha Inc. 2018. NuCaptcha. Retrieved from <https://www.nucaptcha.com>.
- [35] Dracon Projects. 2006. Dracon Visual Flash CAPTCHA. Retrieved from <https://www.dracon.biz/captcha.php>.
- [36] Zhu, B., Liu, J., Li, Q., Li, S., Xu, N.: Image-based captcha exploiting context in object recognition (Jul 9 2013), uS Patent 8,483,518.
- [37] Zhang, K., Zheng, Y.: Information Security: 7th International Conference, ISC2004, Palo Alto, CA, USA, September 27-29, 2004, Proceedings, vol. 3225. Springer(2004).
- [38] Baird, H.S., Bentley, J.L.: Implicit captchas. In: Document Recognition and Retrieval XII. vol. 5676, pp. 191-196. International Society for Optics and Photonics(2005).
- [39] Shirali-Shahreza, M., Shirali-Shahreza, S.: Captcha for blind people. In: 2007 IEEE International Symposium on Signal Processing and Information Technology. pp.995-998. IEEE (2007).
- [40] Rui, Y., Liu, Z.: Artificial: Automated reverse turing test using facial features. *Multimedia Systems* 9(6), 493-502 (2004).
- [41] Zhu, B.B., Yan, J., Li, Q., Yang, C., Liu, J., Xu, N., Yi, M., Cai, K.: Attacks and design of image recognition captchas. In: Proceedings of the 17th ACM conference on Computer and communications security. pp. 187-200. ACM (2010)
- [42] Elson, J., Douceur, J.R., Howell, J., Saul, J.: Asirra: a captcha that exploits interest-aligned manual image categorization. *CCS* 7, 366-374 (2007)
- [43] Golle, P.: Machine learning attacks against the asirracaptcha. In: Proceedings of the 15th ACM conference on Computer and communications security. pp. 535-542 (2008).
- [44] Datta, R., Li, J., Wang, J.Z.: Imagination: a robust image-based captcha generation system. In: Proceedings of the 13th annual ACM international conference on Multimedia. pp. 331-334. ACM (2005).

- [45]Gossweiler, R., Kamvar, M., Baluja, S.: What's up captcha? a captcha based on image orientation. In: Proceedings of the 18th international conference on World wide web. pp. 841-850 (2009).
- [46] Vikram, S., Fan, Y., Gu, G.: Semage: a new image-based two-factor captcha. In:Proceedings of the 27th Annual Computer Security Applications Conference. pp.237{246. ACM (2011).
- [47]Basso, A., Sizzo, S.: Preventing massive automated access to web resources. *computers& security* 28(3-4), 174-188 (2009).
- [48]Von Ahn, L., Maurer, B., McMillen, C., Abraham, D., Blum, M.: recaptcha: Human-based character recognition via web security measures. *Science* 321(5895),1465{1468 (2008).
- [49]Shet, V.: Are you a robot? Introducing no captcharecaptcha. *Google Security Blog* 3, 12 (2014).
- [50]Lopresti, D.: Leveraging the captcha problem. In: *International Workshop on Human Interactive Proofs*. pp. 97-110. Springer (2005).
- [51]Sivakorn, S., Polakis, I., Keromytis, A.D.: I am robot:(deep) learning to break semantic image captchas. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 388-403. IEEE (2016).
- [52]Polakis, I., Ilija, P., Maggi, F., Lancini, M., Kontaxis, G., Zanero, S., Ioannidis, S., Keromytis, A.D.: Faces in the distorting mirror: Revisiting photo-based social authentication. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. pp. 501-512 (2014).
- [53]Krol, K., Parkin, S., Sasse, M.A.: " i don't like putting my face on the internet!": An acceptance study of face biometrics as a captcha replacement. In: 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). pp. 1-7. IEEE (2016).
- [54]Tariq Banday, M., A Shah, N.: Image ipcaptcha. *The ISC International Journal of Information Security* 1(2), 105{123 (2009).
- [55] Osadchy, M., Hernandez-Castro, J., Gibson, S., Dunkelman, O., Perez-Cabo, D.:No bot expects the deepcaptcha! introducing immutable adversarial examples withapplications to captcha. *Cryptology ePrint Archive* (2016).

- [56] D'Souza, D., Polina, P.C., Yampolskiy, R.V.: Avatar captcha: Telling computers and humans apart via face classification. In: 2012 IEEE International Conference on Electro/Information Technology. pp. 1-6. IEEE (2012).
- [57] Cheung, B.: Convolutional neural networks applied to human face classification. In: 2012 11th International Conference on Machine Learning and Applications. vol. 2, pp. 580-583. IEEE (2012).
- [58] Goswami, G., Powell, B.M., Vatsa, M., Singh, R., Noore, A.: Fr-captcha: Captcha based on recognizing human faces. *PloS one* 9(4), e91708 (2014).
- [59] Goswami, G., Powell, B.M., Vatsa, M., Singh, R., Noore, A.: Facedcaptcha: Face detection based color image captcha. *Future Generation Computer Systems* 31, 59-68 (2014).
- [60] Ray, P., Giri, D., Kumar, S., Sahoo, P.: Fp-captcha: An improved captcha design scheme based on face points. In: International Conference on Information Technology and Applied Mathematics. pp. 218-233. Springer (2019)
- [61] Zhang, P., Gao, H., Cheng, Z., Cao, F.: Two novel image-based captcha schemes based on visual effects. In: CCF Chinese Conference on Computer Vision. pp. 14-25. Springer (2017).
- [62] Bera, A., Bhattacharjee, D., Nasipuri, M.: Hand biometric verification with hand image-based captcha. In: Advanced Computing and Systems for Security, pp. 3-18. Springer (2018).
- [63] Bera, A., Bhattacharjee, D., Shum, H.P.: Two-stage human verification using hand-captcha and anti-spoofed finger biometrics with feature selection. *Expert Systems with Applications* 171, 114583 (2021)
- [64] Tang, M., Gao, H., Zhang, Y., Liu, Y., Zhang, P., Wang, P.: Research on deep learning techniques in breaking text-based captchas and designing image-based captcha. *IEEE Transactions on Information Forensics and Security* 13(10), 2522-2537 (2018).
- [65] Cheng, Z., Gao, H., Liu, Z., Wu, H., Zi, Y., Pei, G.: Image-based captchas based on neural style transfer. *IET Information Security* 13(6), 519-529 (2019).
- [66] Chen, H., Jiang, B., Chen, H.: Stylecaptcha: Captcha based on stylized images to defend against deep networks. In: Proceedings of the 2020 ACM-IMS on Foundations of Data Science Conference. pp. 161-170 (2020).
- [67] Narges Roshanbin and James Miller. 2013. A survey and analysis of current CAPTCHA approaches. *J. Web Eng.* 12, 1-2 (Feb. 2013), 1-40.
- [68] G. Mori and J. Malik. 2003. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. In IEEE Computer Society Conference on Computer Vision and Pattern Recognition.
- [69] G. Moy, N. Jones, C. Harkless, and R. Potter. 2004. Distortion estimation techniques in solving visual CAPTCHAs. In IEEE Computer Society Conference on Computer Vision and Pattern Recognition.
- [70] Haichang Gao, Wei Wang, Jiao Qi, Xuqin Wang, Xiyang Liu, and Jeff Yan. 2013. The robustness of hollow CAPTCHAs. In ACMSIGSAC Conference on Computer & Communications Security (CCS'13). Association for Computing Machinery, New York, NY, 1075-1086.
- [71] Ian J. Goodfellow, Yaroslav Bulatov, Julian Ibarz, Sacha Arnoud, and Vinay D. Shet. 2014. Multi-digit number recognition from street view imagery using deep convolutional neural networks. *CoRR abs/1312.6082* (2014).
- [72] C. Rui, Y. Jing, H. Rong-gui, and H. Shu-guang. 2013. A novel LSTM-RNN decoding algorithm in CAPTCHA recognition. In 3rd International Conference on Instrumentation, Measurement, Computer, Communication and Control. 766-771.
- [73] Jeff Yan and Ahmad Salah El Ahmad. 2008. Is Cheap Labour Behind the scene? - Low-cost Automated Attacks on Yahoo CAPTCHAs. Technical Report. School of Computing Science, Newcastle University, England.
- [74] Oleg Starostenko, Claudia Cruz-Perez, Fernando Uceda-Ponga, and Vicente Alarcon-Aquino. 2015. Breaking text based CAPTCHAs with variable word and character orientation. *Pattern Recog.* 48, 4 (2015), 1101-1112.
- [75] Y. Zi, H. Gao, Z. Cheng, and Y. Liu. 2020. An end-to-end attack on text CAPTCHAs. *IEEE Trans. Inf. Forens. Secur.* 15(2020), 753-766.
- [76] Ahmad Salah El Ahmad, Jeff Yan, and Lindsay Marshall. 2010. The robustness of a new CAPTCHA. In 3rd European Workshop on System Security (EUROSEC'10). Association for Computing Machinery, New York, NY, 36-41.
- [77] Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo. 2012. Breaking an Animated CAPTCHA Scheme. In Applied Cryptography and Network Security, Feng Bao, Pierangela Samarati, and Jianying Zhou (Eds.). Springer Berlin, 12-29.

- [78] Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo. 2012. Breaking a 3D-based CAPTCHA scheme. In Conference on Information Security and Cryptology, Howon Kim (Ed.). Springer Berlin, 391–405.
- [79] Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo. 2012. Attacking animated CAPTCHAs via character extraction. In Cryptology and Network Security, Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis (Eds.). Springer Berlin, 98–113.
- [80] Elie Bursztein. 2012. How we broke the NuCaptcha video scheme and what we propose to fix it. Retrieved from <https://elie.net/blog/security/how-we-broke-the-nucaptcha-video-scheme-and-what-we-propose-to-fix-it/>.
- [81] Y. Xu, G. Reynaga, S. Chiasson, J. Frahm, F. Monrose, and P. C. van Oorschot. 2014. Security analysis and related usability of motion-based CAPTCHAs: Decoding codewords in motion. *IEEE Trans. Depend. Sec. Comput.* 11, 5 (2014), 480–493.
- [82] Suphanee Sivakorn, Jason Polakis, and Angelos D. Keromytis. 2016. I’m not a human : Breaking the Google re-CAPTCHA. In BlackHat Conference.
- [83] Binbin Zhao, Haiqin Weng, Shouling Ji, Jianhai Chen, Ting Wang, Qinming He, and Reheem Beyah. 2018. Toward evaluating the security of real-world deployed image CAPTCHAs. In 11th ACM Workshop on Artificial Intelligence and Security (AISec’18). Association for Computing Machinery, New York, NY, 85–96.
- [84] B. Cheung. 2012. Convolutional neural networks applied to human face classification. In 11th International Conference on Machine Learning and Applications. 580–583.
- [85] H. Gao, J. Yan, Fang Cao, Zhengya Zhang, Lei Lei, Mengyun Tang, P. Zhang, X. Zhou, Xuqin Wang, and J. Li. 2016. A simple generic attack on text captchas. In Network and Distributed System Security Symposium.
- [86] J. W. Andrews. 2013. Breaking the MintEye image CAPTCHA in 23 lines of Python. Retrieved from <http://www.jwandrews.co.uk/2013/01/breaking-the-minteye-image-captcha-in-23-lines-of-python/>.
- [87] Mauro Conti, Claudio Guarisco, and Riccardo Spolaor. 2016. CAPTCHAStar! A novel CAPTCHA based on interactive shape discovery. In Applied Cryptography and Network Security, Mark Manulis, Ahmad-Reza Sadeghi, and Steve Schneider (Eds.). Springer International Publishing, Cham, 611–628.
- [88] H. Gao, D. Yao, H. Liu, X. Liu, and L. Wang. 2010. A novel image based CAPTCHA using jigsaw puzzle. In 13th IEEE International Conference on Computational Science and Engineering. 351–356.
- [89] Rosa Lin, Shih-Yu Huang, Graeme B. Bell, and Yeuan-Kuen Lee. 2011. A new CAPTCHA interface design for mobile devices. In 12th Australasian User Interface Conference (AUIC’11). Australian Computer Society, Inc., AUS, 3–8.
- [90] Rabih Al Nachar, Elie Inaty, Patrick J. Bonnin, and Yasser Alayli. 2015. Breaking down Captcha using edge corners and fuzzy logic segmentation/recognition technique. *Secur. Commun. Netw.* 8, 18 (2015), 3995–4012.
- [91] Carlos Javier Hernández-Castro, Shujun Li, and María D. R-Moreno. 2020. All about uncertainties and traps: Statistical oracle-based attacks on a new CAPTCHA protection against oracle attacks. *Comput. Secur.* 92 (2020), 101758.
- [92] Meriem Guerar, Alessio Merlo, Mauro Migliardi, and Francesco Palmieri. 2018. Invisible CAPTCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT. *Comput. Secur.* 78 (2018), 255–266.