



Practicality analysis of utilizing text-based CAPTCHA vs. graphic-based CAPTCHA authentication

Adnan Gutub¹ · Nafisah Kheshaifaty¹

Received: 10 May 2022 / Revised: 31 January 2023 / Accepted: 21 April 2023 /

Published online: 2 May 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

CAPTCHA as “Completely Automated Public Turing test to tell Computers and Humans Apart” is becoming an essential tool to help reduce many automated security authentication attacks. This research focused on studying differences running text-based CAPTCHA vs. graphical-based CAPTCHA in a utilization applicable dominant practicality manner. The ordinary text-based CAPTCHA works simple to prevent automated submissions as thought of being relatively easy to exploit. On the other hand, graphic-based CAPTCHA can be more preferred from users side, but can be providing some complexities making clear tradeoff analysis need between its usability and security. Even though graphic-based CAPTCHA has been generally considered as improvement of text-based CAPTCHA with respect to security, its usage is still not common, raising a practicality gap needing some search for comparing the two methods side by side comprehensively involving usability applicability and cultural preference beside security. In this regard, this research contributes towards filling the gap in knowledge running thorough local experimentations for finding different CAPTCHA performance tradeoffs in terms of real statistical humanoid possibilities of practicality easiness, repetition secrecy, and configuration solving timing, that can be used as basis for conducting further techno improvement human-oriented research.

Keywords Authentication · Access Control · Text Based CAPTCHA · Graphic Based CAPTCHA · Security · Usability

1 Introduction

Different user authentication schemes have become essential for safe and secure online access. One of these schemes is the *challenge-response authentication*, which is a family of protocols whereby one of the parties presents a challenge and the other party must provide a valid response to the challenge so as to be anti-robot authenticated [32]. An example is

✉ Adnan Gutub
aagutub@uqu.edu.sa

Nafisah Kheshaifaty
n_kheshaifaty@hotmail.com

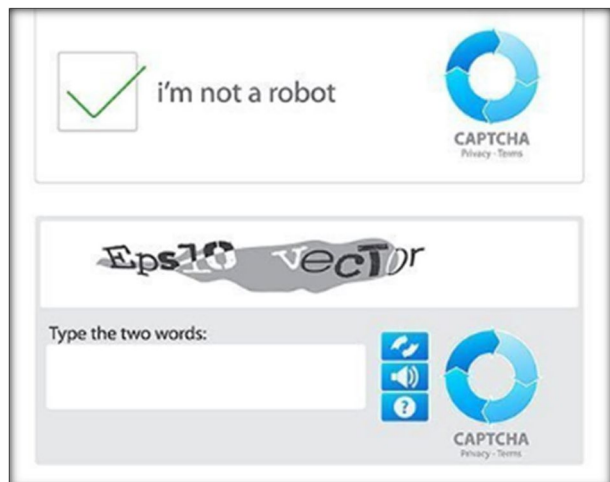
¹ Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia

the password authentication for emails, in which a user must provide a password so as to log in to the email platform, similar to public access authentication [43] avoiding high computation multi-threading vulnerability [1]. However, the common password is not highly secure, as it can be directly accessed within auto-robot databases [25]. Another example of challenge-response authentication is the CAPTCHA, which is an acronym for *Completely Automated Public Turing test to tell Computers and Humans Apart*. Today, most online current platforms use CAPTCHA to check on whether user is a human or not, to prevent flooding attacks such as a distributed denial of service (DDoS) attack, that uses many different unique IPs for attacks [42]. This is also to avoid the automatic consumption of all the available server resources, which can be affected technically as well as untechnical by cultural human acceptance situation.

This investigation experienced the two common types of CAPTCHAs testing 100 random attempts for both all tested on different locals to study the preference from the user point of view. The study focused on the mutual publicly known types of text-based CAPTCHA and graphic-based CAPTCHA. In fact, text CAPTCHA models are found implemented more than graphic CAPTCHAs in many IT applications as found preferred abiding with current network communication speeds and edge computing limitations as well as handheld mobile devices with restricted capabilities and resources [41]. This search reconsidered the CAPTCHA type appropriateness focusing on the user convenience point-of-view beside security, as practicality preparation for the ongoing advancements able to cope within coming networking speed, edge computing capabilities and mobile handy devices starvation situations for the internet of things progressive environments. The work goal is to test both strategies in real-life scenarios within making an overall comprehensive analysis from the users' side, finding confidentiality reappearance and hominid test acceptance as well as convenient challenge delay humans takes for effectiveness experimentation. An example of complex text-based CAPTCHA is shown in Fig. 1. Recall that ordinary CAPTCHA strategy purpose works to prevent automated attempts form submissions, but it should be essentially useful, i.e. possible to be solved correctly for relatively common human exploitation [42].

Timing is very important; whereas single individual can look at a limited number of text-images within a minute, when responding to particular text CAPTCHA, more individuals can look at more images per minute, i.e. when responding to the same CAPTCHA,

Fig. 1 Example of text-based CAPTCHA



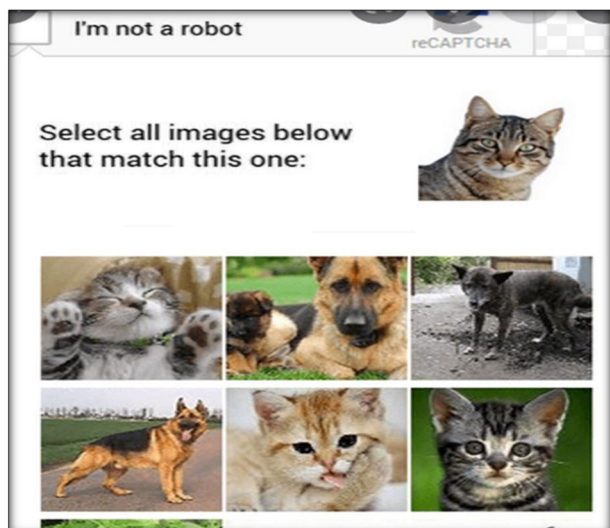
making the effectiveness of the CAPTCHA decreases the more the number of people respond to the CAPTCHA [23]. This timing issue can be affected by cultural background and situations as found providing interesting remarks of how familiar users are with text language letters shapes. As more humans work against specific CAPTCHA makes this CAPTCHA spoiled ineffective. This research can be providing justification for needing more efficient solution for the online users when using e-platforms [9].

Relatively, graphic-based CAPTCHA gives multiple images to deal with as human authentication tool, which is longer in time to be loaded causing noticeable delay due to existing networks and limited capabilities situations. An example of graphic-based CAPTCHA is shown in Fig. 2. Interestingly, when using graphic-based CAPTCHA, rather than text-based CAPTCHA, there might be a clear tradeoff between usability and security. It can be challenging to balance this tradeoff, as the usability considerations restrict IT designers to make schemes that are only as difficult as need to be; whereas security requirements and service providers push the authentication designers to raise the access control difficulty of the CAPTCHAs, aiming to prevent potential computer robot or automated programs [29].

Furthermore, while computing techniques and technologies have been constantly improving and evolving, humans on other hand need to rely on the inherent-abilities that they have, and it is unlikely that they will get better in solving the CAPTCHAs [8]. In one large scale research on the usability of CAPTCHA, part of the findings was that people usually find CAPTCHAs hard to solve, and that large portion of existing research mainly emphasized on making the CAPTCHAs hard for the machines, but did not consider this trade-off with humanoid convenience [12].

Although graphic-based CAPTCHA has generally been considered as an improvement of text-based CAPTCHAs with respect to the security [29], it's not utilized regularly due to more sophisticated graphics utilization presently suffering limitations of resources e-platforms, mobile/handheld devices capabilities, low-power nodes, medical critical situations, cloud/fog services, and dense networks circumstances. This gap did not consider the user convenience and practicality making our search contribution to focus on comparing the two methods side by side from user prospective with respect to both usability as well as

Fig. 2 Example of graphic-based CAPTCHA



security. This study contribution provides comparative study of text-based CAPTCHA versus graphic-based CAPTCHA detailing secrecy repetition, practicality easiness convenience, and common timing/delay of human puzzle solving affectability.

This paper presentation sections flow can be outlined as follows. Section 2 offers the literature review followed by Section 3 of the needed background for exploration anticipated studies. Section 4 discusses the proposed testing, detailing all examinations as well as convenience inspections to be run to understand the practicality situations. Section 5 deliberates the implementations of text-based CAPTCHA and graphic-based CAPTCHA challenging results in brief classified concise manner. Section 6 offers the analysis and comparisons in common background reasonable human-oriented style. Finally, Section 7 concludes the work.

2 Literature Review

CAPTCHA innovations for security application is being improving since some time. For example, Vaithyasubramanian [46] discussed audio CAPTCHA to prevent auto brute force attempts that proofed assistance for visually impaired individuals. This audio study of CAPTCHA has been challenged to noise sounds and pronunciation difficulties degrading its security success [20]. Further CAPTCHA structures adopted puzzle-tricks utilization [2], which can be ignited by involving image retrieval schemes using quantized bins of color pictures components and adaptive transforms [47]. This puzzle-based CAPTCHA displayed verification trails demanding puzzle-based widget for fitting to web optimization. Consequently, Cui [16] requested CAPTCHA to stop nasty commercial adds outbreaks by multi-level CAPTCHA procedures. The effort benefitted from image processing to simplify its utilization for different people cultures in an efficient construction [5]. Statistical formation of alteration object recognition based on spatial layout with respect to deep structures like texture, shape and color for object assortment [39] is a real breakthrough in this recognition authenticity attempts, as secrecy elaborated deeply in [4] and practically in [5].

Furthermore, CAPTCHA is found characterized linked to OCR representations modeled based on Boolean algebra [27]. This confirmation practice stopped general attacks with high governor ratio but suffered complex database which couldn't work for many supplementary e-practices. Likewise, Althamary [7] discussed integrating passwords to CAPTCHA characters showing different authentication strategy. However, its complexity constraint on treaty with human interface reduced its applicability though showed noteworthy expansion determining key logger, phishing, and password guessing attacks.

Kulkarni [30] offered an image-based CAPTCHA scheme adopting AI innovations. The exploration tested numerous graphical contests to alleviate many security issues suitable for public PC security needs. However, the disadvantage of this structure enforced various login passwords making the user inconvenient. Relatively, Lv [33] benefitted from users acceptance of English text CAPTCHA to comprehend via Chinese CAPTCHA proposing a cultural complex authentication philosophy. Some noise falsification has been tolerated by conventional neural network (CNN) methods enhancing the testing accuracy, but could not remove the design complexity. Moreover, Zhang [50] claims refining CAPTCHA involving separation within recognition but is remarked later suffering security consistency. On the same development line, Tirthani [45] studied secure authentication adopting Diffie Hellman and elliptical curve cryptography for uncommon keys management in order to avert DOS outbreaks. Congruently, Alta vista internet platform developed an isolated

CAPTCHA structure to avoid auto computer brute force attacks motivating Malutan [34] to research two dissimilar techniques of image-based passwords that shortened known COSS and CODP arrangements hoping to prevent shoulder surfing attacks. Although the literature reports many CAPTCHA works progresses advancing each other in some out-of-the-box means, most general attempts cornered their view and novelty to servers and networks e-availability limitations. Therefore, this consideration came to place comparing the top view of basic text-based CAPTCHA vs. image-based CAPTCHA aiming to redirect the focus in important user-oriented practicality remarks. In fact, this work can be the seed to build some application specific e-trust schemes. It can further involve combination of multimedia CAPTCHA types that can enhance the authentication security more for added practicality user friendly reworking.

3 Background

CAPTCHA is a type of contest response authentication in which one party asks a question (“challenge”) and the other party must provide a correct answer (“response”) in order to be authorized [28]. For a machine to pass the CAPTCHA, the machine must exhibit intelligent behavior that is equivalent to, or indistinguishable from, that of a human, as determined by the Turing test [9]. CAPTCHAs are, by definition, totally automated, needing little human maintenance or intervention to administer, resulting in cost and reliability benefits. However, when it comes to processing visual input, computer programs currently lack the sophistication that human minds possess in noticing patterns [42]. Whereas computers can be programmed to recognize letters and numbers, they stop recognizing them when they are obscured or distorted too much, like in what CAPTCHA does [29]. CAPTCHAs have several applications for practical security such as preventing comment spam in blogs and protecting email scraper; as bots become more sophisticated however, CAPTCHAs will need to keep up [12]. Two common forms of CAPTCHA are Text Based CAPTCHA and Graphic Based CAPTCHA.

3.1 Text based CAPTCHA

Text-based CAPTCHA is a program that protects websites against bots by generating and grading texts that humans can pass but current computer programs cannot [13], as example shown in Fig. 3. Humans can read the distorted text letters as the one shown: ‘V’ ‘P’ ‘E’ ‘P’, but current computer programs cannot. In other words, these ‘V’ ‘P’ ‘E’ ‘P’ letters is thought of interpreted wrongly if the computer auto systems are used making the security authentication process aware of breach possibility. It is to be mentioned that only CAPTCHA incorrectness cannot be used to assure attacks since some



Fig. 3 Text-based CAPTCHA illustration

given CAPTCHAs can be difficult to guess by humans too. This misleading occurrence is commonly resolved by allowing the user to ask for other CAPTCHA text whenever given one is hard to distinguish, i.e. this Fig. 3 example is given simple for clarification not being the normal case in real life situations. To be specific, this text CAPTCHA can be useful as long as computers are assumed unable to predict their letters focusing on making the auto brute force attacks at a standstill situation.

This type of CAPTCHA challenges the user to correctly evaluate and enter a sequence of letters or numbers visible in a distorted image on their screen [13]. Modern text-based CAPTCHAs are built in such a way that they necessitate the employment of three distinct factors at the same time: *invariant recognition, segmentation, and parsing* [17], in order to execute the task correctly and consistently.

Invariant recognition refers to the ability to recognize the large amount of variation in the shapes of letters [10]. There is an overwhelmingly large number of versions of each character that a human brain can successfully identify but the same is not true for a computer. Teaching it to recognize all those differing formations is a challenging task [17].

Segmentation, or the ability to separate one letter from another, is also made difficult in text CAPTCHAs, as characters are crowded together with no white space in between [10]. The *context* is also critical. The CAPTCHA must be understood holistically to correctly identify each character. For example, in one segment of a CAPTCHA, a letter might look like a “W”. Only when the whole word is taken into context does it become clear that it is ‘V’ and ‘V’ [17].

Parsing can be defined as the task of decomposing an image to its constituent visual elements [13].

Even in isolation, each of these difficulties poses a major difficulty to a computer: a CAPTCHA is tough to solve since all three factors are present at the same time. Humans, as opposed to machines, excel at this type of activity. While segmentation and recognition are two independent processes required for a computer to understand an image [8], they are part of the same process for a person.

3.1.1 Text Based CAPTCHA circumvention

Several techniques have been demonstrated for cheating the Text Based CAPTCHAs, including leveraging cheap human labor to detect them, exploiting technical errors that allow the attacker to totally skip the CAPTCHA, and eventually applying machine learning to develop an automated solver [44].

Machine learning-based attack There was no systematic technique for designing or testing CAPTCHAs in its early editions. As a result, many CAPTCHAs were of a constant length, and so automated tasks could be built to successfully make educated estimates about where segmentation should take place [11]. Other early CAPTCHAs had limited word sets, making the test considerably easier to cheat on. Others made the error of leaning too heavily on the image’s backdrop uncertainty. Algorithms were developed in each case to exploit these design weaknesses and successfully finish the task. These solutions, however, proved brittle, and minor adjustments to the CAPTCHA were quickly able to defeat them [42].

Cheap or unwitting human labor CAPTCHAs can be circumvented by transmitting them to a sweatshop of human operators who are paid to decipher text CAPTCHAs [18]. According to a 2005 study from a W3C working group, such an operator could validate hundreds

of documents every hour [48]. The University of California, San Diego, undertook a large-scale investigation of CAPTCHA farms in 2010 and discovered that the retail price for completing one million CAPTCHAs might be as low as \$1000 [15]. Another method discussed is employing a script to re-post the target site's CAPTCHA as a CAPTCHA to a site owned by the attacker, which unsuspecting individuals visit and properly solve within a short period of time for the script to use. Due to the costs of acquiring enough visitors and sustaining a prominent site, this strategy is likely to be economically impractical for most attackers [48].

Outsourcing to paid services There are numerous Internet companies, such as 2CAPTCHA and DeathByCAPTCHA [38], which provide human and machine-backed CAPTCHA solving services for as little as \$0.50 per 1000 completed CAPTCHAs. These services provide APIs and libraries that allow users to integrate CAPTCHA circumvention into the technologies that CAPTCHAs were originally designed to stop.

Insecure implementation Howard Yeend has found two concerns with poorly designed CAPTCHA systems in terms of execution [31]. Some CAPTCHA protection systems can be circumvented without the use of OCR by simply reusing the session ID of a previously used CAPTCHA picture. CAPTCHAs on shared servers are also problematic; a security breach on another virtual host may render the CAPTCHA issuer's site vulnerable [24]. Users can alter the client to display the un-rendered text if part of the software creating the CAPTCHA is client-side (the validation is done on a server but the text that the user is required to identify is rendered on the client side). Some CAPTCHA systems save MD5 hashes on the client side [6], making the CAPTCHA vulnerable to brute-force attacks [31].

3.1.2 Notable attacks

There have been some notable attacks against various CAPTCHAs schemas. For example, Mori et al. published a paper in IEEE CVPR'03 detailing a method for defeating one of the most popular CAPTCHAs, EZ-Gimpy, which was tested as being 92% accurate in defeating it [35]. The same method was also shown to defeat the more complex and less-widely deployed Gimpy program 33% of the time [35]. However, the existence of implementations of their algorithm in actual use is indeterminate at this time. Another example is PWNtcha, which has made significant progress in defeating commonly used CAPTCHAs, which has contributed to a general migration towards more sophisticated CAPTCHAs [38].

3.1.3 Security and usability

A key requirement of an effective CAPTCHA is that users are able to solve the challenge with a high degree of success, while the possibility of a computer program correctly solving it must be extremely low [28]. Chellapilla et al. suggest that the human success rate should be at least 90%, while the success rate of computer systems should ideally be less than 1 in 10,000 [14]. CAPTCHAs that are difficult or time consuming for legitimate users to solve are frequently seen as irritating and cause significant inconvenience to the users [15]. The trade-off between security and usability is difficult to strike, since security concerns urge designers to make CAPTCHAs more difficult in order to prevent computer programs, while usability concerns limit them to making a scheme only as difficult as it needs to be [15].

Furthermore, while technology and computational approaches are continually growing and improving, humans must rely on their innate abilities and are unlikely to improve at solving CAPTCHAs. According to a large-scale study on CAPTCHA usability, humans frequently find CAPTCHAs difficult to complete, and most research has mostly concentrated on making them tough for machines while paying little attention to usability difficulties [12].

3.1.4 Design considerations

A problem faced by CAPTCHA designers is that the security versus usability requirements is often in conflict [15]. A number of design considerations that deal with the trade-off between security and usability have been described.

Text familiarity Text-based CAPTCHAs generated with familiar text (for example, English terms) improve the usability of the final CAPTCHA. This is related to the fact that individuals prefer to read familiar material over unknown language. Language models, on the other hand, can be used to solve CAPTCHAs utilizing a collection of terms from a lexicon and holistic techniques. Text CAPTCHAs based on language models have been successfully overcome by researchers utilizing holistic ways of detecting entire words rather than identifying individual letters, which can be difficult if characters are very deformed or overlapping [13].

Color and visual clutter Color is a factor to consider when designing text CAPTCHAs [13]. Color is helpful for grabbing a user's visual attention from the standpoint of usability. At the same time, color can make a CAPTCHA more appealing and less obtrusive in its context of use, for example, by matching the color of a webpage. Furthermore, the use of color can potentially aid in the recognition and interpretation of text. Color, on the other hand, might have a negative impact on both the usability and security of a CAPTCHA [18]. This is due to the fact that misusing color can make text difficult to read for humans, for example, if the text color is identical to the background color. Colors can also present issues for persons who are colorblind. Simultaneously, color can result in a computer quickly distinguishing the text from the background, for example, if text is shown in a distinct color. It has been observed that the use of color in many CAPTCHAs is neither helpful nor secure [18]. Many CAPTCHAs additionally employ the use of visual clutter, such as background textures, noise, or lines connecting characters, in an attempt to thwart automated attacks. This can be damaging to the CAPTCHA's usability since humans may struggle to differentiate the text from the clutter. As a result, when building a CAPTCHA, the usage of color and visual clutter must be carefully examined. In general, if color or visual clutter does not add to the security of the CAPTCHA, its use may be purely aesthetic [29].

Distortion Affine transformations and character distortion are common strategies used to obstruct character recognition by an attacker's use of Optical Character Recognition (OCR) software [8]. Transformations, which include translation, clockwise/counterclockwise rotation, and scaling, are simple to solve for both computers and humans. As a result, these are frequently combined with some degree of distortion. Distortions are elastic deformations that can occur at the level of individual characters (i.e., local warping) or at the level of the entire text (i.e., global warping). In fact, the popular "reCAPTCHA" was originally designed to use warped strings that could not be identified by OCR. While text

distortion is used to prevent automated attacks [4], it has a negative impact on the usability of CAPTCHAs because people find it difficult to detect distorted text [13]. As a result, CAPTCHA systems usually give users many attempts to solve tasks.

Another factor to consider when dealing with distorted text from a usability standpoint is that the usage of specific character colors and visual clutter must be carefully examined when developing a CAPTCHA. In general, if color or visual clutter does not add to the security of the CAPTCHA, its use may be purely aesthetic. For example, digits and letters like the digit ‘0’ and the letter ‘O’, the digit ‘1’ and the letter ‘l’, are common causes of confusion. The same applies to upper- and lower-case pairs like ‘S’ and ‘s’, as well as ‘Z’ and ‘z’. Furthermore, certain character combinations like ‘VV’ can be misinterpreted as ‘W’, ‘rn’ as ‘m’, and so on [13].

3.1.5 Attack rate on text CAPTCHA

The security of CAPTCHAs has piqued the interest of scholars and practitioners alike since their introduction. As a result, a number of ways for attacking and defeating CAPTCHAs have been developed. Many academics have identified vulnerabilities in the design of CAPTCHAs that can be exploited, making them vulnerable to automated attacks. This section highlights some of the most important work in the field of text-based CAPTCHA assault [29].

Segmentation Techniques While many CAPTCHAs were created with the segmentation-resistant principle in mind, many of them were discovered to be vulnerable to segmentation attacks [44]. Researchers have demonstrated that design defects can be used to segment CAPTCHAs over the years:

De-noising algorithms: The use of noise is a frequent approach for perplexing segmentation algorithms [19]. As a result, de-noising techniques are utilized to reduce random noise from a CAPTCHA prior to segmentation. The Gibbs method, commonly known as the Markov random field approach, has been proven to be a very successful de-noising algorithm among the different de-noising techniques that have been developed over the years. This technique works by generating an energy value for each pixel based on its surrounding pixels and then eliminating pixels having an energy value less than a particular threshold. This technique is then continued until no more pixels can be removed. Other de-noising techniques include the dilate-erode method, which involves up sampling, dilating, and erasing a CAPTCHA image. As a result, noise, such as lines, is removed yet solid thick characters are retained [19].

Color Filling Segmentation (CFS): This method is similar to running a flood fill algorithm and is frequently used in conjunction with other segmentation approaches. The first stage is to recognize a pixel with a color associated with text in a CAPTCHA. After identifying the original pixel, all nearby pixels with the same color and related to it are traced. This process is repeated until all linked pixels have been recognized [12]. As a result, the connected pixels will disclose either individual or groups of related characters. In the latter scenario, because character-containing portions have been recognized, this technique will make other segmentation methods easier to use [31].

Segmentation based on patterns and shapes: This is a segmentation technique that seeks out patterns and shapes that can be utilized to describe specific features. Characters such as ‘a’, ‘b’, ‘d’, ‘e’, ‘g’, ‘o’, ‘p’, and ‘q’, for example, all feature loops or circular

sections, but characters such as I ‘j’, and ‘l’ often consist of small vertical blocks of pixels, and so on. Once the distinctive patterns and forms of the characters in a CAPTCHA have been identified, this information can be utilized to discover specific aspects in a CAPTCHA that can be exploited to aid in the segmentation process [48].

Segmentation-Resistance Background confusion: The goal of this method is to make it difficult to discriminate between the text and the background in order to avoid segmentation [44]. This can be accomplished through the use of a complicated background, the use of extremely similar colors for the text and the background, the addition of noise, or any combination of these. Bursztein et al. concluded in a study that backdrops should only be used for cosmetic purposes because using background confusion as a security technique does not improve the robustness of a CAPTCHA [11]. This is due to the fact that for usability, a human must be able to distinguish between the text and the background.

Using lines: To discourage segmentation, random lines that cross multiple characters are utilized. These can be little lines that cross a few characters or huge lines that cover the full CAPTCHA. The goal is to mislead segmentation algorithms by tying characters together [11].

Collapsing: The objective behind this method is to make a segmentation task more difficult by connecting or overlapping characters. This is often accomplished by reducing the space between characters, tilting and/or overlapping them, resulting in the characters being crammed together. This strategy is regarded as the most effective mechanism for discouraging segmentation [28].

According to the following research paper, “A low-cost attack on a Microsoft CAPTCHA” [49], the researchers said the following:

“Our simple attack has achieved a segmentation success rate of higher than 90% against this scheme ... For the first time, this article shows that CAPTCHAs that are carefully designed to be segmentation-resistant are vulnerable to novel but simple attacks.” [49] This article has proposed a general text-based CAPTCHA solver focused on CAPTCHA schemes with complex security features. The main aim of the study was to convert the complex CAPTCHAs into simple ones, thereby reducing the difficulty of character segmentation and recognition. To achieve this, the generative adversarial networks was used as the basic framework, combined with adversarial losses and cycle consistency losses to construct the CAPTCHA transformation model. [49].

We will analyze the present study by doing a test run of the code 100 times and do a screen capture and put all the hundred images in a figure on one page and notice whether the CAPTCHA has changed every time or in repetition.

3.2 Graphic CAPTCHA

Graphic-based CAPTCHAs were developed to replace text-based ones but could not due to current many limitations [44]. These CAPTCHAs use recognizable graphical elements, such as photos of animals, shapes, or scenes. Typically, image-based CAPTCHAs require users to select images matching a theme or to identify images that don’t fit. You can see an example of this type of CAPTCHA in Fig. 4. Note that it defines the theme using an image instead of text.

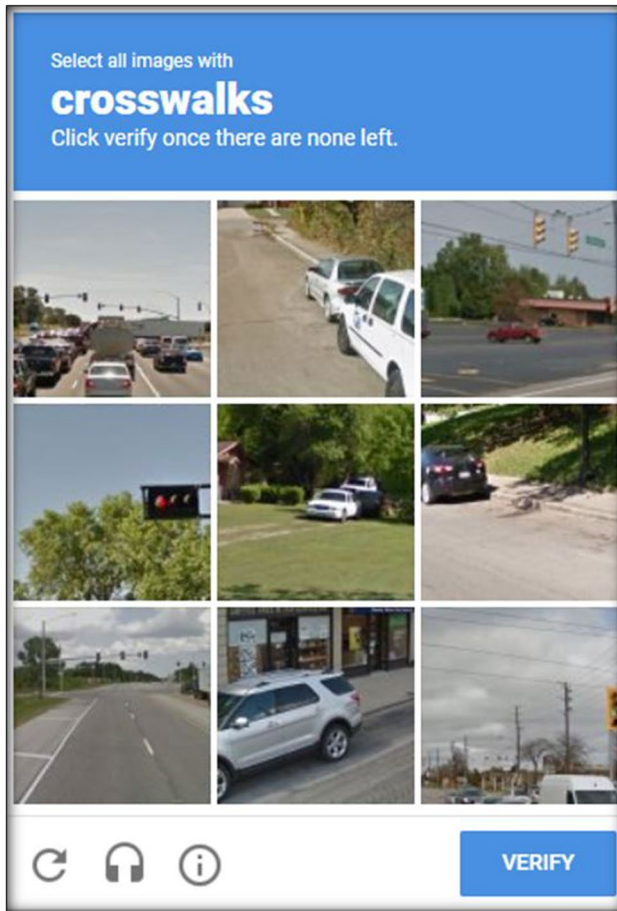


Fig. 4 Graphical-based CAPTCHA illustration

Picture-based CAPTCHAs are typically easier for humans to interpret than text-based [38]. However, these tools present distinct accessibility issues for visually impaired users. For bots, graphic-based CAPTCHAs are more difficult than text to interpret because these tools require both image recognition and semantic classification [44]. Over 100 million CAPTCHAs are displaying every day, on sites such as Facebook, TicketMaster, Twitter, 4chan, CNN.com, StumbleUpon, Craigslist (since June 2008), and the U.S. National Telecommunications and Information Administration's digital TV converter box coupon program website (as part of the US DTV transition).

Cognitive model of solving an image CAPTCHA Solid arrows represent information flow paths, dashed arrows denote mechanical control or connections as evident in Fig. 5 below. The processors run independently and in parallel both with each other and CAPTCHA environment module [44].

As bot-based threats have evolved, so have the CAPTCHA mechanisms intended to stop them. In its early forms, users were asked to read distorted text and submit it in a form.

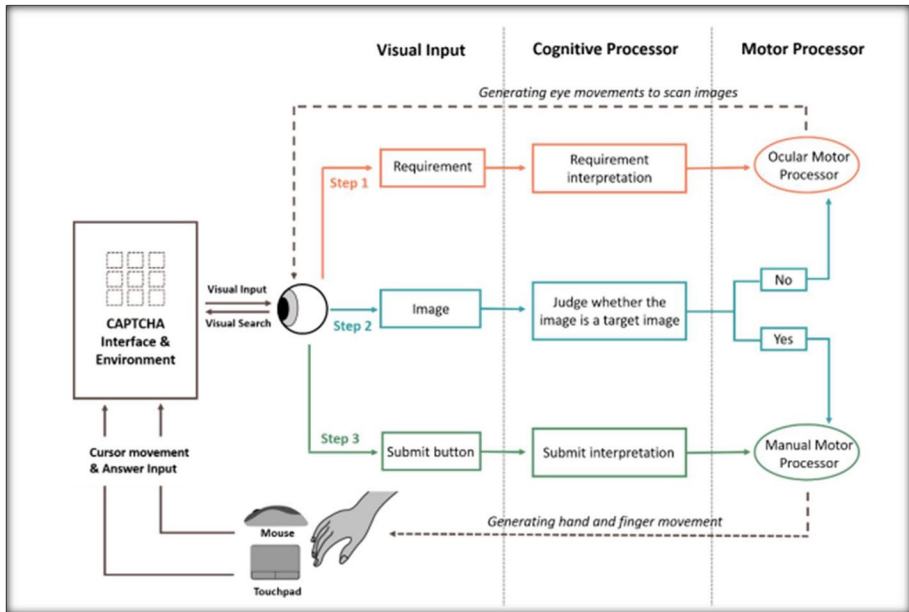


Fig. 5 General CAPTCHA interface environment

Today, Google reCAPTCHA represents the dominant form of CAPTCHA technology in use. One study found that, across one million of the world's top websites that employ CAPTCHA, Google reCAPTCHA was deployed by 94% of them [18].

As the complexity of the images increases, image processing techniques are developed, too. As improving the system to get more secure authentication mechanism, cracking systems are also improving timely in order to crack these new systems [10]. ReCAPTCHA mechanism which is developed by Google is one of the well-known systems. ReCAPTCHA mechanism has two main verification modules. First, of them requires only single click from the user for the authentication process. In this module, the system analyzes user's cookies and browser characteristics which are located in their browser [20]. In the analyzing part, confidence scores are calculated for every user. This score shows that request is originated from an honest user which is not suspicious or originated from a bot. For high confidence scores, the user is only required to click a checkbox. Users which have low-level confidence score respond to Image reCAPTCHA [10].

A report published in 2009 identified flaws in reCAPTCHA that allowed bots to obtain a solution rate of 18% [13]. In 2010, a report revealed a method to reverse the distortion given to photos, allowing a computer program to determine a legitimate response 10% of the time [15]. The reCAPTCHA system was changed on July 21, 2010, just before Houck was scheduled to speak about his solution. Houck changed his algorithm to an "easier" CAPTCHA to discern a legitimate response 31.8% of the time. Houck also emphasized the system's security countermeasures, such as a high-security lockout if an invalid response is delivered 32 times in a row. Adam, C-P, and Jeffball of DC949 gave a presentation at the LayerOne hacker conference on May 26, 2012, outlining how they were able to build an automated solution with a 99.1% accuracy rate. Their strategy was to analyze the audio version of reCAPTCHA, which is available for the visually challenged, using techniques

from machine learning, a subfield of artificial intelligence [28]. Just hours before their talk, Google launched a new version of reCAPTCHA, making significant changes to both the audio and visual portions of their service. The audio version has been lengthened from 8 seconds to 30 seconds in this release, making it much more difficult to understand for both humans and bots. In response to this and the following updates, DC949 members released two more versions of Stiltwalker that passed reCAPTCHA with accuracy rates of 60.95% and 59.4%, respectively. Google reCAPTCHA was updated within a few days of each break. According to DC949, they frequently reverted to previously hacked functionality [31].

Claudia Cruz, Fernando Uceda, and Leobardo Reyes released a paper on June 27, 2012, demonstrating an 82% accuracy system based on reCAPTCHA images. The authors have not said whether their method can answer recent reCAPTCHA photos, despite claiming that their work is intelligent OCR and resistant to some, if not all, changes in the image database [18].

In an August 2012 presentation given at BsidesLV 2012, DC949 called the latest version “unfathomably impossible for humans” – they were not able to solve them manually either. The web accessibility organization WebAIM reported in May 2012, “Over 90% of respondents (screen reader users) find CAPTCHA to be very or somewhat difficult.” DC949 described the current version as “unfathomably difficult for humans” in an August 2012 presentation at BsidesLV 2012 - they were also unable to solve them manually. According to the web accessibility organization WebAIM, “almost 90% of respondents (screen reader users) believe CAPTCHA to be very or moderately difficult.” Therefore, the contagious enhancement on the image CAPTCHA makes it more usable and secure [17].

4 Proposed testing research

This research testing aimed to compare between text-based CAPTCHA and graphic-based CAPTCHA with respect to practicality performance beside the normal security studies, i.e. aiming to specify the gap in exploration comparing the two methods side by side, trying to show fair consistencies analysis in terms security and usability from the user convenience point of view. In other words, this study contribution is detailing secrecy repetition, practicality easiness convenience, and common timing/delay of human puzzle solving affectability testing the two types of CAPTCHAs run 100 times each.

Text-based CAPTCHA is very simple as to be tested and implemented compared to graphic-based captcha, as user have to read within the text images and match it with standard character text letters or numbers [28]. Furthermore, text-based CAPTCHA adopted audio pronunciation pretending to allow disabled or weak vision humans to utilize to insert the letters by hearing them clearly. Normally, text-based or graphical-based CAPTCHA both assume having pictures as puzzle image given in randomized unexpected chunks which human recognition is requested to adjunct to integrate portions building the puzzle. Every CAPTCHA type has pros and cons where all are can be used in real-life applications though text CAPTCHA is currently more common. This work tested both CAPTCHA types of text vs. graphical elaborated thoroughly via running experimentations and survey testing showing all from user prospective. For research completeness analysis, the conditions of both types have been investigated as images to specify common comparison background as will be elaborated next.

Basing on CAPTCHA schemes mentioned above, the design factors evaluated here include the layout of images, number of images, size of images, tilting angle of images and color of images [12]. Because all those factors correlated with one another, for the evaluation of a certain factor, all other factors are set at a fixed value, which estimated the most usable or has been used by most previously reported image CAPTCHA designs. All images used in this study are obtained from the open access project Asirra [12]. To solve a test CAPTCHA, participants are instructed to select cat images from a set of candidate images that contain either cats or dogs.

4.1 CAPTCHA image testing layout

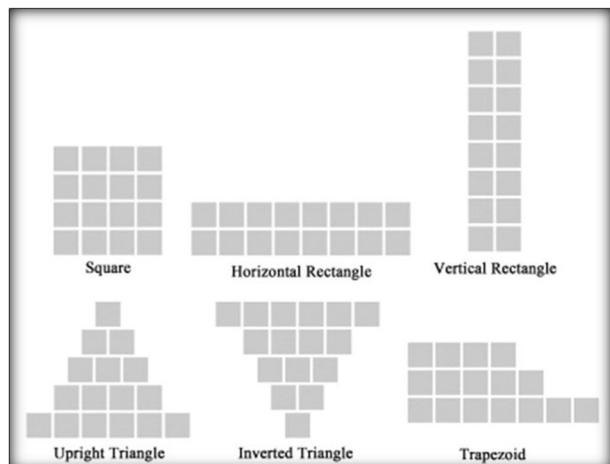
As depicted in Fig. 6, the six layouts evaluated in this study are Square (S), Horizontal Rectangle (HR), Vertical Rectangle (VR), Upright Triangle (UT), Inverted Triangle (IT), and Trapezoid (T). Each layout employs 16 images and the size of each image is 70 pixels \times 70 pixels. The six layouts evaluated in this study is shown in Fig. 6. Square (S), has 4 rows \times 4 columns; Horizontal Rectangle (HR), 2 rows \times 8 columns; Vertical Rectangle (VR), 8 rows \times 2 columns; Upright Triangle (UT), 5 rows \times 1~6 columns; Inverted Triangle (IT), 5 rows \times 6~1 columns and Trapezoid (T), 3 rows \times 4~7 columns. Represents the position of each candidate image. All images are colored and the subject of each image is not rotated (set at 0°).

4.2 CAPTCHA quantity and size

In this section, the numbers of candidate images in each CAPTCHA design are 4, 9, 16 and 25. Square layout is employed and the candidate images are arranged as 2×2 , 3×3 , 4×4 and 5×5 (rows \times columns). The size of each image is 70 pixels \times 70 pixels. All images are colored and the subject on each image is not tilted (set at 0°).

As shown in Fig. 7, images of five different sizes are evaluated: 25 pixels \times 25 pixels, 40 pixels \times 40 pixels, 55 pixels \times 55 pixels, 70 pixels \times 70 pixels, and 85 pixels \times 85 pixels. Except

Fig. 6 Image layout opportunities



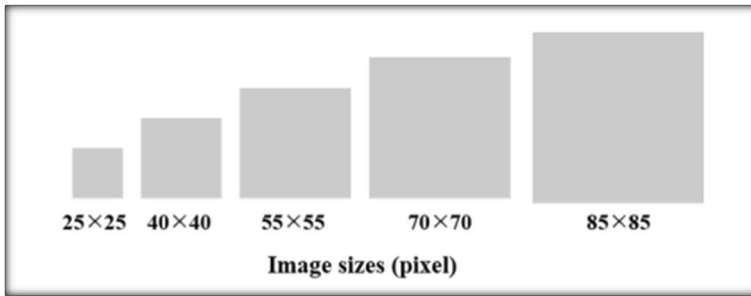


Fig. 7 Testing image size possibility

for the size of candidate images, all other design factors are kept the same: Square layout is employed which includes 9 images and arranges as 3 rows \times 3 columns. All images are colored and the subject on each image is not tilted (set at 0°). The five testing image sizes: 25×25 pixels, 40×40 pixels, 55×55 pixels, 70×70 pixels, and 85×85 pixels.

4.3 CAPTCHA tilting and coloring

As depicted in Fig. 8, the subject on each candidate image is tilted by a certain angle. The 8 angles evaluated are 0° , 45° , 90° , 135° , 180° , 225° , 270° , and 315° . Among all those tilting angles, 0° is chosen as the reference for which the subject of an image is at an ordinary post. All other tilting angles are rotated clockwise with respect to the reference one. Except for the tilting angle, all other design factors are kept the same: Square layout is employed which includes 9 images and arranges as 3 rows \times 3 columns. The size of each image is 70 pixels \times 70 pixels. Illustration of different tilting angles: 0° , 45° , 90° , 135° , 180° , 225° , 270° , and 315° .

All images are colored. The effect of colored or monochrome images are evaluated. Except for the color of candidate images, all other factors are kept the same: Square layout

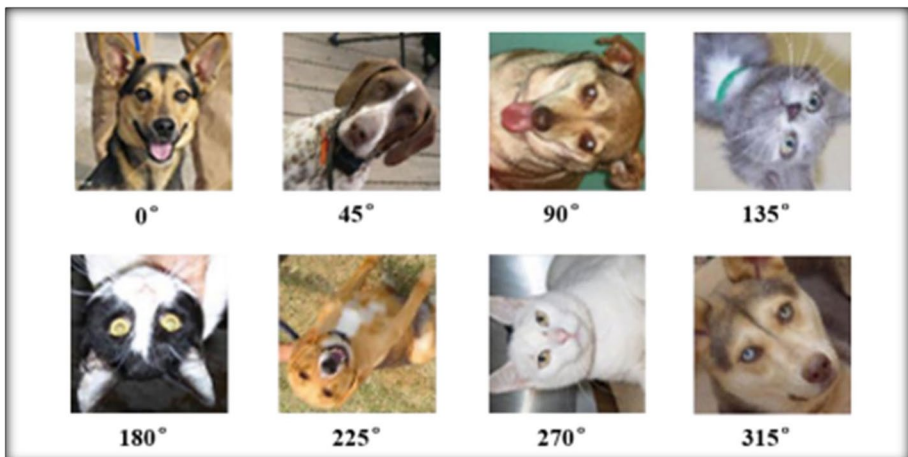


Fig. 8 Tilting angle of images

is employed which includes 9 images and arranges as 3 rows \times 3 columns. The size of each image is 70 pixels \times 70 pixels. The subject of each image is not tilted (set at 0°).

4.4 CAPTCHA satisfactory questionnaire

For each design factor of text and image CAPTCHAs, the corresponding satisfaction questionnaire focuses on the following three aspects:

- Q1. It is visually comfortable;
- Q2. It's easy to be recognized and solved;
- Q3. It's appropriate for application.

Participants are instructed to rate each design factor in terms of

- (Q1) visual comfort,
- (Q2) ease of use and
- (Q3) appropriateness for application.

The scores are defined by a 5-point Likert-scale (1 = strongly disagree, 5 = strongly agree) and all statements scored in a positive scale. The satisfactory result of each design factor is averaged among all the participants and presented in tables.

Through the following four dimensions: eye-tracking, efficiency, effectiveness, and satisfaction. The cognitive processes revealed by eye-tracking indicate that the distribution of eye gaze is equally assigned to each candidate image and irrelevant to the variation of image contents [22]. In addition, the gazing plot suggests that more than 70% of the participants inspected CAPTCHA images row-by-row, which is more efficient than scanning randomly. Those four-dimensional evaluations essentially suggest that square and horizontal rectangle are the preferred layout; image quantities may not exceed 16 while the image color is insignificant. Meanwhile, the image size and tilting angle are suggested to be larger than 55 pixels \times 55 pixels and within $\pm 45^\circ$, respectively. Basing on those usability experiment results, we proposed a design guideline that is expected to be useful for developing more usable image CAPTCHAs.

5 Investigation process results

The results of the text and graphics CAPTCHA human oriented tests have been collected and sorted out in two parts, in order to be listed all together in a practicality figure-of-merit percentages summary. The first part details the text CAPTCHA results and its data table. The second part will highlight the screenshot of the graphic CAPTCHA results and related information table. This focused study tried to be fair in its investigation classifications of testing implementation results sorting the lists into practicality ranges of five categories, very easy, easy, medium, hard, and very hard. Note that all outcomes shown in this section are from running random text CAPTCHA and graphic CAPTCHA codes for one hundred times each. A summary of the implementation results categories concluded the section as preparation for next section detailed analysis and comparisons.

5.1 Text CAPTCHA testing

This research Text CAPTCHA 100 tests snapshots are shown in Fig. 9. Every testing run have recorded five points of testing inputs, namely number, content, repeat, easy, and time, as shown in Table 1. The test number is recording text CAPTCHA simulation counting trail. The ‘content’ is presenting the exact text letters shown, used as main challenge to deceive the computer. The ‘repeat’ value indicated how many times this same CAPTCHA text has been nominated, assuming its repetition as occurrence frequency affecting the human familiarization perception may be degrading the randomization authentication security. The ‘easy’ input indicates the practicality user friendly real average noticing in statistical numeration, which ranges between 1 (very easy) to 5 (very hard). The ‘time’ highlights the time normally taken to solve the challenge correctly in seconds.

Table 1 results have been gathered from normal human average testing sessions. The study run its experimentations on random people voluntarily participated within this study for scientific knowledge development participation. Recall that the investigation run the text CAPTCHA code gathering testing inputs for one hundred dissimilar times, where the process have been supervised and observed fairly completing the table columns.

Based on Table 1 above, it remains evident that some CAPTCHA codes are easier to crack than others. The majority of the codes had zero repeat rate, implying that people got them the first time. In the easy spectrum, the lowest score was 1 while the highest was 5.



Fig. 9 Text CAPTCHA testing benchmark

Table 1 Text CAPTCHA experimentation statistical data

#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)
1	XNZC	0	1	0.5	35	COBY	0	3	0.8	69	OPMK	0	3	0.8
2	CNNK	0	1	0.5	36	PNEX	0	1	0.8	70	XCPJ	0	4	0.9
3	ZMNC	0	1	0.5	37	BUMM	0	3	0.8	71	WDCN	0	1	0.5
4	MRNJ	0	1	0.5	38	TRDP	0	3	0.8	72	DSZT	0	3	0.8
5	TRXC	0	2	0.7	39	ZXHC	0	1	0.5	73	UOAS	0	1	0.5
6	SJHN	0	3	0.8	40	KKDB	0	3	0.8	74	ZOJA	0	2	0.7
7	TEUE	0	1	0.5	41	ZOCW	0	5	1.3	75	TREO	0	1	0.5
8	HUTC	0	2	0.5	42	WZVZ	0	3	0.8	76	TDRU	0	3	0.8
9	ZJBZ	0	4	0.9	43	RHXY	0	3	0.8	77	AURX	0	3	0.8
10	VPEP	0	1	0.5	44	VZWE	0	3	0.8	78	YWVH	0	1	0.5
11	ABNX	0	1	0.5	45	JICA	1	5	1.2	79	MTHX	0	5	1
12	PCBH	0	2	0.6	46	YEHT	0	3	0.8	80	ROWK	0	2	0.7
13	OXCN	0	1	0.5	47	OYJK	0	2	0.6	81	TRTK	1	5	1.3
14	EMJR	0	2	0.6	48	TNUZ	0	2	0.6	82	DNCW	0	5	1.2
15	WXRE	0	3	0.8	49	KXCR	0	1	0.5	83	SUPB	0	1	0.5
16	AADB	0	1	0.5	50	CAPA	1	5	1.2	84	XSNM	0	1	0.5
17	XMAH	0	1	0.5	51	ZVCP	0	2	0.6	85	HXPR	0	3	0.8
18	CJNZ	0	1	0.5	52	WWJJ	0	1	0.5	86	KVPC	0	2	0.6
19	TWVK	0	3	0.8	53	TWKV	0	3	0.8	87	RJJC	0	1	0.5
20	WXDJ	0	2	0.7	54	BSKJ	0	3	0.8	88	SHEE	0	1	0.5
21	ZAME	0	2	0.7	55	MREY	0	4	0.9	89	KJCO	0	5	1.3
22	PCZP	0	4	0.9	56	VTVT	0	4	0.8	90	SCNX	0	2	0.6
23	NAYJ	0	4	0.9	57	HYZP	0	4	0.9	91	YZEN	0	1	0.5
24	YVVT	0	5	1.5	58	SKCY	0	1	0.5	92	JBCU	1	5	1.3
25	WUEU	0	1	0.5	59	JKTC	0	3	0.8	93	NKXZ	0	2	0.6

Table 1 (continued)

#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)
26	NPSN	0	1	0.5	60	BVXP	1	5	1	94	DUYR	0	3	0.8
27	EDYN	0	3	0.8	61	HNVK	0	2	0.6	95	VWUB	0	4	0.8
28	UMAE	0	1	0.5	62	ASRY	0	4	0.9	96	XPDO	0	4	0.8
29	WUWU	0	1	0.6	63	AAYY	0	1	0.5	97	KXEA	0	4	0.8
30	CHUN	0	4	0.9	64	NX SX	0	3	0.8	98	NJYB	0	1	0.5
31	HVHJ	0	3	0.8	65	DARH	0	1	0.5	99	BTHE	0	1	0.5
32	DRTX	0	4	0.9	66	BNYZ	0	3	0.8	100	YBHU	1	5	1.5
33	EMTS	0	4	0.9	67	CDHU	0	2	0.7					
34	XJAT	0	1	0.5	68	YOSD	0	1	0.5					

Also, the least time taken to complete the text CAPTCHA was 0.5 seconds, while the highest was 1.5. These results are beneficial since they will allow a further study into the effectiveness of text CAPTCHAs such as when they are appropriate to use.

5.2 Graphic CAPTCHA testing

Figure 10 showcases a screenshot of the results generated from the graphic CAPTCHA tests. These one hundred graphic CAPTCHA images examinations looked significantly for the ease convenience, solving time taken, and the repeat frequency rate, similar in principle to the text CAPTCHA experimentations listed in Table 1. In other words, Table 2 ratings have been collected from regular human attempts random participations detailing the trialing statistical data to be prepared and classified for the comparisons and analysis serving this research.

Every testing run have recorded five points of testing inputs, similar to Table 1 data given earlier. Table 2 test number is recording the graphical CAPTCHA simulation counting trail. The ‘content’ is presenting the exact graph-image provided by the system randomly, used to betray the computer insight. The ‘repeat’ rate indicated if this same CAPTCHA graph has been observed given before. The ‘easy’ grade specifies the

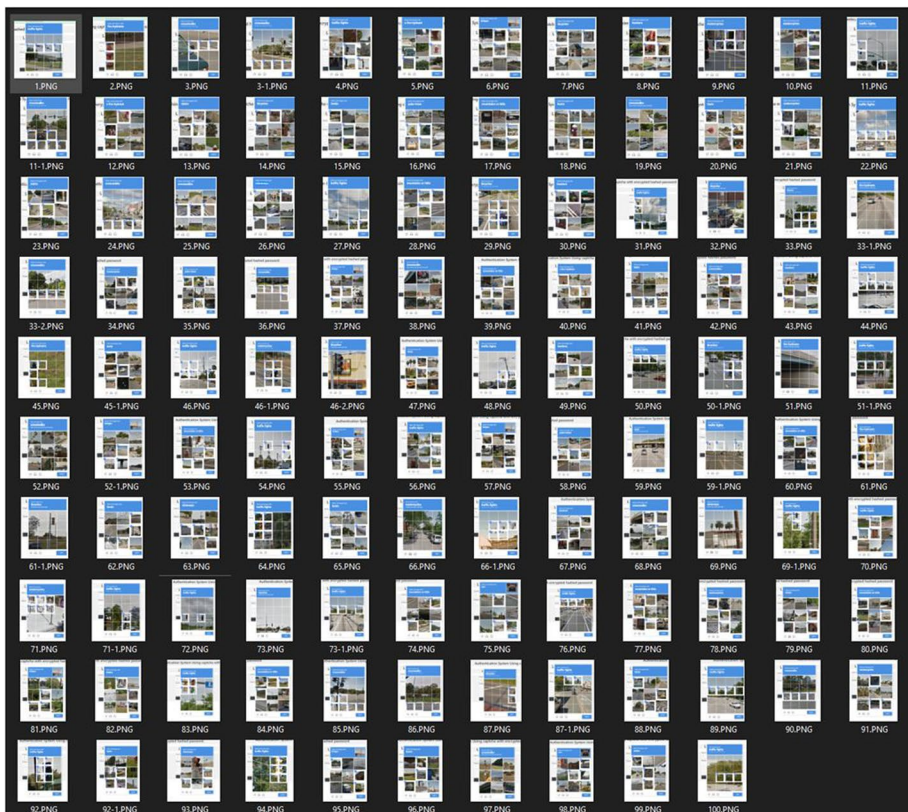


Fig. 10 Graphic CAPTCHA testing benchmark

Table 2 Graphic CAPTCHA experimentation statistical data

#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)
1		0	3	6	35		0	1	4	69		1	4	8
2		0	1	4	36		0	1	3	70		0	1	4
3		1	4	8	37		0	3	7	71		1	3	7
4		0	1	3	38		0	1	3	72		0	1	3
5		0	3	8	39		0	1	3	73		1	4	8
6		0	1	4	40		0	1	3	74		0	1	4
7		0	3	7	41		0	1	4	75		0	5	9
8		0	1	4	42		0	1	3	76		0	1	4
9		0	1	4	43		0	2	5	77		0	3	7
10		0	1	3	44		0	5	9	78		0	1	4
11		0	1	4	45		1	5	9	79		0	1	4
12		0	2	5	46		2	4	8	80		0	1	4
13		0	1	4	47		0	1	4	81		0	1	3
14		0	1	4	48		0	3	6	82		0	1	3
15		0	5	9	49		0	1	3	83		0	4	8
16		0	3	7	50		1	3	6	84		0	1	3
17		0	4	8	51		1	3	7	85		0	3	7
18		0	1	4	52		1	5	9	86		0	1	4
19		0	4	8	53		0	1	3	87		1	4	8
20		0	1	3	54		0	3	7	88		0	1	4
21		0	1	4	55		0	1	4	89		0	1	3
22		0	3	6	56		0	1	4	90		0	1	4
23		0	3	7	57		0	1	3	91		0	3	7
24		0	1	3	58		0	1	4	92		1	3	7
25		0	3	7	59		1	5	13	93		0	1	3

Table 2 (continued)

#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)	#	Content	Repeat	Easy	Time(s)
26		0	4	8	60		0	3	7	94		0	1	3
27		0	3	7	61		1	3	6	95		0	1	3
28		0	4	8	62		0	2	5	96		0	1	4
29		0	3	6	63		0	1	4	97		0	2	5
30		0	1	4	64		0	1	3	98		0	1	3
31		0	5	9	65		0	1	3	99		0	3	7
32		0	1	5	66		1	5	10	100		0	1	4
33		1	5	10	67		0	1	4					
34		0	3	7	68		0	3	6					

Table 3 Practicality (easiness) classification implementation result

	Text CAPTCHA	Graphic CAPTCHA	Estimated Avg Difference	Rate Comments
Very Easy	35%	53%	18%	Higher Graphic CAPTCHA
Easy	16%	2%	14%	Higher Text CAPTCHA
Medium	24%	24%	0%	Similar for both CAPTCHAs
Hard	14%	10%	4%	Higher Text CAPTCHA
Very Hard	11%	9%	2%	Higher Text CAPTCHA

practicality user friendly noticing in statistical estimation, which ranges between 1 (very easy) to 5 (very hard). The ‘time’ archives the normal try human delay, in seconds, to understand the challenge and solve it appropriately.

The results of the graphic CAPTCHA test indicate that the easiness convenience was moderate since the lowest value was one and the highest five. Concerning the time, the lowest was sensed as 3 seconds and the highest as 13 seconds. The repeat rate for most of the images was zero, with the highest repeat rate as one, indicating rich images bank hinting higher secrecy. These results are helpful since they provide information on the performance of graphic CAPTCHA and the various improvement areas.

5.3 Classifications of testing implementation results

Trying to be fair, the research compares the results of the text CAPTCHA against the graphic CAPTCHA tests as average variable factors percentages listed in Table 3 and Table 4, in order to prepare the remarks for the detailed comparison and analysis presented in the coming section. Table 3 compares the two CAPTCHA schemes based on difficulty and easiness collected from the experimentation Table 1 and Table 2 before. Recall that these average estimation results were acquired after running the text and graphic CAPTCHA one hundred times each.

The results of this table indicate that graphic CAPTCHA was the easiest to pass the challenge at 53%, while the text CAPTCHA scored 35%. Moreover, text CAPTCHA had the highest percentage of very hard at 11%, compared to graphic CAPTCHA at 9%.

Similarly, Table 4 below provides a time comparison between text and graphic CAPTCHA results of the 100 testing trails. The summary outcomes indicate that graphic CAPTCHA took the shortest time of three seconds in 23% of the random occurrences, while the shortest text CAPTCHA findings could not be before five seconds for 35%. On the other extreme, the highest delay of ten seconds and above was noted for the text CAPTCHA runs of about 10% testing runs, whereas this timing for graphic CAPTCHA is only for 3%, indicating that text CAPTCHA took longer time to solve, as majority of the tests needing more than 10 seconds had not been solved.

Table 4 Timing classification of different implementation results

Time (s)	3	4	5	6	7	8	9	10 <=
Text CAPTCHA	0%	0%	35%	10%	6%	28%	10%	10%
Graphic CAPTCHA	23%	28%	6%	7%	16%	11%	6%	3%

6 Analysis and comparisons

During this study, the general impression considered is that the text CAPTCHA challenge was harmful to humans' eye making bad user experience [15]. Thus, CAPTCHA needs to make the user more comfortable increasing the ease of passing the challenge and of course consuming less time. In comparison, the graphic CAPTCHA gave a distinctive and attractive shape within the site. Moreover, it enhanced the user experience, thus providing greater convenience for the user and thus an easier test and less time, as mentioned earlier. Accordingly, this section provides comparisons between text CAPTCHA results overview and graphic CAPTCHA results overview detailing many interesting study factors not following the method of coronavirus impact on human feelings via deep learning critical analysis [26].

On the text-based CAPTCHA, the *easy factor* was found 35% of the occasions reported as very easy, and 16% were just easy. However, this easiness was affecting negatively on the security, as the generated letters can be easy for the robot to pass it using sophisticated OCR techniques. Therefore, this could be considered as a disappointment point in the text CAPTCHA.

Returning to the overview results, it was found that 24% showed medium difficulty, which can be considered acceptable in terms of usability and security. However, it remains a small percentage compared to the total number. Moreover, 14% of the results were difficult and 11% is very difficult. The noticeable implication was that it was very difficult for computers to pass these challenges that existed at such levels of difficulty. Whereas this could be considered to be a positive thing, however the problem is that it also meant that the possibility of the user to pass the challenges in this high difficulty level was almost impossible. This was due to the many complications and rendered visual effects which distorted the vision.

It becomes very apparent that the Graphic CAPTCHA won in the comparison of usability/security trade-off. As was previously expected, the visual effects that were added in the graphics made it more difficult for the robot to pass the test while maintaining ease for the user, which is the aim that we are looking for.

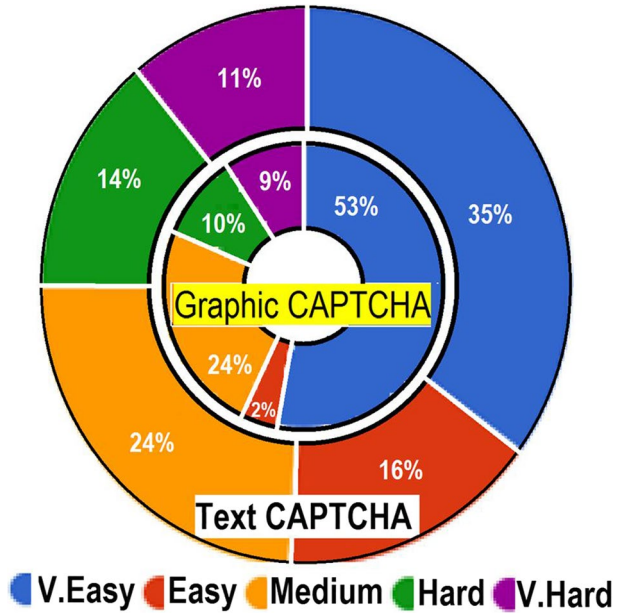
Nowadays, computer systems that require effective and secure access control are increasingly in demand. Due to a lot of data manipulation, ensuring safe access to sensitive information is a significant challenge in today's electronic platforms. As a result, many proposed techniques have had security issues, such as hacks that breach security and further modify sensitive information. The results of the study have followed a technical methodology for cost-effectively securing access to systems.

6.1 CAPTCHAs convenience comparison

The study compares the ease convenience based on the 100 tests of text and graphic CAPTCHAs, as visually summarized in Fig. 11. The text and graphic CAPTCHAs noted 11% vs. 9% very hard and 35% vs. 53% very easy, respectively. Interestingly, the medium level is the same for both CAPTCHA types. These indications assured graphic CAPTCHA challenges as being practically easier than text challenges. Therefore, the research recommendation insists on the importance of increasing difficulty, i.e. involving rational thinking, within graphic CAPTCHA challenges to guarantee more acceptable security.

The 100 tests detailed easiness practicality comparison chart for both text and graphic CAPTCHAs can be briefed as shown in Fig. 12. This chart (Fig. 12) proofs randomness of the testing runs scaling 'easy' on average 16% compared to 2% for text vs. graphic

Fig. 11 Easiness classification evaluations



CAPTCHAs, respectively. These CAPTCHA testing assessments observations assures that system designing cannot entirely rely on ease of use to offer reasonable security. Instead, this can be thought of as open challenge for future findings to put threshold and merits. The main point is to avoid potentially complicated implications balancing security and usability practicality trade-off based on the application precise utilization need.

The finding of 24% of the results being ‘medium’ difficulty can be considered as an acceptable situation in respect to both usability and security, but remains as small percentage compared to the total number of testing for every type. The research observed that

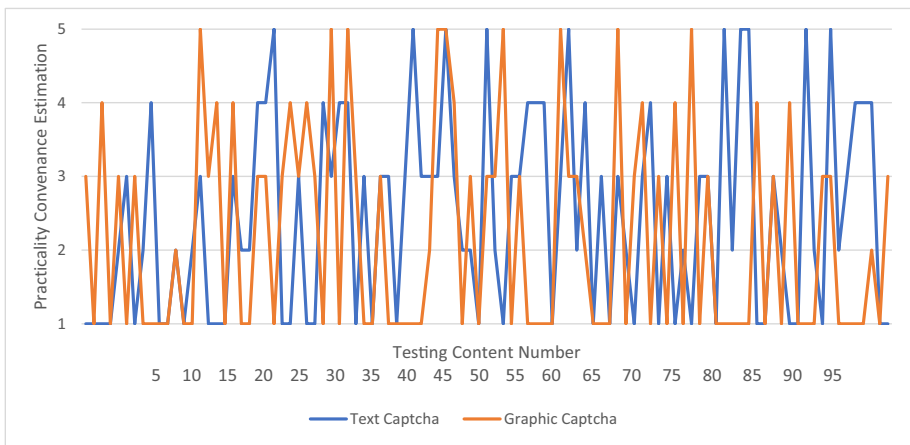


Fig. 12 Easiness overall practicality comparisons

‘very hard’ testing made it difficult for computers to pass the challenges too, which can be considered positive in security respect. However, since it causes inconvenience problem finding possibility of the user not passing the challenges making its practicality very low, i.e. suffering for normal people to grasp the complications distorting the vision. The study showed that more than half runs of the graphical CAPTCHA are building the real preference as well as providing acceptable security, because of difficulties for the robot to pass the graphic CAPTCHA challenges. The same implication applies to the medium level which reached 24%, as it is still save trade-off of usability and security trade off, even in the higher levels of difficulty. 10% of the results were difficult and 9% of the results were very difficult, which is a good percentage as the graphics with respect to the usability. This convenience impression can be shown clearly graph in Fig. 13 as summarizing the discussion above in a side-by-side analysis. Based on the debate arguments above, it remains evident that graphic CAPTCHA can be preferred human-wise easier than text CAPTCHA. This outcome can give hint that text CAPTCHA could be more secure than graphic CAPTCHA, remarking it is easier for people to interpret images compared to text.

6.2 CAPTCHAs delay comparison

The timing to run each of the 100 tests for both CAPTCHA experimentations is averagely classified in seconds as shown in Fig. 14. The outcomes were derived observing the time taken to complete every challenge correctly without any bias or interference.

Figure 14 indicates that the speed for solving graphic CAPTCHA challenge is higher than that of text CAPTCHA challenge. For instance, the average speed for answering graphic challenges vs. text challenges have been 51% vs. 45%, respectively. The medium/slow lowest value was 29% and 20% for the graphic challenge vs. 34% and 21% for the text challenges, respectively. These results are essential as showcase of longer time needed in solving CAPTCHAs of text than graphic based, which implies more security avoiding any eliminating machine-generated hacks.

Consider Fig. 15 showing the details of running the CAPTCHA tests for 100 times. The least time possible to solve the text challenge was 5 seconds, while it was 3 seconds for the graphical trials. Most text CAPTCHA attempts have been recorded for 5 and 8 seconds while the graphic CAPTCHA was mostly less around 3 to 4 seconds. Moreover, the results indicate that the number of people needing to access the CAPTCHA after 10 seconds are higher for text than graphic CAPTCHA supporting the same claim of graphical CAPTCHA preference in terms of timing delay. This reinsurance of visual graphical preference that are

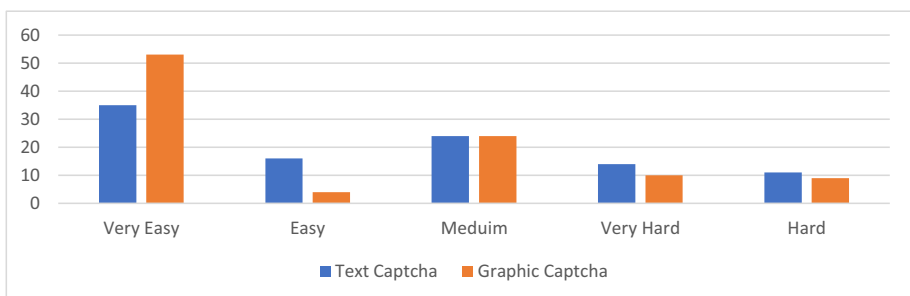


Fig. 13 Convenience observation assessments

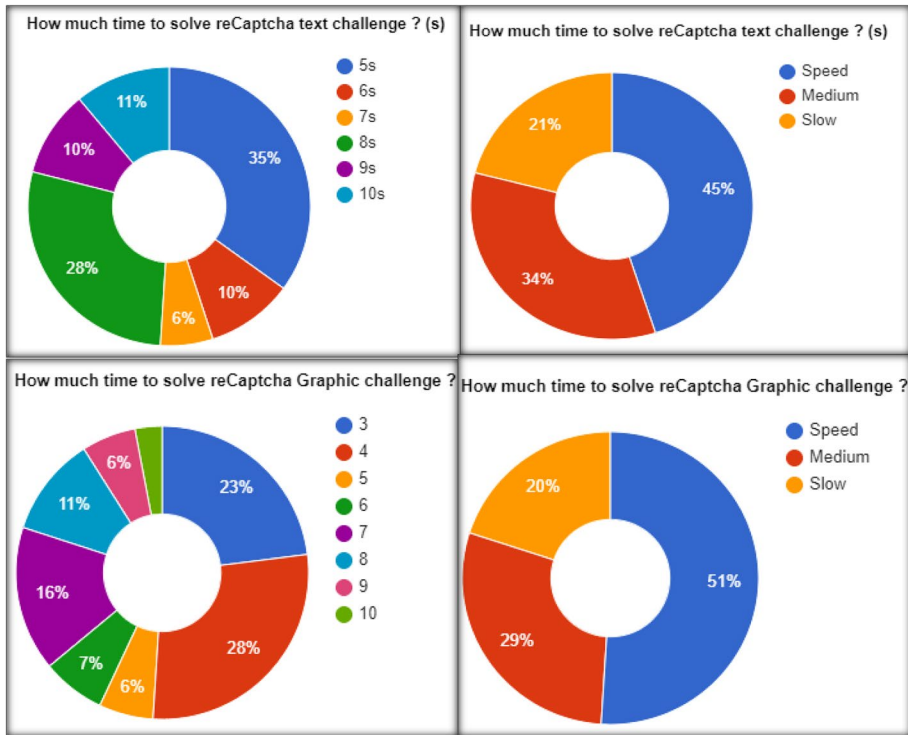


Fig. 14 Timing evaluations and classification analysis

common in human perception make it important to recommend adding difficulty for the robot to pass the test while maintaining ease for the user which is the real aim this study is demanding.

6.3 CAPTCHAs repetition comparison analysis

The CAPTCHA is supposedly given fully randomly by the system. Sometimes the CAPTCHA is found repeated that can be hinting the auto computing to acquire, i.e. via

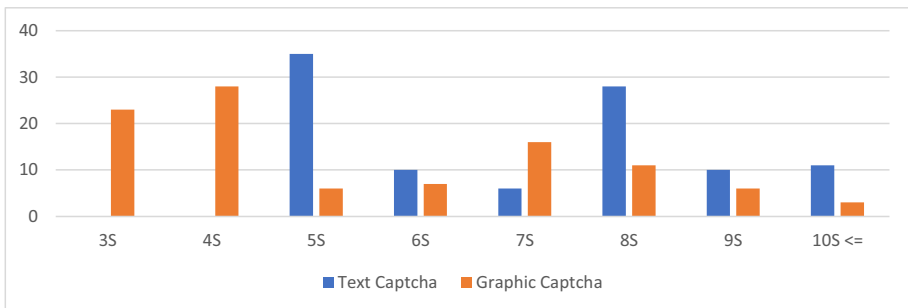


Fig. 15 Time factor in-depth assessment

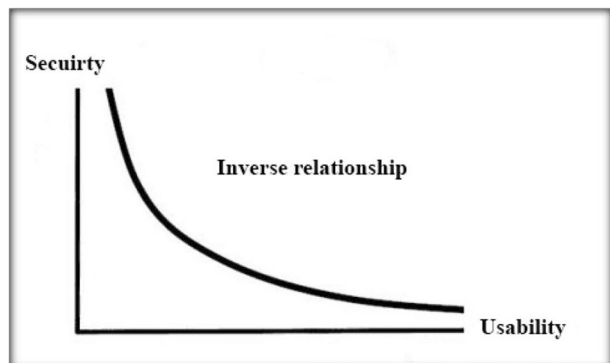
smart machine learning or AI techniques, making security possibility degradation. Accordingly, our 100 tests study verified the repetition rate and its experimentation occurrences between text and graphic CAPTCHA experimentations as noted 6% vs. 16%, respectively. We observed the number of times the same challenges were given as repeat testing degrading the overall security approximation. In fact, this issue can be worse as the case when the same person is getting the same exact challenge repeated making his life easier and can be a hint for the computer to use negatively. In general, from repetition frequency point of view, the investigation results indicate that text CAPTCHAs offer more security than graphic CAPTCHAs.

6.4 Tradeoff remarks

It is tough to strike a balance between security and usability [48]. When it comes to CAPTCHAs, the two metrics usually vary inversely: if more security is needed, its usability is sacrificed, and if more usability is attempted, the system suffers in security. The semantic gap, which is the difference between a human's and a machine's capacity to recognize visual content, is one measure of balance. In fact, any positive difference in human and machine achievement can be magnified to a gap arbitrarily close to one by serial repetition. The maximal gap represents the point at which human and machine performance is most dissimilar. However, a maximal gap may not occur for the most secure or most usable convenience conditions. Therefore, we can obviously see that there is an inverse relationship between the security and usability, as shown in Fig. 16, which is in line with research presented in [9].

Following the showing that word distortion-based CAPTCHAs are vulnerable to machine learning-based attacks, some researchers offered alternatives such as picture-recognition CAPTCHAs, which challenge users to recognize simple objects in the images shown. The justification for these approaches is that tasks such as object identification are often more difficult to execute than text recognition and hence should be more resistant to machine learning-based attacks [9]. To be consistent with all experimentation testing and general overview, the graphical CAPTCHA is more convenient than text CAPTCHA indicating more practicality, except in the case of repetition or OCR smart recognition that can be flipping this complete observation, as can be verified also text security study of [36] as well as hiding authentication of [21]. It is highly recommended to find systems that integrate text CAPTCHA with graphic CAPTCHA in order to gain benefits of both preserving highest possible security standards, following innovative strategy of safety traceability system through blockchain [40].

Fig. 16 Inverse relationship between the security and usability



7 Conclusion

This investigation examined running two types of CAPTCHAs tests trying 100 different random contents for each aiming fair relative comparative study remarks. The two types focused on text-based CAPTCHA and graphic-based CAPTCHA explorations with curiosity intention to be checking which CAPTCHA type is more practical as fast, secure and convenient, option to be recommended. Both CAPTCHA types are heavily used in today's online IT services for access control authentication [3]. Text CAPTCHA models are adopted common in many e-service cases as found fit more than graphic CAPTCHA especially for network communication and edge computing as well as handheld mobile devices with limited capabilities and resources. This research restudied the CAPTCHA suitability from the user convenience and security as practicality point of view. It started the in-depth human-convenience study relating the two approaches applicability side by side with respect to both timing delay and usability convenience. The research filled some of the misperception commonly stated in research directing proportional experimentation of text-based CAPTCHA versus graphic-based CAPTCHA describing security frequency, easiness handiness, and normal humanoid delay of CAPTCHA mystery solving convenience.

The research scope accommodated normal human interaction to sense the ability in preferring text-based CAPTCHA compares to graphic-based CAPTCHA pretending normal challenging real-life situations. The main research influence, from user's perception, can be note as indication that graphic-based CAPTCHA could be more practical than text-based CAPTCHA both in terms of usability and security, but not in terms of repetition frequency. Our CAPTCHA tests convenience recorded 'very easy' 53% vs. 35% of trails for graphic challenges vs. text ones, respectively, gaining 18% over all stimulating higher performance. Furthermore, the typical timing for responding to graphic tests vs. text trials have been 51% vs. 45%, respectively, making the graphic CAPTCHA run expected around 6% faster than text runs. On the other extreme, the randomness testing run scaling 'hard' and 'very hard' together remarking averages of 19% compared to 25% for graphic vs. text CAPTCHAs, respectively, representing that text CAPTCHA is having more complexity inconvenience than graphic CAPTCHA by approximately 6% too. Interestingly the medium suitability rough estimation is found exactly same for both types of CAPTCHAs settling around 24%. The medium and slow delay timing together added-up to 49% vs. 55% for graphic testing better than text challenges, respectively, making the summation performance surprisingly 6% better too. Moreover, the results designate that the number of people needing to access the CAPTCHA after 10 seconds are much more higher for text than graphic CAPTCHA proofing the same claim of graphical CAPTCHA preference in terms of usability timing delay as well as easiness convenience indicating higher practicality.

The study raised-up clearly the challenging equilibrium among security and usability involving CAPTCHA authentication. The two types involved within this exploration enforced the compromise phenomena between security and usability, which are found inversely proportional, making security be degrading as more usability convenience is requested. This stressed the semantic gap between humans and machines intellectual ability to distinguish visually observed content [37]. This motivation of competing smartness race between humanoid and robot's intelligence is raising further studies need based on these ambient advancements. Therefore, this finding from the comparative experimentation research contributes towards filling the gap in knowledge and the findings can be used as basis for conducting further research. Accordingly, in future related study, researchers can build more advancements making innovative graphics-based CAPTCHA explorations

considering specific applications, i.e. geared for efficiency of CAPTCHA specially using limited resources platforms, such as mobile devices, low-power nodes, medical situations, cloud services, and dense networks circumstances. This current real-world utilization is requesting access control authentication to be improving more as security and user experience is becoming involved more and more building proper Internet of Things and AI applications of our digital era automatic, robot and machine life cycles.

Acknowledgments Special thanks to the Computer Engineering Department at Umm Al-Qura University. All appreciation to the genius graduate students of Computer Engineering courses: Advanced Topics in Information Security (1400519) and MS Graduate Research Project (1403699-6), as their overall collaborative work remarked attractive contribution and completion used within this paper. Superior thanks to our great school, Umm Al-Qura University – Makkah, for supporting me by this sabbatical leave year (2022-2023) to focus completing work-out this cybersecurity research hoping to continue offering the MS graduate program as well as allowing for PhD, approved by Ministry of Education within Saudi Arabia, opening doors for progressive scientific activities.

Funding There is no funding source.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Informed consent Informed consent was obtained from all individual participants included in the study.

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Agreement We declare that this work is original and not considered to be published in any other publication media.

References

1. Abu-Hashem M, Gutub A (2022) Efficient computation of Hash Hirschberg protein alignment utilizing hyper threading multi-core sharing technology. *CAAI Trans Intell Technol* 7(2):278–291. <https://doi.org/10.1049/cit2.12070>
2. Ali F, Karim F (2014) Development of CAPTCHA system based on puzzle. *IEEE International Conference on Computer, Communications, and Control Technology*. <https://doi.org/10.1109/14CT.2014.6914219>
3. Almazroie M, Samsudin A, Gutub A, Salleh MS, Omar MA, Hassan SA (2020) Integrity verification for digital Holy Quran verses using cryptographic hash function and compression. *J King Saud Univ - Comput Inf Sci* 32(1):24–34. <https://doi.org/10.1016/j.jksuci.2018.02.006>
4. Almutairi S, Gutub A, Al-Ghamdi M (2019) Image steganography to facilitate online students account system. *Rev Bus Technol Res* 16(2):43–49. <https://doi.org/10.13140/RG.2.2.32048.30727>
5. Almutairi S, Gutub A, Al-Juaid N (2020) Motivating teachers to use information technology in educational process within Saudi Arabia. *Int J Technol Enhanc Learn* 12(2):200–217. <https://doi.org/10.1504/IJTEL.2020.10027118>
6. Alotaibi M, Al-hendi D, Alroithy B, AlGhamdi M, Gutub A (2019) Secure mobile computing authentication utilizing hash, cryptography and steganography combination. *Journal of Information Security and Cybercrimes Research* 2.1, pp. 73–82. <https://doi.org/10.26735/16587790.2019.001>
7. Althamary I, El-Alfy E-S (2017) A more secure scheme for CAPTCHA-based authentication in cloud environment. *IEEE International Conference on Information Technology*. <https://doi.org/10.1109/ICITECH.2017.8080034>

8. Baird HS, Lopresti DP, eds. (2005) Human Interactive Proofs: Second International Workshop, HIP 2005, Bethlehem, PA, USA, May 19–20, 2005, Proceedings. Vol. 3517. Springer
9. Banne SS, Shedge KN (2016) CARP: CAPTCHA as a graphical password based authentication scheme. *Int J Adv Res Comput Commun Eng* 5(1):14–18
10. Bhat MP, Raj RN (2020) Two-Way Image Based CAPTCHA. In: *Advances in Communication, Signal Processing, VLSI, and Embedded Systems*. Springer, Singapore, pp 471–483. https://doi.org/10.1007/978-981-15-0626-0_37
11. Bursztein E et al (2014) The end is nigh: Generic solving of text-based CAPTCHAs. In: 8th {USE-NIX} Workshop on Offensive Technologies ({WOOT} 14), San Diego
12. Bursztein E, et al (2010) How good are humans at solving CAPTCHAs? A large scale evaluation. 2010 IEEE symposium on security and privacy. IEEE, 2010, pp. 15–33. <https://doi.org/10.1109/SP.2010.31>
13. Bursztein E, Martin M, Mitchell J (2011) Text-based CAPTCHA strengths and weaknesses. In: *Proceedings of the 18th ACM conference on Computer and communications security*. <https://eiee.net/static/files/text-based-captcha-strengths-and-weaknesses-text-based-captcha-strengths-and-weaknesses-paper.pdf>. Accessed 29 Apr 2023
14. Chellapilla K et al (2005) Computers beat humans at single character recognition in reading based human interaction proofs (HIPs). CEAS, pp 1–17
15. Chow Y-W, Susilo W, Thorncharoensri P (2019) CAPTCHA design and security issues. In: *Advances in Cyber Security: Principles, Techniques, and Applications*. Springer, Singapore, pp 69–92. https://doi.org/10.1007/978-981-13-1483-4_4
16. Cui J, Zhang W-Z, Peng Y, Liang Y, Xiao B, Mei J-T, Zhang D, Wang X (2010) A 3-layer dynamic CAPTCHA implementation. IEEE International Workshop on Education Technology and Computer Science. <https://doi.org/10.1109/ETCS.2010.575>
17. Daş R, Baykara M, Tuna M (2015) Novel CAPTCHA approaches to protect web forms against bots. The Third International Symposium on Digital Forensics and Security (ISDFS 2015). <https://silo.tips/download/isdfs-2015-program-0930-0945-opening-speeches-prof-eref-sairolu-chair-isdfs-prof>. Accessed 29 Apr 2023
18. Ghorpade J et al (2014) Novel method for graphical passwords using CAPTCHA. *Int J Soft Comput Eng (IJSC)*:2231–2307. <https://www.semanticscholar.org/paper/Novel-Method-for-Graphical-Passwords-using-CAPTCHA-Ghorpade-Mukane/1f4fdfe97fcb23ccd89a0f0b3d9991b291398129>. Accessed 29 Apr 2023
19. Guo P, Deng YW, Zhang HY (2011) A CAPTCHA image recognition algorithm based on edit distance. *Key Engineering Materials*. Vol. 474. Trans Tech Publications Ltd, pp. 2203–2207. <https://doi.org/10.4028/www.scientific.net/KEM.474-476.2203>
20. Gutub A (2021) Regulating watermarking semi-authentication of multimedia audio via counting-based secret sharing. *Pamukkale Univ J Engin Sci* 1000(1000):0–0. <https://doi.org/10.5505/pajes.2021.54837>
21. Gutub A (2022) Integrity verification of Holy Quran verses recitation via incomplete watermarking authentication. *Int J Speech Technol* 25(4):997–1011. <https://doi.org/10.1007/s10772-022-09999-0>
22. Gutub A (2022) Watermarking Images via Counting-Based Secret Sharing for Lightweight Semi-Complete Authentication. *Int J Inform Sec Priv (IJISP)* 16(1):1–18. <https://doi.org/10.4018/IJISP.2022010118>
23. Gutub A, Almeahmadi E (2022) Advancing partial verification of watermarking for Arabic text via utilization of innovative counting-based secret sharing. *Arab J Sci Eng*. <https://doi.org/10.1007/s13369-022-07387-z>
24. Gutub A, AlKhodaidi T (2020) Smart expansion of target key for more handlers to access multimedia counting-based secret sharing. *Multimedia Tools & Applications* 79. <https://doi.org/10.1007/s11042-020-08695-y>
25. Gutub A, Al-Juaid N, Khan E (2019) Counting-based secret sharing technique for multimedia applications. *Multimed Tools Appl* 78(5):5591–5619. <https://doi.org/10.1007/s11042-017-5293-6>
26. Gutub A, Shambour MK, Abu-Hashem M (2023) Coronavirus impact on human feelings during 2021 Hajj season via deep learning critical Twitter analysis. *J Eng Res* 11(1):100001. <https://doi.org/10.1016/j.jer.2023.100001>
27. Kaur R (2016) A non-OCR approach for math captcha design based on boolean algebra using digital gates to enhance web security. IEEE International Conference on Wireless Communications, Signal Processing and Networking <https://doi.org/10.1109/WiSPNET.2016.7566254>
28. Kheshiafaty N, Gutub A (2020) Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions. *Int J Comput Sci Netw Secur(IJCSNS)* 20(9):16–28. <https://doi.org/10.22937/IJCSNS.2020.20.09.3>

29. Kheshaifaty N, Gutub A (2021) Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication. *Journal of Engineering Research*, pp. 1–11. <https://doi.org/10.36909/jer.13761>
30. Kulkarni P, Malwatkar G (2015) The graphical security system by using CaRP. *IEEE International Conference on Energy Systems and Applications* <https://doi.org/10.1109/ICESA.2015.7503319>
31. Kumar S, Kumar S (2019) Artificial intelligence: Concept of Security 7(6):45–52
32. Kushwaha P et al (2021) A Brief Survey of Challenge–Response Authentication Mechanisms. *ICT Analysis and Applications*. Springer, Singapore, pp 573–581. https://doi.org/10.1007/978-981-15-8354-4_57
33. Lv Y, Cai F, Lin D, Cao D (2016) Chinese character CAPTCHA recognition based on convolution neural network. *IEEE Congress on Evolutionary Computation* <https://doi.org/10.1109/CEC.2016.7744412>
34. Malutan R, Grosan C (2015) Web authentication methods using single sign on method and virtual keyboard". *IEEE Conference on Grid, Cloud & High Performance Computing Sciences*. <https://doi.org/10.1109/ROLCG.2015.7367431>
35. Mori G, Malik J (2003) Recognizing objects in adversarial clutter: breaking a visual CAPTCHA. In: 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings, vol. 1. IEEE, pp 1–8. https://www.cs.sfu.ca/~mori/research/papers/mori_cvpr03.pdf. Accessed 29 Apr 2023
36. Roslan NA, Udzir NI, Mahmud R, Gutub A (2022) Systematic literature review and analysis for Arabic text steganography method practically. *Egypt Inform J* 23(4):177–191. <https://doi.org/10.1016/j.eij.2022.10.003>
37. Roy PK, Saumya S, Singh JP, Banerjee S, Gutub A (2023) Analysis of community question-answering issues via machine learning and deep learning: state-of-the-art review. *CAAI Trans Intell Technol* 8(1):95–117. <https://doi.org/10.1049/cit2.12081>
38. Serrao M, Salunke S, Mathur A (2013) Cracking captchas for cash: A review of captcha crackers, vol 2, no 1. <https://www.ijert.org/cracking-captchas-for-cash-a-review-of-captcha-crackers>. Accessed 29 Apr 2023
39. Shaikh RA, Memon I, Hussain R et al (2018) A contemporary approach for object recognition based on spatial layout and low level features' integration. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-018-6796-5>
40. Singh A, Gutub A, Nayyar A, Khan MK (2022) Redefining food safety traceability system through blockchain: findings challenges and open issues. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-022-14006-4>
41. Singh A, Satapathy SC, Roy A, Gutub A (2022) AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope. *Arabian J Sci Engin (AJSE)* 47(8):9801–9831. <https://doi.org/10.1007/s13369-021-06348-2>
42. Singh VP, Pal P (2014) Survey of different types of CAPTCHA. *Int J Comput Sci Inform Technol* 5(2):2242–2245
43. Sufi FK, Alsulami M, Gutub A (2023) Automating global threat-maps generation via advancements of news sensors and AI. *Arab J Sci Eng* 48(2):2455–2472. <https://doi.org/10.1007/s13369-022-07250-1>
44. Tang M et al (2018) Research on deep learning techniques in breaking text-based captchas and designing image-based captcha. *IEEE Trans Inform Forens Sec* 13(10):2522–2537. <https://doi.org/10.1109/TIFS.2018.2821096>
45. Tirthani N, Ganesan R (2014) Data security in cloud architecture based on diffie hellman and elliptical curve cryptography. *IACR Cryptol ePrint Arch*, p 49. <http://eprint.iacr.org/2014/049>. Accessed 29 Apr 2023
46. Vaithyasubramanian S (2016) Review on development of some strong visual CAPTCHAs and breaking of weak audio CAPTCHAs. *IEEE International Conference on Information Communication and Embedded Systems*. <https://doi.org/10.1109/ICICES.2016.7518939>
47. Varish N, Pal AK, Hassan R, Hasan MK, Khan A, Parveen N, Banerjee D, Pellakuri V, Haqis AU, Memon I (2020) Image Retrieval Scheme Using Quantized Bins of Color Image Components and Adaptive Tetrolet Transform. *IEEE Access* 8:117639–117665. <https://doi.org/10.1109/ACCESS.2020.3003911>
48. Yan J, El Ahmad AS (2008) Usability of CAPTCHAs or usability issues in CAPTCHA design. *Proceedings of the 4th symposium on Usable privacy and security* <https://doi.org/10.1145/1408664.1408671>
49. Yan J, El Ahmad AS (2008) A Low-cost Attack on a Microsoft CAPTCHA." *Proceedings of the 15th ACM conference on Computer and communications security*, pp. 543–554. <https://doi.org/10.1145/1455770.1455839>
50. Zhang L Xie Y Luan X He J (2017) Captcha automatic segmentation and recognition based on improved vertical projection. In: *IEEE International Conference on Communication Software and Networks*. <https://doi.org/10.1109/ICCSN.2017.8230294>

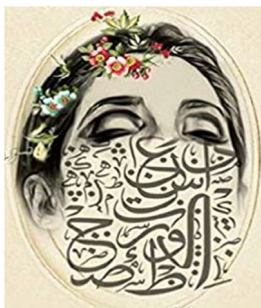
Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Prof. Adnan Gutub is ranked as Full Professor in Computer Engineering specialized in Information and Computer Security within College of Computers and Information Systems at Umm Al-Qura University (UQU). Adnan's academic experience in Computer Engineering was gained from his previous long-time work as Associate Professor, Assistant Professor, Lecturer, and Graduate Assistant, all in Computer Engineering at King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran, Saudi Arabia. He received his Ph.D. degree (2002) in Electrical and Computer Engineering from Oregon State University, USA. He had his BS in Electrical Engineering and MS in Computer Engineering both from KFUPM, Saudi Arabia. Adnan's research work can be observed through his 130+ publications (international journals and conferences) as well as his 5 US patents registered officially by USPTO with his main research interests involved optimizing, modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has

some work in modeling architectures for RSA and elliptic curve crypto operations. His interest in computer security also involved steganography and secret-sharing focusing on image-based steganography and Arabic text steganography as well as counting based secret sharing. Adnan's research interest in computing and information technology have been broaden to also relate to smart crowd management and intelligent transportation engineering systems as smart systems and internet of things (IoT) research because of the involvement in Hajj and Omrah Research at UQU - Makkah. Administratively, Adnan Gutub filled many executive and managerial academic positions at KFUPM as well as UQU. At KFUPM - Dhahran, he had the experience of chairing the Computer Engineering department (COE) for five years until moving to Makkah in 2010. Then, at UQU - Makkah, Adnan Chaired the Information Systems Department at the College of Computers & Information Systems followed by his leadership of the Center of Research Excellence in Hajj and Omrah (HajjCoRE) serving as HajjCoRE director for around 3-years until the end of 2013. Then, he was assigned his position (until March 2016) as the Vice Dean of HRI, i.e. the Custodian of the Two Holy Mosques Institute of the Hajj & Omrah Research, followed by his last 2-year administrative position as general supervisor of UQU Scientific Council, which ended September 2020.



Nafisah Matouq Kheshaifaty completed her Master of Science (MS) degree in Computer Science and Engineering from Umm Al-Qura University (UQU) defending her MS Thesis in June 2022. She worked her Thesis research as full-time student within the Computer Engineering Department under supervision of Prof. Adnan Gutub following computer security track offered at UQU, sponsored fully by UQU - Ministry of Education at Saudi Arabia. Ms. Nafisah hard work inspired related exploration remarked as genuine parts of this paper, running special tasks connecting to her graduate studies Thesis research entitled "Engineering Systems Accessibility via Multi-Level Password Authentication" which has been completed in an excellent level of contribution accomplishments.