A SURVEY ON CAPTCHA: ORIGIN, APPLICATIONS AND CLASSIFICATION

Abdalnaser Algwil

Alasmarya Islamic University
Faculty of Information Technology
Zliten, Almuntarha Street
a.algwil@it.asmarya.edu.ly

ABSTRACT

Captcha challenges have become the most widely used techniques to deter the misuse of services on the Internet. The majority of current Captcha schemes are principally based on distorted text challenges. However, many of these schemes suffer from inadequacies in terms of *security*, *usability*, or the balance between them. This calls for alternative Captcha approaches to be devised. In fact, it has become an active research area in the exploration of alternative designs for example, image-based Captcha, motion-based Captcha, and game-based Captcha. This paper reviews the extant literature of the Captcha phenomenon to identify the more praiseworthy aspects and shortcomings of different types of Captcha. We present the origin of Captcha, its importance and uses, Captcha types and their features, as supported with pictorial examples, and key problems in security and usability aspects. Captcha issues on mobile devices is also presented.

Keywords: Captcha, Security, Usability.

1. INTRODUCTION

Various kinds of Captchas (acronym for **C**ompletely **A**utomated **P**ublic **T**uring Tests to Tell **C**omputers and **H**umans **A**part) have been evolved for preventing malicious bots from abusing Internet services or resources such as automatically signing up for mail accounts, submitting bogus comments to product reviews in consumer services, and so on. The Captcha technology, being a de facto standard security mechanism for that purpose, can be found on almost every website nowadays [1].

In 2000, the term of Captcha was coined by a team from Carnegie Mellon University. Since then, it has become increasingly widespread on the Internet as a defensive mechanism against undesirable bots by several

commercial web sites such as *Yahoo*, *Google* and *Microsoft* [2]. The reason behind this is that the Captchas are based on open Artificial Intelligence (AI) problems which are hard to solve programmatically.

A Captcha challenge, which is known as a *Human Interaction Proof* (HIP), is a challenge-response test that is created and validated automatically by computer to distinguish whether the user identity is human or a malicious bot program. For this reason, a Captcha should be easy to solve by humans and very difficult to solve by automated software [3]. This balance between aspects of ease for humans, represented in *usability*, and aspects of difficulty for programs, represented in *security*, is hard to attain in the same scheme.

Over the past twenty years, different types of Captcha have been evolved for balancing between security and usability aspects for example, text-based Captcha, image-based Captcha, and Cognitive-based Captcha.

Although text-based Captchas are those most popularly deployed on the Internet, there are many new sorts of Captchas that emerge every year as a result of the disadvantages of former ones, which were a key reason in the success of adversarial attacks against them. These successful adversarial attacks led to the improvement of a next generation of Captchas each time. These enhancements were mostly to overcome deficiencies in *usability* and *security* or lack of balance between them [4][5].

In the last years, many non-text-based Captcha schemes have been developed to reduce user frustration and to be more convenient for mobiles devices, especially with the increased access to the Internet using small touch screen devices. ComScore [6] reports that small touch screen devices exceeded traditional PCs as a basic method used by users to access the

Internet. The report showed that small touch screen devices now account for around 37% of the time users spend online.

Consequently, it is very difficult to neglect the use of Captcha on mobile and tablet devices. Almost the majority of these non-text-based Captchas are principally designed to use mouse-based input, which means they can be solved with drag/drop or some clicks of a mouse, finger tip or stylus on a touch screen device. Although, the usability of these schemes seems to be superior to the other forms of text-based Captchas, many are in need of more security analysis to be a viable alternative to conventional systems. To date, a Captcha scheme that achieves a balance between *usability* and *security* across different devices is still beyond reach.

Research Aims. This paper aims to provide a reasonably in-depth background to the Captcha phenomenon and other related work through focusing mainly on the foundation of Captcha, its applications, types of Captcha and their evolution.

Research Methodology. The search adopts the descriptive analytical approach, which is in line with the nature of the subject.

The remaining paper is organized as follows: Section 2 explains the origin and foundation of Captcha. Section 3 presents Captcha applications in terms of both practical security and collateral benefits supported with real-life examples. Section 4 classifies different categories of Captcha designs. Section 5 discusses Captcha issues on mobile devices. Section 6 concludes the paper.

2. THE ORIGIN AND FOUNDATION OF CAPTCHA

Although Captcha tests have only recent emerged, the idea of distinguishing between human and machine was first proposed since more than sixty years ago. In 1950, Alan Turing considered the question "*Can machines think?*" [7] and then proposed a test to evaluate it. In the original Turing Test, an "*imitation game*" is played by a human interrogator and taken by two interlocutors – one is a human and the other is a machine. The human interrogator stays in a room apart from the other two players, and communicates with them via typewritten text so that tone of voice cannot aid the interrogator. The human judge poses a series of questions to the two players – both of which pretend to be the human – and eventually has to decide which is which. If the human interrogator fails sufficiently often to determine correctly which of the two is the human and which is the machine competitor, the machine is then said to have passed the Turing Test as it can successfully imitate a human being. In fact, with this game, Turing reframed the original question from "*Can machines think?*" to "*Can machines do what we can do?*".

Machines are still not able to pass the Turing test in its original sense [8]. However, Turing's proposal has been widely influential in a variety of research communities such as computer science, cognitive science, and so on [9]. Perhaps the most obvious phenomenon relating to this test within the security arena is the Captcha mechanism. Like the Turing Test, Captcha is designed principally to distinguish humans from computers, despite the differences in the design goal. That is, the design goal of the original Turing test is to measure the progress of Artificial Intelligence, whereas the Captcha is designed as a security mechanism [10]. The other major

difference between them is that a Captcha test is administered by a computer rather than a human. In addition, the Captcha poses only one challenge (or very few) to only one user, rather than a series of challenges to two players [11]. For this reason, Captcha schemes are sometimes called *reverse Turing tests* in the literature. However, to avoid confusion between the *Captcha* and *Reverse Turing test*, von Ahn et al. [12] distinguished between the two terms by citing that the participants in a *Reverse Turing test* attempt to prove they are the computer, while in Captcha test users try to prove they are human to a machine interrogator. Thus, they describe Captcha as an "*Automated Turing test*" rather than "*Reverse Turing test*". In the same context, the terms *Captcha* and *Human Interactive Proof* (HIP) are also often be used interchangeably. However, Chew and Henry [13] pointed out that Captcha tests are a special class of HIPs that are defined broadly in [9] as "*a class of challenge/response protocols which allow a human to be authenticated as a member of a given group e.g., an adult (vs. a child), a human (vs. machine), a particular individual (vs. everyone else), etc*.". In the course of this paper, the acronym "*Captcha*" will be used.

Theoretically, Moni Naor, in a 1996 unpublished manuscript [14], was the first to informally suggest the use of an Automated Turing test to distinguish between human users and automated programs. His proposal for a 'humanity' test was to use the original Turing Test whilst substituting the human interrogator for a computer program. Naor's aim was to propose a scheme that could discourage and exclude software robots from abusing Web services originally offered for human use only. Naor provided several possible areas from vision and natural language processing as the proposed sources for challenges which are reliably human-solvable but machine-

unsolvable, such as gender recognition, understanding facial expression, finding body parts, handwriting recognition, speech recognition, amongst others. It is worth noting that most of these proposals have been developed as Captcha schemes over the subsequent several years.

Practically, in 1997, a technical team at AltaVista was the first to develop an Automated Turing test (henceforth referred to as Captcha). AltaVista offered a free "add-URL" service to expand its search coverage and include Websites that were important to its most motivated customers. This service was abused extensively, however, in that it received vast numbers of automated URL submissions from malicious bots in an attempt to skew the importance-ranking algorithms of the AltaVista search engine, and thus artificially inflate their search ranking [9]. To combat this, a team of developers, composed of Andrei Broder, Chief Scientist of AltaVista, and his colleagues, created a verification mechanism to distinguish between human users and bots. Their method was to construct a text-recognition Captcha resistant to OCR attack using various typefaces, randomly rotated/skewed/ translated characters, obfuscated backgrounds, and so forth (see Fig. 1). As a result, the Captcha so developed was able to successfully reduce bot abuse of the "add-URL" service by more than 95% [9]. A U.S. patent [15] for the developed system was issued in 2001.

Fig. 1.Example of an AltaVista challenge

In 2000, Yahoo! was experiencing similar problems with their chat room. That is, chatbots were joining online chat sessions and irritating legitimate users by inviting them to advertising sites [8]. To identify all bots and prevent their entry to chat rooms, Yahoo!'s chief scientist approached researchers at Carnegie Mellon University (CMU) with this problem, which in turn gave birth to the Captcha project [16]. The CMU team, including the Captcha pioneers Manual Blum, Luis von Ahn, and John Langford, in a practical effort to differentiate humans from machine users on the Web, developed an automatic method. Their solution came in the form of three text-based Captcha schemes: Gimpy, EZ-Gimpy and Gimpy-r, which were developed particularly for Yahoo! to protect its various services. In fact, they coined the term Captcha itself [17].

Many others have followed in their footsteps ever since. Whereas numerous new text-based Captcha designs such as BaffleText [13], PessimalPrint [11], ScatterType [19] and others have been proposed by other research groups, various large corporations (e.g., Microsoft, Google, and so on) have also developed their own textual Captcha tests to safeguard their services against malicious abuse. Given that Captcha has become the most widely used technique to protect web services, the following section highlights their practical applications.

3. CAPTCHA APPLICATIONS

Nowadays, Captcha has a wide variety of applications on the Web. For example, they can be effectively used to:

- ***Prevent automated account registration.*** Many companies offer free online registration services such as free e-mail, fora, social networks and blogs. Bots can automatically sign up for a large number of

accounts very quickly. On the one hand, these created accounts can lead to account management problems, as well as increase the burden on servers. On the other, they may become a tool for spamming that spread vast amounts of unsolicited messages [17]. To address this issue, Captcha is effectively utilized to hinder bots and ascertain that only humans can sign up for free account.

- ***Protect online opinion polls and product recommendation systems***. Automated vote-casting bots can vote thousands of times in order to stuff ballots or artificially inflate/deflate product ratings. For instance, on high-traffic shopping websites (say, eBay), unprincipled sellers may employ a malicious bot to rate themselves positively a huge number of times so as to deceive purchasers into believing that they are trustworthy [13]. In addition, the opinion poll results might be biased and untrustworthy unless pollsters use a proper humanity test to filter out auto-voting practices.

- ***Thwart brute force and dictionary attacks in password systems***. In a password-guessing attack, an automated computer program tries to iterate every possible username/password combination until a correct one is found. A classic method to prevent such attacks is to lock out an account after a certain number of failed logins. However, a major drawback of the account lockout approach is that it enables denial of service attacks against legitimate users [20][21]. Alternatively, Pinkas and Sander [20] have proposed using a Captcha mechanism to deter dictionary attacks. More precisely, Captcha challenges must first be solved (supposedly by human users, rather than bots) after a specified number of unsuccessful login attempts.

- ***Suppress comment spam.*** Spambots have the capability to submit a large number of unsolicited bogus comments to blogs, forums, product reviews in consumer services, and so on. Their key purposes might be either for: commercial promotions, such as displaying unrelated advertisements, increasing backlinks to the spammer's website in order to raise its search engine ranks, and so forth; or for the purposes of harassment and vandalism. Captcha challenges offer an efficient solution to combat spambots.

- ***Restrain bulk ticket purchases***. Within seconds of a large event going on sale, automated bots can help online touts to harvest tickets in bulk and then resell them on secondary ticketing sites at exorbitant prices compared to their face value. In fact, this may cause a serious problem for the majority of ordinary fans, who want to buy tickets directly but are unable to because tickets sell out within minutes of becoming available. In this instance, the Captcha mechanism can effectively protect ticket buyers from the cyber-touts [22]; that is, a Captcha challenge must be solved by a human when exceeding some set limit to the number of tickets that can be bought.

- ***Protect email from worms and spam***. The idea is simple: an email is only accepted if a sender behind another computer is verified as being a human via Captcha [23]. The SpamArrest service [24], for instance, is already using this technology. That is, emails from unauthorized senders receive an auto-reply message asking them to solve a Captcha challenge. Once the sender successfully completes the solution, the email in the waitlist is then delivered to the recipient, whilst adding the sender to the recipient's authorized list.

- ***Limit Denial-of-Service (DoS) attacks***. DoS attacks aim to render a targeted machine or network resource unavailable to its legitimate users. One way to launch such attacks is by overloading a target website with a very large number of fake requests in an attempt to exhaust server resources and thus deprive intended users legitimate access. Wilkins [21] suggests that the Captcha mechanism can be effectively applied as an alternative to a hard limit on a resource intensive request in unauthenticated services.

- ***Avert Web crawling or spidering***. Not all bots conduct nefarious activities; search engine bots (also called spiders or crawlers), for instance, can typically accomplish useful tasks for the purposes of Web indexing. These crawlers often visit websites without approval in order to index content and provide up-to-date data to their search engines. However, some website owners might have legitimate reasons for not wanting to index some of their Web pages. For that, the site's administrators can usually use either the Robots Exclusion Protocol or particular HTML tags, politely instructing search engine bots which Web pages are indexable and, just as importantly, which ones are not. In fact, these mechanisms are purely advisory and not a mandatory limitation to bots reading a particular web page. Thus, malicious bots often do not honour such directives and may entirely ignore them; worse still, malware bots may start with pages that are preferably non-indexable and go straight to them. Captcha can be effectively used to solve this issue [23].

Given the importance of Captcha mechanisms in protecting Web services, the following section will shed light on the types of Captcha.

4. TYPES OF CAPTCHA

Many types of Captcha have been proposed and developed to prevent misuse services on the Internet. They can be classified under five main categories as follows:

4.1. Text-based Captcha

In this category of Captcha, an image of distorted text is generated and displayed to the user, who is prompted to recognize and transcribe the text as a response. The Roman characters and/or digits are usually used to create a string in the OCR Captcha image, whilst discarding certain characters that can confuse human users such as O and 0, I and 1 and so forth. Typically, a string within an image is either a randomly generated text or a word chosen from a predefined dictionary. Various types of transformations, clutter, noise, and complicated colour combinations, among others, are commonly applied to the foreground and/or background with a view to making the Captcha image more challenging to attackers.

Captcha designers have put serious effort into the development of Captcha challenges that are reliably human-legible but computer-illegible. However, with ever-increasing advances in computer vision, deep learning and pattern recognition research, as well as sophisticated attacks on OCR Captcha schemes that have been successfully implemented, the existing gap between humans and computers in recognizing distorted text has been considerably reduced, which was the key motivation for designers to use more complicated techniques that are increasingly resistant to automated attack. In fact, this difficulty reflects negatively on the usability of the scheme because it is also hard for humans to solve the challenges. Nevertheless, text Captchas are still the most commonly used in today's web services.

Well-known examples of early text-based Captcha schemes are the Gimpy family. In the Gimpy scheme, five pairs of overlapping distorted English words are randomly chosen from an 850-word dictionary and rendered for the user on a colourful, noisy background, who is challenged to read and transcribe a certain number of them correctly. Fig. 2 (a) shows an example of the Gimpy challenge. Gimpy was developed by researchers at CMU for Yahoo! to protect a variety of its online services. However, Yahoo users experienced difficulties with it, complaining extensively about to its complexity, which in turn led to Gimpy being withdrawn from service [9][13]. Alternatively, easier versions of the Gimpy Captcha (called EZ-Gimpy and Gimpy-r) were developed and then adopted by Yahoo as shown in Fig. 2 (b)&(c). However, these Captcha schemes had been successfully broken using computer vision techniques in [26][27].

(a) Gimpy (b) EZ-Gimpy (c) Gimpy-r

Fig. 2. Examples of images from the Gimpy family

In 2001, Coates et al. [11] have proposed another form of OCR Captcha called "*Pessimal Print*". In this Captcha, as shown in Fig. 3 (a), a single English word is rendered with a randomly chosen typeface among a predefined list. The word-image is then degraded using the image degradation model that simulates physical defects resulting from copying and scanning of printed text in an attempt to baffle OCR attacks [13]. However, the Mori-Malik attack was able to break it 40% of the time [13].

In 2003, Chew and Baird [13] developed a new breed of Captcha called *BaffleText* that exploits the Gestalt perception ability of the human brain, which is very good at inferring a complete picture regardless of its incompleteness, sparsity, or fragmentation of its information in contrast to computers. BaffleText uses different masking techniques to degrade images of pronounceable non-dictionary words, as shown in Fig. 3 (b). However, computer-vision attacks were able to break it with a 25% success rate [13].

A couple of years later, *ScatterType* Captcha was introduced by Baird and Riopka [19]. ScatterType used images of English-like nonsense words whose characters are horizontally and vertically cut into fragments and scattered in a way that no automatic approach can reassemble into characters, as shown in Fig. 3 (c). It is principally designed to frustrate character-segmentation attacks, while still being user friendly [28][29].

(a) Pessimal Print (b) BaffleText (c) ScatterType

Fig. 3. Examples on Pessimal Print, BaffleText and ScatterType Captchas

Captchaservice.org [30] was the first publicly-available web service for Captcha generation, as developed by Tim Converse in 2005. The service offers simple, controllable APIs that allow site designers to incorporate Captcha challenges into their pages. In 2007, a simple attack [31] was able to break the visual image Captcha challenges provided by this service with a high rate of success. Another example of attacks on Captcha services is API attacks on the CCaptcha service [109]. However, Algwil [110] shows how to securely design Captcha as a web service to avoid such attacks.

In 2003, Simard et al. [32] at Microsoft Research argued that the segmentation task is much more difficult than the recognition task, and poses an invincible challenge for the state-of-the-art technologies. Accordingly, they developed a segmentation- and recognition-based Captcha to protect Microsoft's online services. In this Captcha, a string image is randomly generated, distorted, and then covered by arcs of both foreground and background colour, as shown in Fig. 4. However, a simple attack was able to break it with a success rate of 60% [33].

Fig. 4. The use of arcs as an anti-segmentation mechanism

The "*Crowding Character Together*" (CCT) method is another segmentation resistant approach that is commonly used in Captcha designs such as those implemented by *Google*, *Microsoft*, *Baidu* and *eBay*, as shown in Fig. 5. CCT is considered the most secure anti-segmentation strategy by which to strengthen text-based Captcha schemes [34]. In this approach, white spaces between characters are eliminated with the intention of deliberately connecting characters with each other. However, some attacks, such as those described in [35][34][36] broke Captchas that adopted this approach with reasonable success rates.

(a) Google (b) Microsoft (c) Baidu (d) eBay

Fig. 5. examples of CCT-based Captcha schemes

Other researchers have proposed the use of different techniques to hide the location of individual characters, via such techniques as background confusion, in an attempt to blend the Captcha text with its background, thus making character segmentation very challenging to computers. This can be typically done by either adding noise to the Captcha image, using a complex image background, or by applying similar colours for both the foreground and the background [34]. For example, Ferzli et al. [37], Martinović et al. [38], Ince et al. [39] proposed different approaches to prevent character extraction from a complex background.

Rusu et al. [41][40][42] have exploited the ability gap in reading handwritten text images between humans and computers to build a new class of Captcha. Handwritten Captcha offers the challenges of deformed handwritten word images that are either randomly chosen from a database of handwritten names of American cities or synthetically constructed by gluing together isolated handwritten character images. Fig. 6 shows some examples of handwritten Captcha.

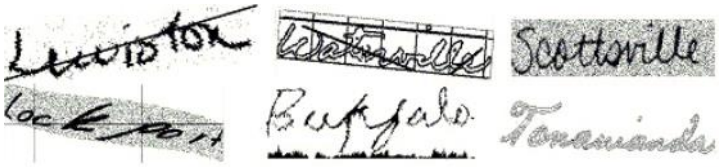


Fig. 6. Examples of handwritten Captcha with various transformations

Non- Roman text-based Captcha schemes have been also developed in various languages such as *Arabic*, *Chinese*, and so on, with the potential of being more convenient for users on websites in those languages. However, the overwhelming majority of non-English Captcha schemes are designed in the same style as in their traditional English text counterparts. That is, a text

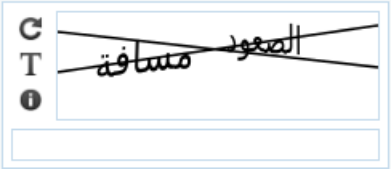
Captcha is created from a particular alphabet (e.g., Chinese, Arabic, and so on) and the users are then required to recognize this string and type it in their own languages to pass a test. However, Algwil et al. [108] investigated many real-world Chinese Captchas using Convolutional Neural Networks and showed that most of them are not secure.

Shirali-Shahreza et al. [43], Khan et al. [44], ArCaptcha [45], and Hsoub Captcha [46] are examples on Arabic Captchas (see Fig. 7). Yet, the recent work [47] has reported that all previously proposed Arabic Captcha schemes are not secure, being particularly vulnerable to segmentation attack.

(a) Persian/Arabic Captcha

(b) Arabic Captcha

(c) ArCaptcha



(d) Hsoub Captcha

Fig. 7. Examples of Arabic Captcha schemes

Recently, Shi et al. [48] introduced a novel adversarial Captcha scheme named aCaptcha. In this scheme, adversarial examples are elaborately injected to text-based Captchas to fool the machine learning techniques into producing wrong results..

Similarly, Kwon et al. [49] designed a new scheme to generate text Captcha using adversarial example techniques such as the fast-gradient sign method (FGSM), iterative FGSM, and the DeepFool method. Despite such

mechanisms add a little bit of noise to the original Captcha image, it is still easy to read by human, but not by a machine.

The same group [50] also applying *style transfer learning* in the Captcha domain, in which they generated a new Captcha image via merging the content feature of the original Captcha image with the style feature of another Captcha image.

The above and other recent research [51][52][53] have undoubtedly illustrated that deep learning techniques are extremely vulnerable to adversarial examples, which can be utilized as a defense mechanism against deep learning methods.

4.2. Image-based Captcha

The underlying principle in this category of Captcha is to exploit the ability of the superiority of human over machine to semantically interpret pictures. To solve an image-based Captcha challenge, a user is asked to categorize or recognize some images or objects as distinct from others based on their characteristics. Such tasks are easy to solve by humans, however they are still unable to accomplish by computers. Thus, image-based Captchas improve usability levels across different devices.

However, to achieve a satisfactory security level in image-based Captcha, a sufficiently large database of images should be used to avoid displaying the same image many times to users. Additionally, various effects are typically applied to the images such as rotation, overlapping, adding lines, distortion, blurring, and so on, in order to make image classification/recognition procedures more challenging to computers. Further, more advanced actions usually need to be completed by the user to solve the challenge; for

example, drag and drop, rotate image, mouse area selection, clicking on image or objects, match pictures with labels, and so forth.

Many image Captchas have been proposed over recent years. ESP-PIX[12] is an early well-known example of the image Captcha. The user is asked to choice a common word that best describes four similar subject images randomly selected from a large database. Yet, a random guess attack may break this Captcha due to the limited image categories in the chosen list.

ARTiFACIAL [55] is new image Captcha based on detecting the human face and facial features. The user is asked to detect the face and click on the four corners of the eyes as well as two corners of the mouth to pass the test. However, machine learning attacks [4] were able to break it with a reasonable success rate.

Along the same lines, Deapesh and Kris [57], Darryl et al. [58], and Guido et al. [59] designed different image Captchas based on a human face recognition/classification. In these Captchas, the user is required to either match distorted facial pictures of many people, correctly chose all the avatar faces from a number of mixed pictures of human and avatar faces, or categorize a group of pictures on the basis of gender and age.

Ritendra et al. [60] developed another novel image Captcha, called IMAGINATION. A user is required to correctly accomplish two click-annotate stages to solve the challenge (see Fig. 8 (a)). Unfortunately, it has been successfully broken by automated attacks in [4].

Implicit Captcha [62] is another kind of image Captcha, where the user is asked to click on a specific part of a given picture or click on a particular word within a picture that is made up of several words. However, this

scheme cannot be used in large-scale applications due to that the reference points need to be prepared manually by humans.

Image classification is another approach in the image-based Captcha category. An example of this approach is Microsoft ASIRRA [63], which asks users to select cats from a set of 12 images of cats and dogs. Nevertheless, ASIRRA Captcha has been broken in [64].

Confident Captcha [65], is a Captcha design that is built on image semantics. The user is asked to click those pictures out of a total of nine according to a given description (see Fig. 8 (b)). The major issue with this Captcha is its scalability.

In a similar approach, the reCaptcha (version 2 and version 3) service from Google [66] has used image-based to protect web services, in which the suspicious users are required to choice some pictures that best match a keyword in the text description (see Fig. 8 (c)). However, the reCaptcha version 2 has already been broken successfully in [67] and version 3 has also been broken successfully in [68].

(a) IMAGINATION Captcha (b) Confident Captcha (c) reCaptcha v2

Fig. 8. Examples of image-based Captcha schemes

Orientation-based Captcha schemes are another form of image challenge, where the user is required to recognize and correct the orientation of a number of misoriented images. Gossweiler et al. [69], Sketcha scheme [70], PiSHi Captcha [71] and image flip Captcha [72] are examples of the orientation-based Captcha designs. A great feature of these Captchas is that they are label-free. However, the images used must be cautiously selected to avoid ambiguity.

Tang et al. [73] proposed a new image-based Captcha design named SACaptcha that is based on on neural style transfer technique.in this scheme, the user is required to click foreground style-transferred areas in a synthetic image based on a given description.

Likewise, Ray et al. [74] designed a Style Matching Captcha, called SMC, using the same technique as the previous one. The challenge can be solved by matching the style image applied in the Neural Style Transfer method along with the content image. In other words, the user must understand the semantic correlation between the content and styled output image.

Some other image-based Captcha methods were also proposed, but most of these are designed in a similar fashion to the afore-mentioned schemes.

To summarise, all image-based Captchas can be classified into three categories: Click-, Slide-, and Selection-based Captchas. Surprisingly, Zhao et al. [75][76] reveal the vulnerability of the three image-based Captcha categories, in which their attacks achieved highly success rate on a variety of real-world popular image Captchas from the three categories, including ReCaptcha v2/v3 from Google, Facebook, China Railway, and etc.

4.3. Audio-based Captcha

This category of Captcha exploits the superiority of humans over computers to Automatic Speech Recognition (ASR) technologies in distinguishing spoken words or letters and/or digits in the presence of noise. To solve a sound-based Captcha challenge, an audio clip made up of a series of distorted words or characters spoken by different people is presented to the user, who has to type the characters spoken in the sound clip. There are many countermeasures that can be used to confuse ASR systems such as background noise, various speakers for each letter, random intervals between letters, and so on.

Sound-based Captchas are often used as a non-visual alternative for visually impaired users. Therefore, most popular websites such as Google, Yahoo and Microsoft offer both visual and audio Captcha schemes in their challenges, allowing the user to select which one (s)he prefers to use. Interestingly, eBay statistics have shown that almost 1% of its Captcha were consumed by users who prefer to solve audio Captcha challenges over their text-based counterparts [77]. However, images and sound alone cannot provide full accessibility, since users who have problems with both their vision and hearing cannot solve either.

Early efforts towards building sound Captcha schemes were the two simultaneously presented pieces work by Chan [78] and Daniel et al. [79] at the first HIP Conference. Based on the ASR limitations in understanding synthesized utterances within a noisy environment, Chan proposed the use of a digit-sequence utterance generated by a text-to-speech synthesizer in a noisy background. The sound challenge is then presented to the user, who is asked to listen to and input the digits spoken. Daniel et al. proposed the use

of hard problems derived from the natural language processing where human ability vastly outperforms that of computers. More precisely, a simple spoken question based on shared domain knowledge is synthetically generated and rendered to the user, for instance: "*what number comes after (or before) x?*", where *x* is a random integer number. The user first needs to process the audio clip, semantically understand the question, and then input the correct answer. Recently, Fanelle et al. [80] and Alnfiai[81] also proposed some various designs of sound-based Captcha schemes for people with visual impairments. In fact, there are few security investigations of audio-based Captcha schemes in the literature [82][83][84] that show a wide range of them were broken with high success rates.

4.4. Motion-based Captcha

Motion-based Captcha schemes exploit the gap in perceptual ability between humans and computers in recognizing a movie's semantic content to verify whether the user is a human or a robot. Motion in video makes understanding semantic items (e.g., animated object, moving text, translating an action, and so forth) extremely difficult for computers, yet very easy for humans because of their innate perceptual abilities in detecting complex patterns within motion scenes. Animated video challenges in this category can be rendered to users in various formats such as GIF, Flash movies, Java Applets, HTML5, and so on.

Many motion-based Captchas have already been proposed and developed in the literature and in real-life applications. An example of animated Captcha was proposed by Athanasopoulos [85] to avoid laundry attacks. In this scheme, a Java applet shows some randomly moving items on a changing background. The user must click one of these items based a given text.

Shirali-Shahreza et al. [86] proposed a video Captcha based on describing actions of a person. That is, a short movie of an actor performing a certain action along with a list of sentences describing various actions are shown to the user, who is asked to select the proper sentence to describe the action.

Kluever et al. [87] suggested a similar approach to design a novel Captcha using content-based video labelling. Their Captcha shows a YouTube video to the user, who is asked to type three descriptive tags that they feel best describe its contents (see Fig. 9 (a)). The user must match any of the three submitted words with one of the author-supplied labels to pass the test.

NuCaptcha [88] is a prominent commercial service that serves millions of video challenges daily. Its approach is based on a brief video display of a text moving from right to left on a different animated background. The user is then required to recognize and type the last characters of the moving text (typically coloured in red), as shown in Fig. 9 (b). As in the reCaptcha v3, NuCaptcha utilizes a behavioural analysis system to detect inhuman interactions with the platform, which in turn shows easy challenges to legitimate users and increasingly difficult ones to suspected abusers.

(a) Video Captcha (b) NuCaptcha

Fig. 9. Examples of motion Captcha schemes

4.5. Cognitive Captcha

Cognitive-based Captcha tests typically involve a more involved mental process (such as thinking and reasoning) to accomplish a certain cognitive task. Over the past 20 years, a wide variety of cognitive-based Captcha schemes have been proposed that require advanced human cognitive processing capabilities such as semantic interpretation of texts and pictures, performing calculations, solving puzzles, and so on.

Linguistic Captcha schemes (Captcha challenges in the text domain) are a major class among the family of cognitive-based challenges. It is worth noting that text-based Captcha schemes may be differentiated from linguistic Captcha schemes; while the former are images based on the visual recognition of distorted text, the latter employ standard character encoding schemes to present challenges in plain texts on a web page. Although the linguistic Captcha schemes can be easily solved by blind and/or deaf people, the generation of these Captcha tests is not an easy task.

Among a variety of Captcha schemes in the text domain is an earlier work by Godfrey [89], who introduces three Captcha proposals as follows: the "*Find the Bogus Word*" Captcha, the "*Find the Coherent Sentence*" Captcha, and the "*Remove the Inserted Words*" Captcha.

In practice, the Web service `TextCaptcha.com` [90] has been developed to provide textual logic-based questions that are accessible to everyone. Service's database is supported by over 180 million questions. Its questions typically use maths and simple riddles, such as, "*What is 8 minus six?*".

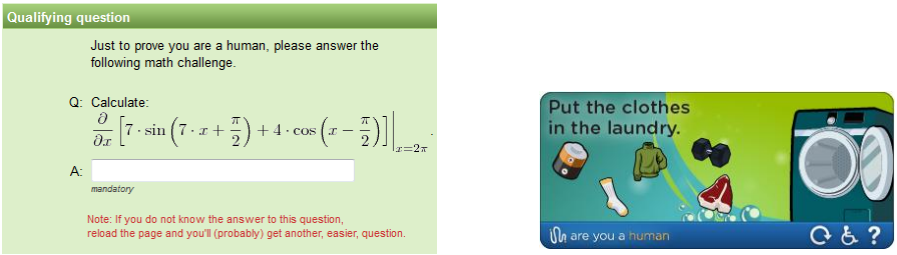
An interesting Math Captcha has been deployed to protect the registration process for the Quantum Random Bit Generator Service [91]. In this scheme, a complex mathematical equation, as shown in Fig. 10 (a), is

presented to the user, who has to correctly solve and type the answer to pass the challenge and register with the service. In fact, such Captcha seems to be difficult for ordinary users to solve. However, an attack [92] was able to successfully break it.

Wang et al. [93] introduced a visual reasoning Captcha scheme that is based on both computer vision and natural language processing. In this Captcha, the user is required to find specific object(s) in an picture based on a given question. Unfortunately, this Captcha was broken In [94].

zxCaptcha [95] is a Captcha test that combines the properties of text-, image-, and cognitive-based Captcha schemes. It shows nine images to the user , each image containing groups of text. Each text group contains 3-5 characters. The user has to choose all corresponding images in the correct order based on the text-based Captcha and their subject background.

Interestingly, some Captcha designs frame the puzzle as a game to make Captcha-solving an enjoyable activity for the user. An example is the PlayThru Captcha from the company Are You a Human [96]. As shown in Fig. 10 (b), this Captcha asks users to accomplish a simple and funny task. However this Captcha was broken in [97].



(a) Math Captcha (b) PlayThru Captcha

Fig. 10. Examples of cognitive-based Captcha schemes

5. CAPTCHA SCHEMES ON MOBILE DEVICES

Since 2009, the dominance of mobile devices within technology space has been ever-increasing, while the desktop's share of web traffic has steadily decreased. According to the web analytics company StatCounter, mobile and tablet internet usage surpassed that of desktops for first time in October 2016. That is, the combined traffic from mobile and tablet devices accounted for 51.3% of internet usage worldwide, compared to 48.7% by desktop computers [98]. Even more, in July 2023, mobiles accounted for 56.8% of traffic, against 43.2% for PCs according to StatCounter [99].

Therefore, Captcha tests should be developed to be easily serviceable and solvable across multiple devices. However, conventional text-based Captcha schemes in their current designs are not suitable to work effectively with small touch screen devices. Simply, they have several problems as a result of the limited input and output capabilities of small devices. That is, both the text-based challenge and the virtual keyboard which, individually, typically occupy almost half of the display, are being shown on the same small screen. Accordingly, the user usually needs to zoom and pan to scrutinize the distorted text; however, the keyboard impedes the Captcha and the auto-correct feature may additionally alter the entered text. Moreover, the user must switch between numbers and letters on the visual keyboard while typing the solution [100]. All these issues are, in fact, a key source of user frustration and annoyance, which in turn may result in the abandonment of the use of the services that contain Captcha tests, the loss of visitors to websites and, therefore, considerable economic losses.

Accordingly, it has become hard to ignore the importance of the use of Captcha tests on mobile devices. For this reason, various Captcha schemes

have been proposed in order for them to be well-suited for use with the touch screens of mobile devices. In other words, the majority of these non-text-based Captcha schemes are principally designed to use mouse-based input, which means they can be solved with drag/drop or clicks of a mouse, fingertip or stylus on a touch screen device.

For instance, Chow et al. [101] introduced a generic approach for turning regular textual Captcha schemes into clickable ones. That is, a grid of textual Captcha challenges (e.g., a 3×4 grid - see Fig. 11 (a)) is rendered to users, who must click on some grid elements that satisfy certain specific requirements (e.g., Captcha images which represent real English words).

Drawing Captcha [102] is another example designed for small devices. In this scheme, a large number of dots are randomly drawn on a noisy background. The shapes of some dots are slightly different from others (e.g., a few diamond-shaped dots versus many square dots), as shown in Fig. 11 (b). The user is required to connect these few distinct dots to each other to pass the test. However, this Captcha was broken in [103].

Desai and Patadia [104] proposed a novel Captcha named drag-and-drop (DnD) Captcha, in which a distorted text image, similar to standard Captcha images along with character blocks and blank blocks as shown in Fig. 11 (d), are presented to the user, who must recognize the distorted text, and then drag and drop the character blocks into their respective blank blocks as per the order they appear in the Captcha image.

Truong et al. [105] introduced a novel interactive Captcha called iCaptcha, where a user is asked to interactively solve a traditional text-based Captcha in multiple steps. In each step, several character buttons are retrieved and shown to the user (see Fig. 11 (f)). The user must then click on the

corresponding character button, as per the order they appear in the Captcha image.

In 2015, Leiva and Álvaro [106] developed *μCaptcha*, in which a random mathematical expression is generated and presented on a web canvas. To pass the challenge, a user must draw the mathematical expression on a touch screen using, for instance, their finger, a stylus, or even a mouse on a PC. Fig. 11 (e) illustrates an example of a μCaptcha challenge.

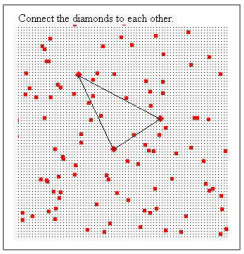
GISCHA is a gamified Captcha variation for handset devices introduced by Yang et al. in [107]. In the GISCHA challenge, the user is prompted to fulfil a simple web-based game using simple arrow keys, mouse movements, or gestures, rather than inconvenient alphabet inputs. For instance, in the rolling ball game shown in Fig. 11 (c), the user must move the ball into the circular hole to pass the test.

Aburada et al. [18] suggested an interactive Captcha scheme for mobile devices. In this scheme, multiple moving objects are presented to the user, who must choose any object and track its movement with her finger through the touch panel for a definite period of time. The user passes the challenge If tracking success time is longer than the specified time threshold.

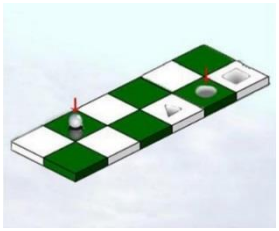
Feng et al. [25] introduced an orientation sensor-based Captcha scheme designed for mobile devices, called SenCaptcha. In this scheme, an animal image is shown to the users, who must tilt their device to direct a red ball to the target location (i.e., the center of the animal's eye) to pass the challenge.

Some other Captcha schemes designed for mobile devices are: *Captcha Zoo* and *Mobile Text Captcha* [103], *Highlighting* Captcha[54], *CAPTCHaStar* [56], *SeeSay* and *HearSay* Captcha [61].

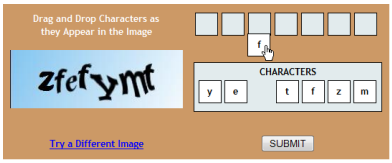
(a) Clickable Captcha



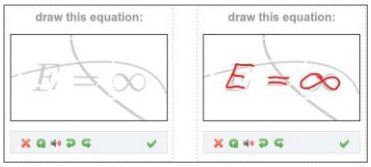
(b) Drawing Captcha



(c) GISCHA



(d) Drag and drop Captcha



(e) µCaptcha

(f) iCaptcha

Fig. 11. Captcha designed for mobile devices

6. CONCLUSION

This paper has reviewed the background and related work on Captcha schemes and the applications in which they have been utilized. It has also provided a detailed presentation of Captcha taxonomy, including those Captcha designs based on distorted text, image, audio, motion and cognitive tasks. Captcha issues on mobile devices have been also widely deliberated within this work. In a nutshell, many investigations have been done on Captcha security for both offensive and defensive purposes, and the arms race between Captcha designers and attackers is still ongoing.

REFERENCES

[1] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Computers beat Humans at Single Character Recognition in Reading based Human Interaction Proofs (HIPs)," in *2nd Conference on Email and Anti-Spam (CEAS)*, California, USA, 2005.

[2] J. Yan and A. S. El Ahmad, "Captcha robustness: A security engineering perspective," *Computer*. pp. 54–60, Feb-2011.

[3] J. Yan and A. S. El Ahmad, "Usability of Captchas or usability issues in Captcha design," *Proceedings of the 4th symposium on Usable privacy and security - SOUPS '08*. ACM, New York, NY, USA, 2008, pp. 44–52.

[4] B. B. Zhu, J. Yan, Q. Li, C. Yang, J. Liu, N. Xu, M. Yi, and K. Cai, "Attacks and design of image recognition Captchas," *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10*. ACM, New York, NY, USA, 2010, pp. 187–200.

[5] R. Pakdel, S. Ranjbar, and M. Hashemi, "A User-friendly Captcha Scheme Based on Usability Features," *Info. Technol. J.* , vol. 12, no. 1, pp. 61–70, 2013.

[6] "Mobile Future in Focus 2013," ComScore, Inc., 2013. [Online]. Available: http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Mobile_Future_in_Focus.

[7] Turing, A. M. "Computing Machinery and Intelligence-AM Turing," *Mind*, 59, no 236, 1950, pp. 433–460.

[8] Baird, H. & Popat, K. "Human Interactive Proofs and Document Image Analysis," In *International Workshop on Document Analysis Systems*, Springer Berlin Heidelberg, NJ, USA, 2002, pp. 507–518.

[9] Baird, H. "Complex Image Recognition and Web Security," *Data Complexity in Pattern Recognition*, London, Springer, 2006, pp. 287–298.

[10] Yan, J. Bot, "Cyborg and Automated Turing Test: (or 'Putting the Humanoid in the Protocol')", In *Security Protocols Workshop*, Springer Berlin Heidelberg, 2006, pp. 190–197.

[11] Coates, A. L., Baird, H. S. and Fatema, R. J. "Pessimal Print: A Reverse Turing Test," In *Proceedings of the Sixth International Conference on Document Analysis and Recognition*, Seattle, WA, 2001, pp. 1154–1158.

[12] Ahn, L. v., Blum, M. and Langford, J. "Telling Humans and Computers Apart Automatically," *Communi. of the ACM*, vol. 47, no. 2, 2004, pp. 57–60.

[13] Chew, M. & Baird, H. S. "BaffleText : A Human Interactive Proof," In *Proceedings of the International Society for Optical Engineering*, Santa Clara, California, USA, 2003, pp. 305–316.

[14] Naro, M. "Verification of a Human in the Loop or Identification via the Turing Test". Unpublished Draft From http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human_abs .html, 1996.

[15] Lillibridge, M. D., Abadi, M., Bharat, K. and Broder, A. Z. "Method for Selectively Restricting Access to Computer Systems," U.S. Patent 6195698 B1, Feb.27,2001.

[16] The Official Captcha Site [Online]. Available: http://www.captcha.net. [Accessed: 01-08-2023].

[17] Ahn, L. v., Blum, M. and Langford, J. "Telling Humans and Computers Apart Automatically or How Lazy Cryptographers Do AI," Sch. of Comp. Sci., Car. Mel. Uni., Pittsburgh, Pennsylvania. U.S., Tech. Rep. CMU-CS-02-117, 2002.

[18] Aburada, K., Usuzaki, S., Yamaba, H., Katayama, T., Mukunoki, M., Park, M. and Okazaki, N. "Implementation of Captcha suitable for mobile devices," IEICE Comm. Expr., vol. 8, no. 12, pp. 601–605, 2019.

[19] Baird, H. S. and Riopka, T. "ScatterType: A Reading Captcha Resistant to Segmentation Attack," In *Proceedings of the International Society for Optical Engineering*, San Jose, California, USA, 2005, pp. 197–207.

[20] Pinkas, B. and Sander, T. "Securing Passwords Against Dictionary Attacks," In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ACM, 2002, pp. 161–170.

[21] Wilkins, J. "Strong Captcha Guidelines," v1.2, 2009, pp. 1–18, 2009, [Online]. Available:http://www.123seminarsonly.com/Seminar-Reports/008/47584359-captcha.pdf

[22] Ahn, L. v., Maurer, B., Mcmillen, C., Abraham, D. and Blum, M. "reCaptcha: Human-Based Character Recognition via Web Security Measures". *Science*, vol. 321, no 5895, pp. 1465–1468, 2008.

[23] Ahn, L. v., Blum, M., Hopper, N. J. and Langford, J. "Captcha: Using Hard AI Problems for Security," In *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, pp. 2003, 294–311.

[24] Spamarrest [Online]. Available: http://www.spamarrest.com. [Accessed: 01-08-2023].

[25] eng, Y., Cao, Q., Qi, H. and Ruoti, S. "SenCAPTCHA: A Mobile-First Captcha Using Orientation Sensors," *the ACM on Intera., Mob., Weara. & Ubiqu.Tech.*, vol. 4, no. 2, pp. 1–26, 2020.

[26] Mori, G. and Malik, J. "Recognizing Objects in Adversarial Clutter: Breaking a Visual Captcha," In Pr*oceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Madison, WI, U.S., IEEE, 2003, pp. 1–8.

[27] Moy, G., Jones, N., Harkless, C. and Potter, R. "Distortion Estimation Techniques in Solving Visual Captchas," In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Washington, DC, U.S., IEEE, 2004, pp. 23–28.

[28] Baird, H. S., Moll, M. A. and Wang, S. Y. "A Highly Legible Captcha That Resists Segmentation Attacks," In *Second International Workshop on Human Interactive Proofs*, Springer, Berlin, Heidelberg, 2005, pp. 27–41.

[29] Baird, H. S., Moll, M. A. and Wang, S. Y. "ScatterType: A Legible but Hard-to-Segment Captcha," In *Proceedings of the Eighth International Conference on Document Analysis and Recognition*, Seoul, Korea, IEEE, 2005, pp. 935–939.

[30] Converse, T. "Captcha Generation as a Web Service," In *Human Interactive Proofs*, Springer, Berlin, Heidelberg, 2005, pp. 82–96.

[31] Yan, J. and El-Ahmad, A. S. "Breaking Visual Captchas With Naïve Pattern Recognition Algorithms," In *the Twenty-Third Annual Computer Security Applications Conference*, Miami Beach, FL, USA, IEEE, 2007, pp. 279–291.

[32] Simard, P. Y., Szeliski, R., Benaloh, J., Couvreur, J. and Calinov, I. "Using Character Recognition and Segmentation to Tell Computer From Humans," In *Proceedings of the Seventh International Conference on Document Analysis and Recognition*, Edinburgh, UK, IEEE, 2003, pp. 418–423.

[33] Yan, J. and El-Ahmad, A. S. "A Low-Cost Attack on a Microsoft Captcha," In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, U.S., ACM, 2008, pp. 543–554.

[34] Bursztein, E., Martin, M. and Mitchell, J. "Text-Based Captcha Strengths and Weaknesses". In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, Chicago, Illinois, U.S., ACM, 2011, pp. 125–138.

[35] El-Ahmad, A. S., Yan, J. and Tayara, M. "The Robustness of Google Captchas," Comp. Sci. at Newcastle Uni, Tech. Rep. 1278, 2011.

[36] Gao, H., Yan, J., Cao, F., Zhang, Z., Lei, L., Tang, M., Zhang, P., Zhou, X., Wang, X. and Li, J. "A Simple Generic Attack on Text Captchas," In *Network and Distributed System Security Symposium*, San Diego, CA, U.S., 2016, .

[37] Ferzli, R., Bazzi, R. and Karam, L. J. "A Captcha Based on the Human Visual Systems Masking Characteristics." In *Proceedings of the 2006 IEEE International Conference on Multimedia and Expo*, Toronto, Canada, IEEE, 2006, pp. 517–520.

[38] Martinović, G., Attard, A. and Krpić, Z. "Proposing a New Type of Captcha: Character Collage," In *Proceedings of the 34th International Convention*, Opatija, Croatia, IEEE, 2011, pp. 1447–1451.

[39] Chew, M. & Tygar, J. D. "Image Recognition Captchas". In *Proceedings of the 7th International Information Security Conference*, Springer, 2004, pp. 268–279.

[40] Rusu, A. and Govindaraju, V. "A Human Interactive Proof Algorithm Using Handwriting Recognition," In *Proceedings of the International Conference on Document Analysis and Recognition*, Seoul, Korea, IEEE, 2005, pp. 967–971.

[41] Rusu, A. and Govindaraju, V. "Handwritten Captcha: Using the Difference in the Abilities of Humans and Machines in Reading Handwritten Words," In *Proceedings of the Ninth International Workshop on Frontiers in Handwriting Recognition*, Kokubunji, Japan, IEEE, 2004, pp. 226–231.

[42] Thomas, A. O., Rusu, A. and Govindaraju, V. "Synthetic Handwritten Captchas," *Patt. Reco*., vol. 42, no. 12, pp. 3365–3373, 2009.

[43] Shirali-Shahreza, M. H. and Shirali-Shahreza, M. "Persian/Arabic Baffletext Captcha," *J. of Uni. Comp. Sci.*, vol. 12, no. 12, pp. 1783–1796, 2006.

[44] Khan, B., Alghathbar, K., Khan, M. K., AlKelabi, A. and AlAjaji, A. "Cyber Security Using Arabic Captcha Scheme," *Int. Ar. J. of Info. Tech.*, vol. 10, no. 1, pp. 76–84, 2013.

[45] ArCaptcha - Arabic Open Source Automated Test to Tell Computers & Humans Apart [Online]. Available: http://arcaptcha.anini.me. [Accessed: 01-08-2023].

[46] Hsoub Captcha [Online]. Available: https://captcha.hsoub.com/. [Accessed: 01-08-2023].

[47] Alsuhibany, S. A., Alrobah, N., Almohaimeed, F., Alduayji, S. and Parvez, M. T. "Evaluating Robustness of Arabic Captchas," In *the 2nd International Conference on Anti-cyber Crimes (ICACC)*, Abha, Saudi Arabia, IEEE, 2017, pp. 81–86.

[48] Shi, C., Xu, X., Ji, S., Bu, K., Chen, J., Beyah, R. and Wang, T. "Adversarial Captchas," *IEEE Tran. on Cyb.*, vol. 52, no. 7, pp. 6095–6108, 2021.

[49] Kwon, H., Yoon, H. and Park, K. W. "Captcha image generation: Two-step style-transfer learning in deep neural networks," *Sensors*, vol. 20, no. 5, pp. 1495, 2020.

[50] Kwon, H., Yoon, H. and Park, K. W. "Robust Captcha image generation enhanced with adversarial example methods," *IEICE Trans. on Info. & Sys.*, vol. 103, no. 4, pp. 879–882, 2020.

[51] Papernot, N., Mcdaniel, P., Jha, S., Fredrikson, M., Celik, Z. B Papernot, N., Mcdaniel, P., Jha, S., Fredrikson, M., Celik, Z. B. and Swami, A. "The limitations of deep learning in adversarial settings," In *Proceedings of IEEE European Symposium on Security and Privacy*, Saarbrucken, Germany, IEEE, 2016, pp. 372–387.

[52] Zhang, Y., Gao, H., Pei, G., Kang, S. and Zhou, X. "Effect of Adversarial Examples on the Robustness of Captcha," In *Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Zhengzhou, China, IEEE, 2018, pp. 1–10.

[53] Su, J., Vargas, D. V. and Sakurai, K. "One Pixel Attack for Fooling Deep Neural Networks," *IEEE Trans. on Evo. Comp.*, vol. 23, no. 5, pp. 828–841, 2019.

[54] Shirali-Shahreza, M. "Highlighting Captcha," In *Conference on Human System Interactions*, Krakow, Poland, IEEE, 2008, pp. 247–250.

[55] Rui, Y. and Liu, Z. "Artificial: Automated Reverse Turing Test Using Facial Features," *Multi. Sys.*, vol. 9, no. 6, pp. 493–502, 2004.

[56] Conti, M., Guarisco, C. and Spolaor, R. "CAPTCHaStar! A Novel Captcha based on Interactive Shape Discovery," In *Proceedings of the 14th International Conference on Applied Cryptography and Network Security*, Springer, 2016, pp. 611–628.

[57] Misra, D. and Gaj, K. "Face Recognition Captchas," In *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services*, Guadeloupe, French Caribbean, IEEE, 2006, pp. 122-127.

[58] D'Souza, D., Polina, P. C. and Yampolskiy, R. V. "Avatar Captcha: Telling Computers and Humans Apart via Face Classification," In *IEEE International Conference on Electro Information Technology*, Indianapolis, USA, 2012, pp. 1–6.

[59] Schryen, G., Wagner, G. and Schlegel, A. "Development of Two Novel Face-recognition Captchas: A Security and Usability Study," *Comp.&Sec.*, Elsevier, vol. 60, pp. 95–116, 2016.

[60] Datta, R., Li, J. and Wang, J. Z. "IMAGINATION: A Robust Image-based Captcha Generation System," In Pro*ceedings of the 13th annual ACM international conference on multimedia*, Singapore, ACM, 2005, pp. 331–334.

[61] Shirali-Shahreza, S., Penn, G., Balakrishnan, R. and Ganjali, Y. "Seesay and Hearsay Captchas for Mobile Interaction," In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Paris, France ACM, 2013, pp. 2147–2156.

[62] Baird, H. S. and Bentley, J. L. "Implicit Captchas," In P*roceedings of SPIE Document Recognition & Retrieval XII Conference*, San Jose, CA, 2005, pp. 191–196.

[63] Elson, J., Douceur, J. R., Howell, J. and Saul, J. "Asirra: A Captcha That Exploits Interest-Aligned Manual Image Categorization," In *Proceedings of 14th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, U.S., ACM, 2007, pp. 366–374.

[64] Golle, P. "Machine Learning Attacks Against the Asirra Captcha," In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, U.S., ACM, 2008, pp. 535–542.

[65] Confident Captcha [Online]. Available: http://confidenttechnologies.com/confident-captcha/. [Accessed: 27-09-2017].

[66] Google reCaptcha [Online]. Available: https://www.google.com/recaptcha/intro/. [Accessed: 01-08-2023].

[67] Sivakorn, S., Polakis, I. and Keromytis, A. D. "I am Robot: (Deep) learning to break semantic image Captchas,". In *Proceedings of the IEEE European Symposium on Security and Privacy*, Saarbruecken, Germany, IEEE, 2016, pp. 388–403.

[68] Akrout, I., Feriani, A. and Akrout, M. "Hacking Google reCaptcha v3 using Reinforcement Learning," arXiv:1903.01003, 2019. . Retrieved from https://arxiv.org/abs/1903.01003.

[69] Gossweiler, R., Kamvar, M. and Baluja, S. "What ' s Up Captcha? A Captcha Based On Image Orientation," In P*roceedings of the 18th international conference on World wide web*, Madrid, Spain, ACM, 2009, pp. 841–850.

[70] Ross, S. A., Halderman, J. A. and Finkelstein, A. "Sketcha: A Captcha Based on Line Drawings of 3D Models," In *Proceedings of the 19th international conference on World wide web*, Raleigh, North Carolina, U.S., ACM, 2010, pp. 821–830.

[71] Mehrnezhad, M., Ghaemi Bafghi, A., Harati, A. and Toreini, E. "PiSHi: Click the Images and I Tell if You Are a Human,". *Int. J. of Info. Sec.*, vol. 16, no. 2, pp. 133–149, 2017.

[72] Banday, M. T. and Shah, N. A. "Image Flip Captcha," *ISC Int. J. of Info. Sec.*, vol. 1, no. 2, pp. 105–123, 2009.

[73] Tang, M., Gao, H., Zhang, Y., Liu, Y., Zhang, P. and Wang, P. "Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha," *IEEE Tran. on Info. Fore. & Sec.*, vol. 13, no. 10, pp. 2522–2537, 2018.

[74] Ray, P., Bera, A., Giri, D. and Bhattacharjee, D. "Style matching Captcha: match neural transferred styles to thwart intelligent attacks," *Multimedia Systems*, 2023, pp. 1–24.

[75] Zhao, B., Weng, H., Ji, S., Chen, J., Wang, T., He, Q. and Beyah, R. "Towards evaluating the security of real-world deployed image Captchas," In *Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security*, Toronto, Canada, 2018, pp. 85–96.

[76] Weng, H., Zhao, B., Ji, S., Chen, J., Wang, T., He, Q. and Beyah, R. "Towards understanding the security of modern image captchas and underground captcha-solving services," *Big Data Min. & Anal.*, vol. 2, no. 2, pp. 118–144, 2019.

[77] Bursztein, E., Bethard, S., Fabry, C., Mitchell, J. C. and Jurafsky, D. "How Good Are Humans at Solving Captchas? A Large Scale Evaluation," In t*he 2010 IEEE Symposium on Security and Privacy*, Berkeley, California, IEEE, 2010, pp. 399–413.

[78] Chan, N. "Abstract of Sound Oriented Captcha," In *Proceedings of the First HIP Conference*, 2002, p. 35.

[79] Lopresti, D., Shih, C. and Kochanski, G. "Human Interactive Proofs for Spoken Language Interfaces," In *Proceedings of the First HIP Conference*, 2002, pp. 30–34.

[80] Fanelle, V., Shah, A., Karimi, S., Subramanian, B. and Das, S. "Blind and human: Exploring more usable audio Captcha designs," In *Proceedings of the 16th Symposium on Usable Privacy and Security*, 2020, pp. 111–125.

[81] Alnfiai, M. "A novel design of audio Captcha for visually impaired users," *Inter. J. of Comm. Net. & Info. Sec.*, vol. 12, no. 2, pp. 168–179, 2020.

[82] Bock, K., Patel, D., Hughey, G. and Levin, D. "unCaptcha: A Low-Resource Defeat of reCaptcha's Audio Challenge," In *Proceedings of the 11th USENIX Conference on Offensive Technologies*, Vancouver, BC, Canada, 2017.

[83] Bursztein, E., Beauxis, R., Paskov, H., Perito, D., Fabry, C. and Mitchell, J. "The Failure of Noise Based Non-continuous Audio Captchas," In *Symposium on Security and Privacy*, Oakland, CA, U.S., IEEE, 2011, pp. 19–31.

[84] Sano, S., Otsuka, T. and Okuno, H. G. "Solving Google's Continuous Audio Captcha With HMM-Based Automatic Speech Recognition," In *Advances in Information and Computer Security*, Springer, Berlin, Heidelberg, 2013, pp. 36–52.

[85] Athanasopoulos, E. and Antonatos, S. "Enhanced Captchas: Using Animation to Tell Humans and Computers Apart," In *the 10th International Federation for Information Processing (IFIP)*, Springer, Berlin, Heidelberg, 2006, pp. 97–108.

[86] Shirali-Shahreza, M. and Shirali-Shahreza, S. "Motion Captcha," In *the Conference on Human System Interactions*, Krakow, Poland, IEEE, 2008, pp. 1042–1044.

[87] Kluever, K. A. and Zanibbi, R. "Balancing Usability and Security in a Video Captcha," In *Proceedings of the 5th Symposium on Usable Privacy and Security*, Mountain View, California U.S., ACM, 2009, pp. 1–11.

[88] NuCaptcha [Online]. Available: http://www.nucaptcha.com/. [Accessed: 25-08-2017].

[89] Godfrey, P. B. "Text-Based Captcha Algorithms," In *First Workshop on Human Interactive Proofs*, 2002, Available Electronically:

http://www.aladdin.cs.cmu.edu/hips/events/abs/godfreyb_abstract.pdf.

[90] TextCaptcha v41 [Online]. Available: http://textcaptcha.com/. [Accessed: 01-08-2023].

[91] Stevanović, R. Quantum Random Bit Generator Service [Online]. Available: http://random.irb.hr/. [Accessed: 01-08-2023].

[92] Hernandez-Castro, C. J. and Ribagorda, A. "Pitfalls in Captcha Design and Implementation: The Math Captcha, a Case Study," *Comp. & Sec.*, vol. 29, no. 1, pp. 141–157, 2010.

[93] Wang, H., Zheng, F., Chen, Z., Lu, Y., Gao, J. and Wei, R. "A Captcha Design Based on Visual Reasoning," In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing*, Calgary, AB, Canada, IEEE, 2018, pp. 1967–1971.

[94] Gao, Y., Gao, H., Luo, S., Zi, Y., Zhang, S., Mao, W., Wang, P., Shen, Y. and Yan, J. "Research on the security of visual reasoning Captcha," In *Proceedings of the 30th USENIX Security Symposium*, 2021, pp. 3291–3308.

[95] Trong, N. D., Huong, T. H. and Hoang, V. T. "New Cognitive Deep-Learning Captcha," *Sens.*, vol. 23, no. 4, p. 2338, 2023.

[96] Are You a Human [Online]. Available: http://areyouahuman.com. [Accessed: 06-12-2013].

[97] Bypass Captcha, Areyouahuman Captcha System [Online]. Available: https://bypasscaptchasite.wordpress.com/2016/09/09/areyouahuman-captcha-system/. [Accessed: 01-08-2023].

[98] Mobile and Tablet Internet Usage Exceeds Desktop for First Time Worldwide [Online]. Available: http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide. [Accessed: 01-08-2023].

[99] Desktop vs Mobile Market Share Worldwide [Online]. Available: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet. [Accessed: 01-08-2023].

[100] Reynaga, G. and Chiasson, S. "The Usability of Captchas on Smartphones," In *International Conference on Security and Cryptography*, Reykjavik, Iceland, 2013, pp. 1–8.

[101] Chow, R., Golle, P., Jakobsson, M., Wang, L. and Wang, X. "Making Captchas Clickable," In *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, Napa Valley, Cl, U.S., ACM, 2008, pp. 91–94.

[102] Shirali-Shahreza, M. and Shirali-Shahreza, S. "Drawing Captcha," In *Proceedings of the 28th International Conference on Information Technology Interfaces*, Cavtat, Croatia, IEEE, 2006, pp. 475–480.

[103] Lin, R., Huang, S.-Y., Bell, G. B. and Lee, Y.-K. "A New Captcha Interface Design for Mobile Devices. In *Proceedings of the Twelfth Australasian User Interface Conference*, Perth, Australia, 2011, pp. 3–8.

[104] Desai, A. and Patadia, P. "Drag and Drop: A Better Approach to Captcha," In *Proceedings of Annual IEEE India Conference*, IEEE, 2009, pp. 1–4.

[105] Truong, H. D., Turner, C. F. and Zou, C. C. "iCaptcha: The Next Generation of Captcha Designed to Defend Against 3rd Party Human Attacks," In *IEEE International Conference on Communications*, Kyoto, Japan, IEEE, 2011, pp. 1–6.

[106] Leiva, L. A. and Álvaro, F. "μCaptcha: Human Interaction Proofs Tailored to Touch-Capable Devices via Math Handwriting," *Inter. J. of Hum. Com. Intera*., vol. 31, no. 7, pp. 457–471, 2015.

[107] Yang, T. I., Koong, C. S. and Tseng, C. C. "Game-Based Image Semantic Captcha on Handset Devices," *Multi. Too. & App*., vol. 74, no. 14, pp. 5141–5156, 2015.

[108] Algwil, A., Ciresan, D., Liu, B. and Yan, J. "A security analysis of automated Chinese turing tests," in *Proceedings of the 32nd annual conference on computer security applications*, United Stats, 2016, pp. 520-532.

[109] Algwil, A. and Yan, J. "Failures of security APIs: A new case," in *Proceedings of Financial Cryptography and Data Security*, Springer Berlin Heidelberg, 2016, pp. 283–298.

[110] Algwil, A. "Click-based Captcha paradigm as a web service," J. of App. Sci., vol. 35, no. 2, pp. 1-26, 2022.