Computers, Materials & Continua
DOI: 10.32604/cmc.2023.031245
Article

An Improved Text-Based and Image-Based CAPTCHA Based on Solving and Response Time

Ademola Olusola Adesina[1], Patrick Seun Ayobioloja[2], Ibidun Christiana Obagbuwa[3], Tola John Odule[1], Adenrele A. Afolorunso[2] and Sunday Adeola Ajagbe[4,*]

[1]Department of Mathematical Sciences, Olabisi Onabanjo University Ago-Iwoye, 120107, Nigeria
[2]National Open University of Nigeria, Abuja, 900001, Nigeria
[3]Sol Plaatje University, Kimberley, Northern Cape, 8305, South Africa
[4]Computer Engineering Department, Ladoke Akintola University of Technology, LAUTECH, Ogbomoso, 210214, Nigeria
*Corresponding Author: Sunday Adeola Ajagbe. Email: saajagbe@pgschool.lautech.edu.ng
Received: 13 April 2022; Accepted: 29 June 2022

Abstract: CAPTCHA is an acronym that stands for Completely Automated Public Turing Test to tell Computers and Humans Apart (CAPTCHA), it is a good example of an authentication system that can be used to determine the true identity of any user. It serves as a security measure to prevent an attack caused by web bots (automatic programs) during an online transaction. It can come as text-based or image-based depending on the project and the programmer. The usability and robustness, as well as level of security, provided each of the varies and call for the development of an improved system. Hence, this paper studied and improved two different CAPTCHA systems (the text-based CAPTCHA and image-based CAPTCHA). The text-based and image-based CAPTCHA were designed using JavaScript. Response time and solving time are the two metrics used to determine the effectiveness and efficiency of the two CAPTCHA systems. The inclusion of response time and solving time improved the shortfall of the usability and robustness of the existing system. The developed system was tested using 200 students from the Federal College of Animal Health and Production Technology. The results of each of the participants, for the two CAPTCHAs, were extracted from the database and subjected to analysis using SPSS. The result shows that text-based CAPTCHA has the lowest average solving time (21.3333 s) with a 47.8% success rate while image-based CAPTCHA has the highest average solving time was 23.5138 s with a 52.8% success rate. The average response time for the image-based CAPTCHA was 2.1855 s with a 37.9% success rate lower than the text-based CAPTCHA response time (3.5561 s) with a 62.1% success rate. This indicates that the text-based CAPTCHA is more effective in terms of usability tests while image-based CAPTCHA is more efficient in terms of system responsiveness and recommended for potential users.

Keywords: CAPTCHA; computational intelligence; information security; response time; solving time

1 Introduction

For more than a decade, information technology (IT) has been an important product for humankind as the trend and development in IT have changed every sphere of life. The purpose of digitization through information technology has been easy to enhance human activities in the areas of e-health, e-commerce, and communication to mention a few. Digitization has improved productivity and access to daily information both in the office and at home through the use of the internet. However, IT invention may be chaotic whenever bots and spam invade web services as online users' productivity and activity are reduced thus affecting both users and web services providers. Bot and spam are automated machines that slow down user activity during online transactions [1]. To contain this situation, various security mechanisms have been developed (in form of authentication and authorization) to prevent this interference. Authentication is the process of identifying a user's true identity, while the authorization mechanism is the process of authorizing a user for a particular task [2–4].

CAPTCHA acts as a security measure to prevent attacks by web bots during online transactions (automatic programs). The major function of CAPTCHA is to distinguish between humans and computers. CAPTCHAs act as Human Interactive Proof (HIP) so as to distinguish between humans and web bots using artificial intelligence (AI). AI programs can secure websites from web bots by protecting both real users (humans) and automated users (computers). Applying AI allows real users (humans) to pass challenging tests, that may be difficult for automated users to pass [5].

However, CAPTCHAs are not only a difficult problem to solve but also a real problem embedded in the Internet environment and can be used to verify a user's authentication before granting access. CAPTCHA technology identifies real users (humans) trying to access a network or service from automated users (computers) and prevents other hacks such as UDP from flooding network traffic or running out of bandwidth. DoS (Denial-of-Service) denies the actual user access to information systems or devices through the actions of malicious cyber threat actors. Email, websites, bank online accounts, and other services may be affected. A denial of service condition is caused by flooding the destination host or network with traffic until it becomes unresponsive or crashes, preventing legitimate users from accessing the system. The role of a hacker in providing false information can cause traffic congestion and reduce the performance of the entire information system [6,7]. In addition, there are many web service activities that add significantly to human interaction aspects, online registration is one such activity that provides users with the opportunity to register and use some services such as *Gmail* and *Paypal*. Scripts may be intentionally designed to steal valuable information that is highly sensitive to computer users in order for hackers to access websites.

A novel technique for CAPTCHA detection was proposed by [8], the technique simultaneously resolved preprocessing images and proper segmentation of CAPTCHA using stroke and data training. Accuracy, recall, precision, execution time, F-Measure and error rate were used as performance metrics. Image enhancement and binarization are performed in preprocessing based on the stroke region of the CAPTCHA. These areas' key points are based on the SURF feature. The preliminary results show that the model has a good recognition impact on CAPTCHA with foundation commotion and character grip bending.

CAPTCHA was classified based on text, image, audio, and video but this research will rest more on image and text-based CAPTCHA because of its frequent use [9–12]. CAPTCHA techniques employ various patterns or concepts that are easy for users to recognize but challenging for machine programs to replicate. This paper aims at comparing the performance of Text-based and Image-based CAPTCHA using the response time and solving time metrics, and; the objectives are to (i) design

both text-based and image-based CAPTCHA systems; (ii) perform a usability test on both text-based and image-based CAPTCHA systems; and (iii) evaluate both text-based and image-based CAPTCHA system, using solving time and response time.

Based on the literature survey, the time taken to solve the security challenges posed by the machine in form of a CAPTCHA image or text has been an open issue. Also, an in-depth review of literature showed that little or no research has been done on usability and robustness. These lapses then create a challenge to analyze (in terms of security of access, the user's efficiency and performance) while solving the challenge pose. Therefore, the development of an improved text-based and image-based CAPTCHA with solving and response time that will ensure users' confidentiality, integrity, and performance/efficiency is the goal of this paper.

2 Related Work

The security mechanism of CAPTCHA is based on the early concept of artificial intelligence and the Turing Test developed by Alan Turing in 1950 [13]. CAPTCHA security measures can be used in protecting some confidential web pages which are kept un-indexed to forestall others from finding them easily. HTML tags are available to prevent bots from stepping into confidential pages. If the user is determined to gain access to the data, then a trial is employed to resolve the CAPTCHA challenge and eventually gain access to the page but the computer programme (bot), may deny the access [14–16].

He et al. [17] described the mitigating comment spam method as irrelevant comments posted to a blog for the purpose of dropping a link to the spammer's website. Most bloggers were acquainted with programs that submitted bogus comments, usually with the aim of raising the computer programme ranks of some website. Comment spam is additionally called a spomment (i.e., a mix of the words spam and comment) but CAPTCHA can be employed to stop the comment spam. It also serves as a security strategy as the case may be. Basso et al. (2008) [18] explained preventing dictionary attacks as a frequent approach to prevent computer users from logging in against the same password. After a login failure, the user is required to complete a CAPTCHA test. This approach appears to be superior to locking the account after a specified number of failed login attempts. A dictionary attack (very popular among users) is a way of breaking into a password-protected computer or server by inputting every word in the dictionary as one password after the other. Dictionary assaults are prevented by using CAPTCHAs technology as the system prompts the user to complete the CAPTCHA problem after a specified number of failed login attempts.

Roshanbin et al. [19] described CAPTCHA as standard security for defending against attacks and with the ability to differentiate human users from robots. However, the CAPTCHA system is grouped into six — Image-based CAPTCHA, Text-based CAPTCHA, Video-based CAPTCHA, Audio-Based CAPTCHA, Puzzle CAPTCHA and Math CAPTCHA. According to Wang et al. (2020) [20], the most widely used Captcha scheme is text-based, with the vast majority of existing text CAPTCHAs designed with English letters and Arabic numerals. Recently, text CAPTCHAs with large character sets are increasingly popular. Wang et al. (2020) [20] also proposed a 3D image-based scheme that combines semantic comprehension and dragging. According to preliminary experimental results, 3D image-based schemes are more robust than text-based schemes. Meanwhile, CAPTCHA which can prevent computer programs from attacking websites has been identified as the most important security technology in recent times. Nouri et al. [21] described how to crack a visual CAPTCHA text through an automated solution based on deep learning. The research investigated the weaknesses in the CAPTCHA generator system and therefore, developed a more robust CAPTCHA without the risk of manual trials or errors. Kaur et al. [5] designed a secure text-based CAPTCHA

with an improved text-based CAPTCHA that is safer and more robust. The CAPTCHA designed combined randomly generated mathematical algebraic equations and alphanumerical words using an experimental approach. This results into an increase automated bot systems or software that abuse and destroy public web services.

In the standard model, Gu et al. [22] presented a traceable attribute-based signature method for monotone predicates. Their suggested approach was more efficient than other traceable attribute-based signature schemes. However, the solving time and response time of the proposed system were not considered, therefore, the effectiveness of the system may not be ascertained.

The location data privacy protection technique presented by Gu et al. [23] detected the association between location data in a database and protect the location data mined. Because a user's location preference may be linked to a private location, it was critical to protect very frequently accessing location data when mining location data. By distorting accessing frequencies, the suggested approach provides a means to protect very frequently accessing location data. Experiments revealed that the proposed scheme's data availability was higher and its privacy protection was fair when compared to other systems. Meanwhile, the effectiveness of the system may not be guaranteed as solving time and response time of the proposed system were not measured.

In a huge data context, Ghani et al. (2020) [24] presented a novel clustered-purpose based access control for users' long-term data privacy protection. The clustered-purpose based access control makes a substantial contribution to the proper treatment of personal data for specified, unambiguous, and legitimate reasons. From the sample space, the suggested algorithm selects specific records. It protects the long-term viability and proper use of data by validating current privacy tags and assigning new privacy tags using a clustered-purpose technique. The proposed solution provides the security and long-term privacy of existing and new personal data maintained in massive databases repositories. The suggested algorithm outperforms existing non-purpose based conventional techniques of long-term privacy preservation, according to a comparative examination of relevant results [24]. Although, the study proposed a security mechanism that is similar to a text-based CAPTCHA but the image-based system was not taken into consideration in the paper and the system was not evaluated with the state-of-the-art metrics to guarantee the efficiency and effectiveness of the paper.

Brodić et al. [25], Brodić et al. [2] described image and interactive CAPTCHA usability analysis for reaction time prediction. The article analyzed the predictability of response times to image and game-based CAPTCHA tests using typical demographic characteristics regression tree strategy. This represents a valuable analysis of CAPTCHA usability and reveals three important aspects. (i) response times to image-based CAPTCHAs are highly predictable using the model, (ii) the addition of interactive tasks improves predictability in the image-based CAPTCHA, and (iii) the device on which the test is performed has a slight impact on the prediction of reaction time to the game-based CAPTCHA.

Summarily, the review of the literature shows concerted efforts has been contributed toward security and intelligence system through the development of CAPTCHA, arising from the users' experience on CAPTCHA, the response time and solving time of both text-based and image-based have been long issues that are discouraging most of the users from taking the inherent security measure in the CAPTCHA. Incidentally, the scholars of the reviewed literature have addressed the issues, though the authors of [5] acknowledged the issues. Hence, this paper focuses on the development of an improved text-based and image-based CAPTCHA based on response time and solving time.

3 Experimental Design

The design phase is divided into three parts, the first phase included the design of text-based and image-based CAPTCHA systems; the second phase described the usability performance of both text-based and image-based CAPTCHA systems while the last phase discussed the evaluation of the usability performance of the developed CAPTCHA system using solving time and response time.

3.1 Design of Text-based CAPTCHA System

The development of the text-based CAPTCHA system follows the model shown in Fig. 1 and the algorithm in Fig. 2. The model has four modules which are the CAPTCHA Database module, CAPTCHA generator, obfuscator and display.

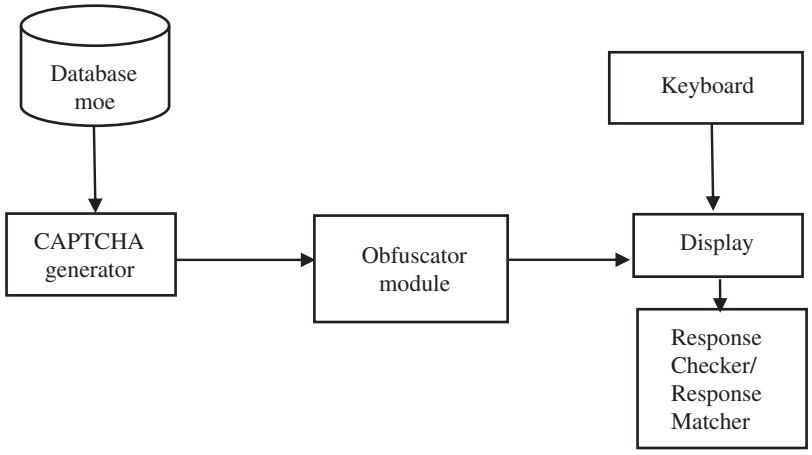


Figure 1: Text-based CAPTCHA model

Step1: Start
Step2: Randomly generate 6 characters from the database module
Step3: Initialize an empty canvas for drawing the CAPTCHA
Step4: Display CAPTCHA characters on the canvas
Step5: Display random lines on the canvas
Step6: Accept User input from the keyboard
Step7: If the user input is equal to the generated characters:
Step8: Save user response to the database
Step9: Redirect to a page where it displays the success message
Step10: Else:
Step11: Display an Error message to the user
Step12: End

Figure 2: Algorithm for text-based CAPTCHA system

The developed system was measured using a usability test for the human acceptability of the generated code. 200 Students from the Federal College of Animal Health and Production Technology between the age of 19 to 25 years were used to run the application and the result of each participant was recorded in the database.

The Database module contains the Latin character set which includes the English alphabet character i.e., the upper and lower case letter (A–Z) and number (0–9). The CAPTCHA generator module randomly generates six characters from the CAPTCHA database and the character includes

the combination of both the upper and lower case letters from the English alphabet and numbers from 0 to 9. The Obfuscator module takes randomly generated codes from the CAPTCHA generator and adds a random line to the CAPTCHA to form the background image for the developed CAPTCHA code and also serves as a security mechanism to protect the CAPTCHA code from the automated program. The Display module displays the generated CAPTCHA codes and contains three other sub-modules which are Keyboard, Response Checker and Response Matcher:

(a.) Keyboard unit allows the user to input the challenge pose.

The keyboard used is the standard 101 QWERTY. Both physical and virtual keypads can be used by the user to input the challenge pose;

(b.) Response checker determines whether the system has responded to the users' requests and;
(c.) Response matcher determines the correctness of the user's response matches the challenge pose.

3.2 Design of Image-based CAPTCHA System

The development of an image-based CAPTCHA system follows the model shown in Fig. 3 and the flowchart in Fig. 4. The model has four modules which are: Google image database module, image randomizer, display and response checker.

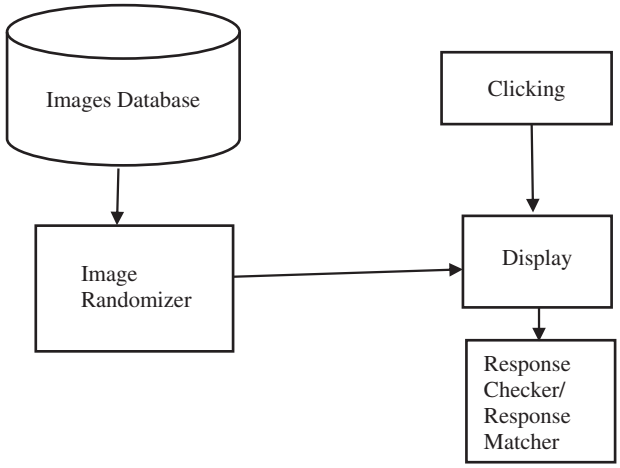


Figure 3: Image-based CAPTCHA model

The algorithm for the text-based CAPTCHA system development is depicted in Fig. 2.

3.3 Experimental Methodology

The design of the two improved CAPTCHA systems involves consideration for user-friendliness, security and platform support. The Graphical User Interface (GUI) used for these new systems was very interactive and easy in terms of flexibility and can be used by any user regardless of academic background. The newly developed system is platform-dependent and can work across the mobile platform and all browsers. However, the text-based and image-based CAPTCHA systems examined the capabilities of the browser in real-time and display the best possible CAPTCHA based on the browser configuration. The browser configuration does not have any effect on the efficiency of the CAPTCHA. The system does not require a flash and plug-in application. The developed system examines the possibility of a new CAPTCHA system to be able to add an authentication system

i.e., the time it takes to respond to an authentication request which starts from the user input and displays the result in form of access or denial (called response time) and the time it takes to respond to challenge pose when it has displayed CAPTCHA codes for authentication, this can be regarded as solving time. The developed system was tested by 200 students from the Federal College of Animal Health and Production Technology, Ibadan Nigeria to run the application and the bugs encountered were debugged, attest plan was developed and run on a given set of test data provided by the users. The average results from each user were analyzed to determine the most effective one. The developed CAPTCHA systems were evaluated using two parameters (i) response time and (ii) solving time performance metrics.

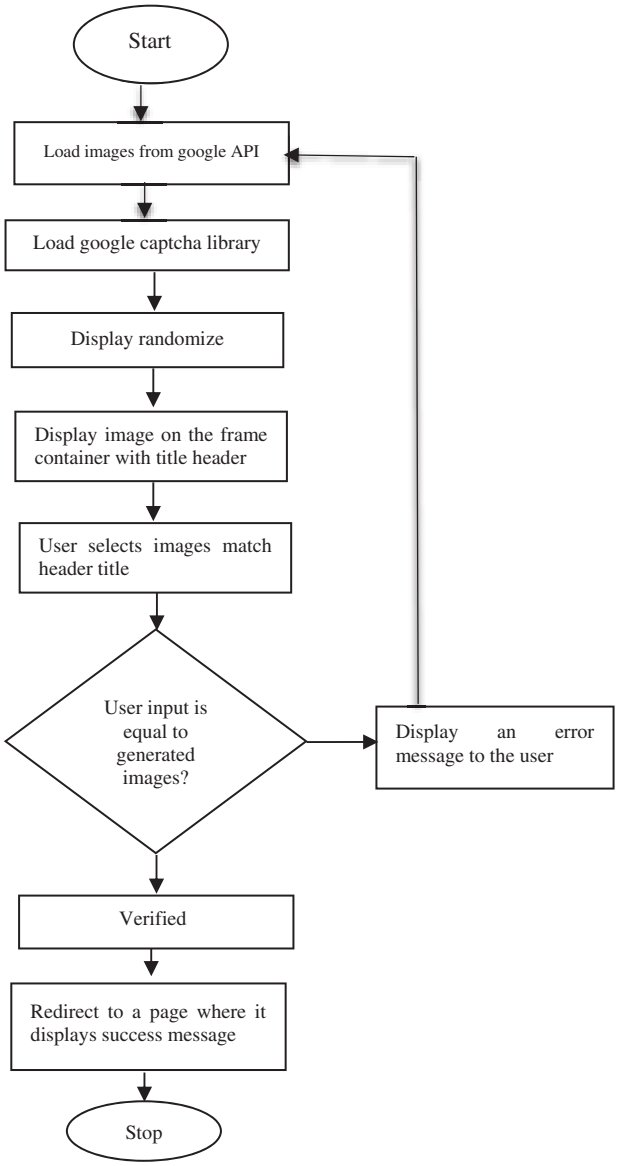


Figure 4: Flowchart for the image-based CAPTCHA

The developed CAPTCHA system was implemented by integrating it into an institutional repository website. A sequence of letters and digits are mixed together and the addition of random lines is a modification to the characters to prevent automated programs from accessing the actual characters. The text-based CAPTCHA was integrated into the login page of the institutional repository website i.e., the Welcome (Home) page. This page welcomes the user and requires the user to solve the text-based CAPTCHA by entering an Alphanumeric code (in Figs. 5 and 6).

Lower case with number Upper case and Lower case with the number

Figure 5: Sample code generation for text-based CAPTCHA

The image contains a car, road cross, building Image contains tress, bike car and road with crossing.

Figure 6: Sample code generation for image-based CAPTCHA

This sample code generation for the text-based and image-based system is the success of objective one. It is important to note that the image-based CAPTCHA was designed with additional features of response time and solving time which the existing system as an additional feature that will allow it to be compared with the new system and make the comparison.

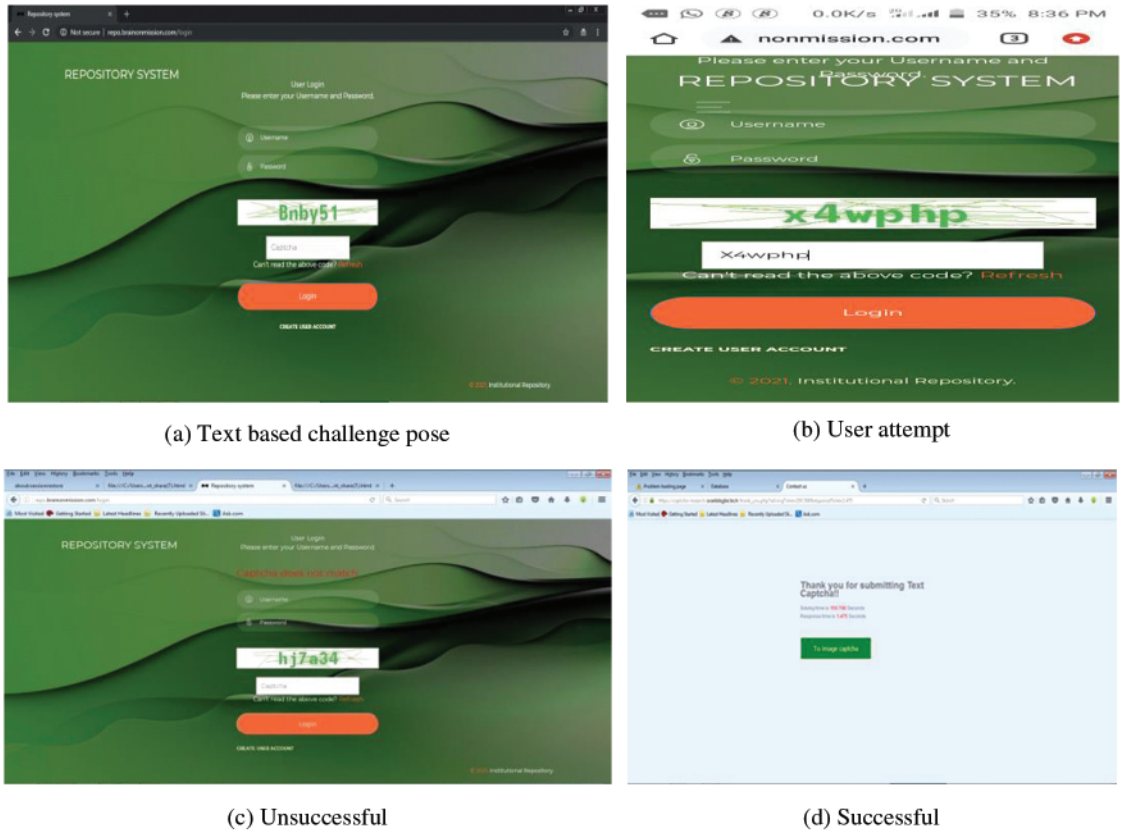
Thereafter, followed by the analysis of the data collected and the discussion of the results obtained. The developed CAPTCHA systems which include text-based and image-based were put to use through the comparative analysis of text-based CAPTCHA and image-based CAPTCHA using solving time and response time. Two hundred (200) respondents were subjected to the use of both CAPTCHAS following an equal time span of solving and response time. An equal number of participants (100 respondents) to an image-based CAPTCHA and text-based CAPTCHA at different experimental periods. The presentation is guided by the research questions raised and the hypotheses generated for the study.

3.4 Implementation of Text-based and Image-based CAPTCHA

The CAPTCHA system determines the usability convenience of the user in terms of the *Solving time*: how well can a user solve a CAPTCHA challenge? For example, how many times a user has to try in order to pass a test, and *Response time*: how long does it take for a user to respond to the challenge posed. These key criteria were used for evaluating the usability performance of CAPTCHAs. However, this key offers little specific guidance on *how* to improve efficiency using response time and solving time.

i. Text-based CAPTCHA

The implementation of text-based CAPTCHA was achieved using the model in Fig. 1 and it follows the algorithm in Fig. 2 as shown in Fig. 7. The challenges posed in text-based CAPTCHA were depicted in Fig. 7a, the user attempt is shown in Fig. 7b. and the unsuccessful and successful attempts are shown in Figs. 7c and 7d respectively.



(a) Text based challenge pose

(b) User attempt

(c) Unsuccessful

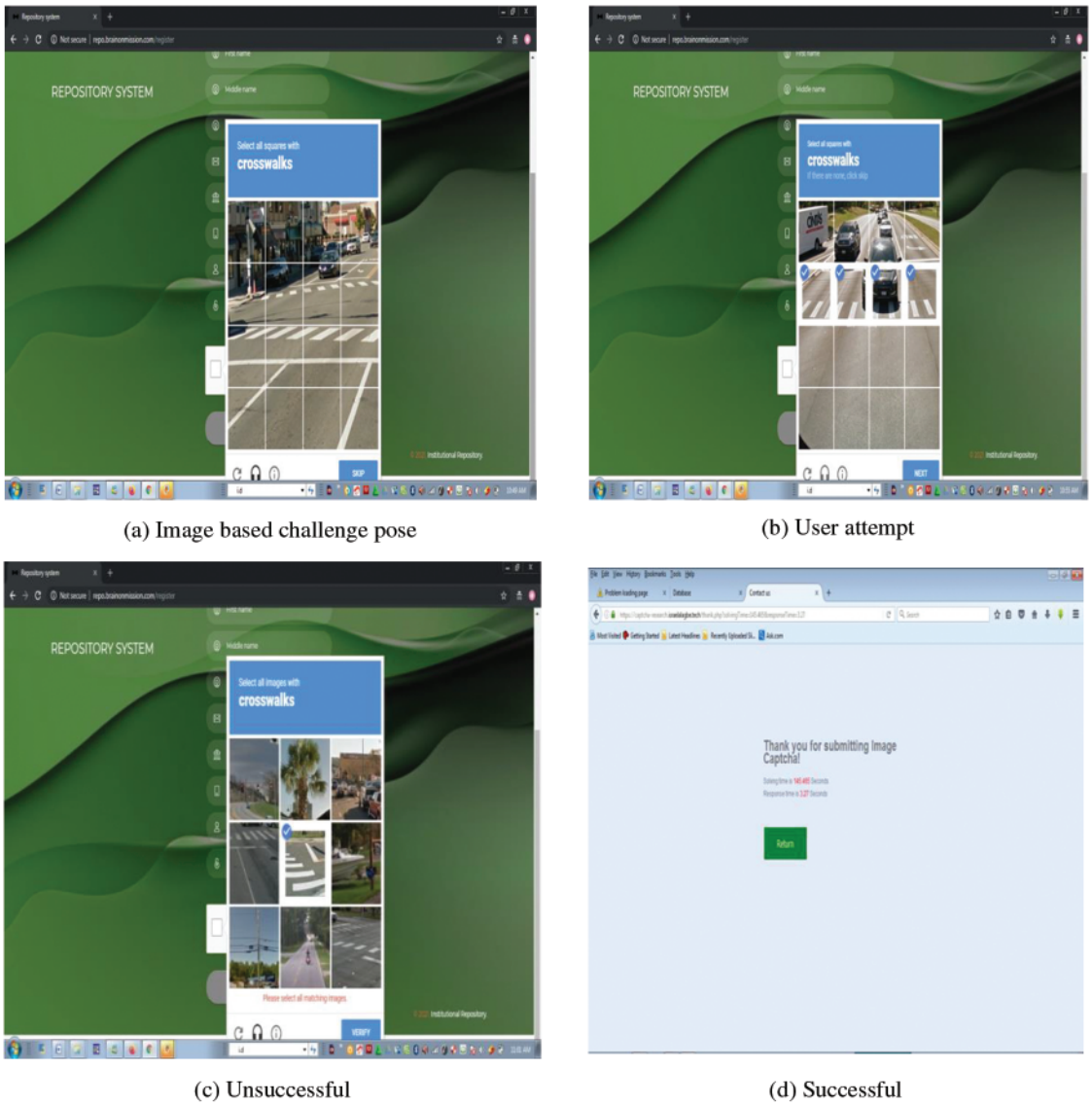
(d) Successful

Figure 7: Text-based operation

ii. Image-based CAPTCHA

The implementation of image-based CAPTCHA is shown in Fig. 8 displays the outcome of the development of image-based CAPTCHA following the model in Fig. 3 and the flowchart in Fig. 4.

In Fig. 8a the image-based challenge pose shows the challenge instruction with the target object name, for which the user must solve and in Fig. 8b user attempts or requires the user to select all images with the target object named "crossworks". Thereafter, the user clicks on verify to know whether what it has selected is correct in order to authenticate the system. Fig. 8c shows the unsuccessful operation to what the user has selected as it did not match the challenge pose. However, as the authentication fails, it also reports, *please select all matching pictures*. Finally, Fig. 8d shows success when what the user has selected matches the challenge pose which shows response time and solving time.



(a) Image based challenge pose

(b) User attempt

(c) Unsuccessful

(d) Successful

Figure 8: Image-based operation

4 Results and Evaluation Metrics

The results of the experiment are presented in this section, the researchers evaluated the average solving and response time. Tab. 1 is the overall average solving and response time gathered from 100 users during the testing of the developed Text-based and Image-based CAPTCHA. The mean statistics with the variants are presented in Tab. 2 (Average solving time for CAPTCHA type) and Tab. 3 (Average response time for CAPTCHA type).

Table 1: Text-based/image-based CAPTCHA response time and solving time

	CAPTCHA NAME		Statistic	Bootstrap[a]			
				Bias	Std. error	95% confidence interval	
						Lower	Upper
Response time	TEXT-BASED	N	100				
		Mean	3.5561	−.0210	.5148	2.6140	4.6477
		Std. deviation	5.35115	−.22875	1.30429	2.25142	7.48083
		Std. error mean	.53511				
	IMAGE-BASED	Mean	2.1855	−.0068	.1462	1.9234	2.4978
		Std. deviation	1.46438	−.06094	.33746	.79279	2.05910
		Std. error mean	.14644				
Solving time	TEXT-BASED	Mean	21.3333	−.0023	1.2258	19.0612	23.7164
		Std. deviation	11.71097	−.15118	1.22820	9.19384	13.98394
		Std. error mean	1.17110				
	IMAGE-BASED	Mean	23.5138	−.1474	1.7596	20.0103	26.9574
		Std. deviation	17.87384	−.24603	1.66107	14.13916	20.66252
		Std. error mean	1.78738				

Table 2: Average solving time for CAPTCHA type

CAPTCHA NAME	Mean (s)	Success rate (%)
TEXT-BASED	21.3333	47.8
IMAGE-BASED	23.5138	52.2
Total	22.4236	100

Table 3: Average response time for CAPTCHA type

CAPTCHA NAME	Mean (s)	Success rate (%)
TEXT-BASED	3.5561	62.1
IMAGE-BASED	2.1855	37.9
Total	2.8708	100

4.1 Independent Sample Test

To further deepen the investigation and infer the strength of the developed CAPTCHAS, the systems were further evaluated using an independent sample test, this was used to calculate the significance level of the variables. When the alpha level is greater than 0.05 ($P > 0.5$) the result is null and the hypothesis will be rejected, which means that there is a significant difference between the two variables (image-based and text-based CAPTCHA). This is represented in Tab. 4 as an independent sample test.

Table 4: Independent samples test

		Levene's test for equality of variances		T-test for equality of means						
		F	Sig.	T	Df	Sig. (2-tailed)	Mean difference	Std. error difference	95% confidence interval of the difference	
									Lower	Upper
Response time	Equal variances assumed	12.323	.001	2.470	198	.014	1.37059	.55479	.27653	2.46465
	Equal variances not assumed			2.470	113.745	.015	1.37059	.55479	.27153	2.46965
Solving time	Equal variances assumed	11.551	.001	−1.020	198	.309	−2.18048	2.13687	−6.39442	2.03346
	Equal variances not assumed			−1.020	170.772	.309	−2.18048	2.13687	−6.39856	2.03760

4.2 Discussion

The developed CAPTCHA system can be implemented on any operating system and the source code can be read and translated by any web browser effectively. The usability test conducted shows two hundred (200) results for both text-based and image-based CAPTCHA respectively. The two CAPTCHA types have an alteration appearance of One hundred (100) concurrencies each. The excellent performance of the participant shows that the developed CAPTCHA codes generated are easy to solve by a human. The solving time and response time are the two metrics used to compare the statistical performance of the two developed CAPTCHA types. The result shows that the average solving time for text-based CAPTCHA is 21.33 s while solving for image-based CAPTCHA is 23.51 s. This implies that the code for text-based CAPTCHA is more readable and easy to use by humans compare to image-based as shown in Tab. 2. In essence, the usability performance was carried out by giving out the developed system to students and the time taken by the user to solve the CAPTCHA (image and text) was recorded and the time taken by the system to respond to the user request was recorded. These data sets were extracted from the result of a usability test performed by the student. The result shows the efficiency of the developed system as the improved solving time and response time were achieved.

From Tab. 3, the average response time for image-based is 2.19 s while text-based average response time is 3.56 s, this implies that the generated code for image-based CAPTCHA responses to the user request is faster compared to text-based CAPTCHA (i.e., the image-based code loads the CAPTCHA image faster than the text-based CAPTCHA).

The overall result shows that text-based CAPTCHA is better than image-based in terms of user performance but as regards system responsiveness, the image-based system responds to user's requests better than the text-based. The data analyzed in Tab. 4 revealed that the calculated significance level is greater than the alpha level of 0.05 which made the null hypothesis to be rejected. Therefore, this means that there is a significant difference between image-based and text-based CAPTCHA using solving and response time. Tab. 1 shows that the participants found text CAPTCHA by the higher Mean statistic more convenient and easy to solve than image CAPTCHA at both solving and response time. In all, the new approach resulted in an improved performance and novel system, it guaranteed the system usability and robustness that ensures confidentiality, integrity and the security of the information.

5 Conclusion

The time taken to solve the security challenges posed by the machine in form of a CAPTCHA image or text has been an open issue. Also, an in-depth review of literature showed that little or no research has been done on usability and robustness. These lapses then create a challenge to analyze (in terms of security of access, the user's efficiency and performance) while solving the challenge pose. This paper developed an improved system that displays the generated CAPTCHA codes and contains three other sub-modules which were Keyboard, Response Checker and Response Matcher for text-based CAPTCHA. Also, a model has four modules which are: Google image database module, image randomizer, and display and response checker for image-based CAPTCHA. The result shows that text-based CAPTCHA has the lowest average solving time of 21.3333 s with a 47.8% success rate while image-based CAPTCHA has the highest average solving time of 23.5138 s with a success rate of 52.2%. The average response time for the image-based CAPTCHA was 2.1855 s with a 37.9% success rate lower than the text-based CAPTCHA response time of 3.5561 s with a 62.1% success rate. This indicates that the text-based CAPTCHA is more effective in terms of usability tests while image-based CAPTCHA is more efficient in terms of system responsiveness. Hence, it improves the operations of

CAPTCHA. More studies can still be carried out on text-based CAPTCHA to enable more security and protection against cyber-crime and other high-tech malicious acts.

Funding Statement: The research is supported by Sol Plaatje University, South Africa

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. V. Ahn, M. Blum and J. Langford, "Telling humans and computers apart automatically," *Communications of the ACM*, vol. 47, pp. 56–60, 2004.

[2] D. Brodić and A. Amelio, "New trends and challenges in CAPTCHA programming," in *The CAPTCHA: Perspectives and Challenges. Smart Innovation, Systems and Technologies*, Cham: Springer, vol. 162, pp. 105–122, 2020. https://doi.org/10.1007/978-3-030-29345-1_10.

[3] W. Sun, G. C. Zhang, X. R. Zhang, X. Zhang and N. N. Ge, "Fine-grained vehicle type classification using lightweight convolutional neural network with feature optimization and joint learning strategy," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30803–30816, 2021.

[4] L. Tan, N. Shi, K. Yu, M. Aloqaily and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green internet of things," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, pp. 1–20, 2021.

[5] K. Kaur and S. Behal, "Designing a secure text-based captcha," *Procedia Computer Science*, vol. 57, pp. 122–125, 2015.

[6] W. K. A. Hasan, "A survey of current research on captcha," *International Journal of Computer Science and Engineering Survey (IJCSES)*, vol. 7, pp. 141–157, 2016.

[7] Y. Matsuura, H. Kato and I. Sasase, "Adversarial text-based CAPTCHA generation method utilizing spatial smoothing," in *IEEE Global Communications Conf. (GLOBECOM)*, Madrid, Spain, 2021.

[8] D. Kumar, R. Singh and S. S. Bamber, "Your CAPTCHA recognition method based on deep learning using MSER descriptor," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2981–2996, 2022.

[9] M. Kumar, M. Jindal and M. Kumar, "A systematic survey on CAPTCHA recognition: Types, creation and breaking techniques," *Archives of Computational Methods in Engineering*, vol. 29, pp. 1107–1136, 2022.

[10] S. A. Ajagbe, K. A. Amuda, M. A. Oladipupo, O. F. Afe and K. I. Okesola, "Multi-classification of Alzheimer disease on magnetic resonance images (MRI) using deep convolution neural network approaches," *International Journal of Advanced Computer Research (IJACR)*, vol. 11, pp. 51–60, 2021.

[11] S. A. Ajagbe and A. O. Adesina, "Design and development of an access control based electronic medical records (EMR)," *Centrepoint Journal (Science Edition)*, vol. 26, no. 1, pp. 98–119, 2020.

[12] J. M. G. Hidalgo and G. Alvarez, "Captchas: An artificial intelligence application to web security," in *Advances in Computers*, vol. 83, no. 4, pp. 109–181, 2011.

[13] G. Rana, R. Saha and G. Geetha, "Analysis of relation between entropy and factors in image-based CAPTCHAs," *International Journal of Engineering and Technology*, vol. 7, no. 6, pp. 2105–2108, 2014.

[14] R. Saha, G. Geetha and G. -S. Lee, "CLAPTCHA-A novel captcha," in *Int. Conf. on Security Technology*, Berlin, Heidelberg, pp. 94–100, 2011.

[15] L. Y. Xiang, X. B. Shen, J. H. Qin and W. Hao, "Discrete multi-graph hashing for large-scale visual search," *Neural Processing Letters*, vol. 49, no. 3, pp. 1055–1069, 2019.

[16] A. Pahuja and V. Srivastav, "Set based CAPTCHA"-comparison with text-based CAPTCHA and image-based CAPTCHA," *Advances in Computer Science and Information Technology (ACSIT)*, vol. 3, no. 4, pp. 254–261, 2016.

[17] P. He, Y. Sun, W. Zheng and X. Wen, "Filtering short message spam of group sending using CAPTCHA," in *First Int. Workshop on Knowledge Discovery and Data Mining (WKDD 2008)*, Adelaide, SA, Australia, pp. 558–561, 2008.

[18] A. Basso and M. Miraglia, "Avoiding massive automated voting in internet polls," *STM2007, Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 149–157, 2008.
[19] N. Roshanbin and J. Miller, "A survey and analysis of current captcha approaches," *Journal of Web Engineering*, vol. 12, pp. 001–040, 2013.
[20] P. Wang, H. Gao, Q. Rao, S. Luo, Z. Yuan *et al.,* "A security analysis of captchas with large character sets," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, pp. 2953–2968, 2020.
[21] Z. Nouri and M. Rezaei, "Deep-CAPTCHA: A deep learning-based CAPTCHA solver for vulnerability assessment," pp. 1–9, 2020, SSRN Elsevier Available at http://dx.doi.org/10.2139/ssrn.3633354.
[22] K. Gu, K. M. Wang and L. L. Yang, "Traceable attribute-based signature," *Journal of Infomation Security and Applications*, vol. 49, pp. 102400, 2019.
[23] K. Gu, L. H. Yang and B. Yin, "Location data record privacy protection based on differential privacy mechanism," *Information Technology and Control*, vol. 47, no. 4, pp. 639–654, 2018.
[24] N. B. A. Ghani, M. Ahmad, Z. Mahmoud and R. M. Mehmood, "A pursuit of sustainable privacy protection in big data environment by an optimized clustered-purpose based algorithm," *Intelligent Automation & Soft Computing (IASC)*, vol. 26, no. 6, pp. 1217–1231, 2020.
[25] D. Brodić, A. Amelio, N. Ahmad and S. K. Shahzad, "Usability analysis of the image and interactive CAPTCHA via prediction of the response time," in *Int. Workshop on Multi-Disciplinary Trends in Artificial Intelligence*, Gadong, Brunei Darussalam, vol. 6, no. 3, pp. 252–265, 2017.