International Journal of Information Technology and Computer Engineering
Vol: 05, No. 01, Jan - June 2025
ISSN: 2455-5290, DOI: 10.55529/ijitc.51.1.14

Research Paper

A comparative analysis of the effectiveness of recaptcha v3 against recaptcha v2, hidden fields, and other anti-spam techniques

Tracy Fitz-Inteseful[1*], Joshua Sunkwa[2], Dr. William Asiedu[3]
[1*, 2, 3]Department of Information Technology Education Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED), Kumasi, Ghana.

Article Info

Article History:
Received: 08 September 2024
Revised: 20 November 2024
Accepted: 26 November 2024
Published: 12 January 2025

Keywords:
Captcha V3
Captcha V2
Anti-Spam
Hidden Fields
User Experience
Bot Detection

ABSTRACT

This work aims at comparing the performance of the following: reCAPTCHA v3, reCAPTCHA v2, hidden fields, and plain forms in the fight against bot activity. To do so, each of the methods was performed while in a WordPress staging environment and the robot was checked for its capability to bypass spam submissions. A preliminary evaluation of the results shows that plain forms and hidden fields do not prevent much automation; reCAPTCHA v2 has moderate effectiveness but is penetrable by advanced bots. On the other hand, reCAPTCHA v3 excels as per its efficiency standards; it employs behavioral analysis to rate user response instead of posing visible tests; thus, the bot access is immediately denied without affecting genuine users. However, user tracking becomes an issue of concern in reCAPTCHA v3 due to the vast amount of tracking done by this system. This study reveals that security, user experience, and privacy are important factors in anti-spam solutions; therefore this paper recommends v3 reCAPTCHA as the most effective solution despite the problems associated with its implementation and privacy considerations.

Corresponding Author:
Tracy Fitz-Inteseful
Department of Information Technology Education Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED), Kumasi, Ghana.
Email: tracyadjoa@yahoo.com

1. INTRODUCTION

Since the advent of the internet, everyone has had an online presence, from social media handles, shopping carts, online commerce, online banking, E-learning, and flight booking thereby making user and customer details available on thousands of servers all around the world. , as a result, there is a rise in cybercrime which is the act of attacking computers, network devices, and data transferred on the internet. A lot of online applications use automated bots to aid in early responses. An example is WhatsApp business automatic response to messages, allowing bots unrestricted access to these services is not a good practice because attackers with malicious intent are drawn to this technology and use it to either steal information, impersonate, or bombard the system to prevent legitimate users from accessing the system. There are various forms of bots namely chatbots, social media bots, web crawlers, spam bots, malware bots, personal assistant bots, etc.

Bot activities have been a constant security issue for internet users, to curtail these bots' activities there are a lot of technologies that can detect and prevent these bots, some of these technologies are Intrusion Detection Systems (IDS), Honeypots, Traffic analysis, Machine Learning, and AI and CAPTCHA was introduced to help identify bot activities from human activities. CAPTCHA stands for (Completely Automated Public Turing Test to Tell Computers and Humans Apart) it's a technology that performs an authentication process called challenge-response authentication in which the user is presented with a challenge of some form before they are allowed into the website [1]. This challenge is very difficult for bots to answer but it is very easy for humans to answer them and that is how the difference is identified. Since the introduction of CAPTCHA, there have been different versions like Text-based, Image-based, Audio-based, Video-based, and Puzzle Captcha among others.

This research checks if various anti-spam methods like reCAPTCHA v3, reCAPTCHA v2, hidden fields and plain forms are effective by running tests within a WordPress staging site. The outcome of this research will help to identify which of the methods give pleasing security features while at the same time being user friendly.

2. RELATED WORK

History of Captcha

The Completely Automated Public Turing Test to Tell Computers and Humans Apart, or CAPTCHA, is an essential security tool for telling automated programs from human beings. Due to advancements in computational intelligence and the recognition of patterns, conventional 2- dimensional fixed CAPTCHAs are increasingly vulnerable to attacks by malicious programs.

Innovative solutions have been developed to overcome these difficulties, such as 3D text-based CAPTCHAs like DotCHA, which needs users to rotate a 3D text model in order to recognize letters. This keeps the model usable and resistant to many types of attacks. Furthermore, it has been suggested to increase security by using dynamic CAPTCHAs with multiple layers and incorporating biological vision theories. This will make it harder for automated programs to crack, even with multiple frames, by taking advantage of computers' limitations in recognizing complex visual patterns [2], [3], [4].

CAPTCHA V2

CAPTCHA v2 was developed from the previous text-based CAPTCHA to advanced image-based schemes, for instance, Google's that uses the drag and drop and the image selection option to filter out bots. However, just like the above-mentioned image-based CAPTCHAs have also posed problems, with the recent innovations in machine learning and computer vision; the automated systems have bent the test with high success rates of 99%. Currently, 8% accuracy is attained against some variants of reCAPTCHA. Due to the continuous arms race between CAPTCHA creators and abusers, new approaches and adversarial techniques along with behavioral-based.

CAPTCHAs have been developed in order to facilitate better security while using user's interaction patterns. Nevertheless, these shortcomings lie with some risks hence requires constant study toward coming up with more secure and friendly CAPTCHA designs [5].

Key Features of CAPTCHA V2

Some of the characteristics of this CAPTCHA v2 include a two layered CAPTCHA from Microsoft which incorporates both the text and image based tests which increases protection against aggressive bots. This system lets users solve CAPTCHAs quite fast, usually within less than 2 seconds while it slows down bots, whose attack rates stand around 9 on average. Usually, it takes 05 seconds on standard desktop computers [2]. The idea of the multiple- layer CAPTCHA encompasses letters and digits as well as special signs along with a randomly chosen image, with checkboxes to interact with it [2]. It is the approach that primarily focuses on making websites easier to use for humans while at the same time making them difficult for bots to infiltrate [4], [2].

CAPTCHA V3

In contrast to v2, reCAPTCHA v3 offers an invisible verification system that uses behavioral analytics to assign risk scores to users without requiring any interaction [6]. This eliminates friction for users but raises concerns about privacy, as it relies on extensive tracking of user behavior [7].

Key Features CAPTCHA V3

Key enhancements are added to CAPTCHA V3 to improve security against malevolent bot assaults. The suggested CAPTCHA method creates a multilayered challenge that is challenging for bots to solve by combining text-based elements such as letters, numerals, and special characters with randomly chosen images from a database [2]. To further prevent automated attacks, the system also includes a time-based component that requires users to complete the CAPTCHA within a given amount of time [2], [3] Additionally, the CAPTCHA methodology offers a flexible and safe solution to site security by creating texts in several languages, transforming them into images with noise added, and storing them in a database for user authentication. All things considered, CAPTCHA V3 makes use of text, graphics, and time limits to provide a strong defense against harmful bot programs, guaranteeing effective human verification and protecting online platforms [2], [3].

Hidden Fields

Non-invasive techniques such as hidden fields are one of the simplest forms of anti-captcha which are frequently applied to web forms to tell the difference between the human and the bots. Essentially, this method entails insertion of form fields which are inactive and unheard of to the users; this typically can be done using a hidden CSS that conceals the said fields from view or simply by placing them outside the graphic interface, where they cannot be seen. So, while legitimate users will fill out the form normally and hence do not tamper with these fields, the form can be subjected to malicious users. Still, bots, which are usually designed to complete all the fields in a form, will engage with those hidden fields. This behavior is a sign of automation and this is where we can consider flagging or banning any automation activities by the bots.

As with most techniques it is simple to perform and can also work well against certain bots; yet it has several problems. In fact, it is possible to distinguish between the fields and hide it, and more advanced bots are capable of avoiding such fields. Therefore hidden fields can be employed as an additional security measure in combination with more effective security mechanisms, such as CAPTCHA or honeypots [8].

This method is best suitable for the websites with little traffic and are likely to encounter complex bots hence may not be enough in websites that needs extra security.

Plain Forms

Plain Forms refer to basic webs forms, which have no check or mechanism for the incorporation of anti-spam that is functional. These forms simply consist of input fields which the users then fill and submit, with no additional verification procedures to spot the script. Despite the fact that plain forms are easy to use and very friendly to legitimate users, they are very vulnerable to spam bots that are in a position to take advantage of plain forms by providing unwanted or otherwise harmful information [9].

There is an instance where bots wander the internet looking for such open forms and the moment they locate them, they have the ability to send out automated entries that flood systems with unwanted data or spam. This represents a big problem, especially for contact forms, comment sections or any interface with the intention of getting users' information.

To augment the security of plain forms, developers may integrate rudimentary protective strategies such as Data Entry Validation, Rate Limiting, and JavaScript-based Validation.

These enhancements may keep away basic bots, but they are not always sufficient to protect the high-traffic forms. Solutions like CAPTCHA or behavior analysis might be necessary for enhanced security measures [9].

3. METHODOLOGY

In order to compare the efficiency of the above approaches, an experiment with a spam filter was done in a WordPress staging area. It created a means through which different anti-spam methods could be tried out on the same forms as those in a live Website but without interfering with the Website. The purpose of this experiment with the four methods was to determine to what extent they were effective in deterring automated bot submissions. Figure 1 is the submission logs for the experiment.

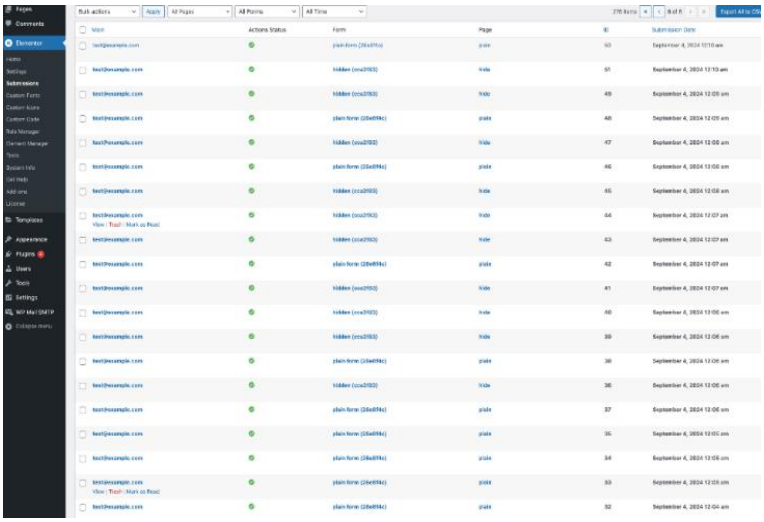

Figure 1. Status Overview of Automated Actions in Word Press Site Using WP All Import

Figure 1, the dashboard provides a detailed view of scheduled and completed import actions using the WP All Import plugin in Word Press. Each row indicates the domain, action type, form, page type, and the timestamp of the import activity along with its status.

Experiment Set-Up

With this setup, it is desirable to gauge the effectiveness of different anti-spam approaches by creating a supervised spam environment using a WordPress staging server. Such staging context enables testing without having an effect on an effective working site. Below is an elucidation of the structural composition of the testing environment.

The Four Types of Forms

Form with reCAPTCHA v2: This variation uses the reCAPTCHA v2 platform which normally requires the user to complete a particular task such as identifying pictures or solving a maze in order to prove that he or she is not a robot.

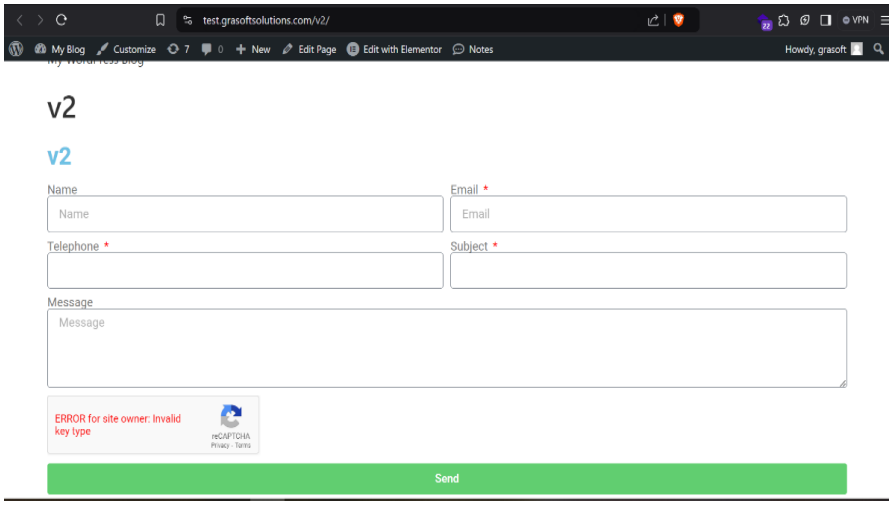

Figure 2. Contact Form Interface with reCAPTCHA Error on Word Press Page

Figure 2, the contact form displays a reCAPTCHA error stating "Invalid key type," indicating a configuration issue that needs to be resolved by the site owner.

Form with reCAPTCHA v3: The reCAPTCHA v3 is a more significant model as compared to the v2 one that takes place unnoticed, without involving users into the process. This function assigns the risk score based on the behavior of users and the form can be blocked if the score shows that there is probability of a bot using it.

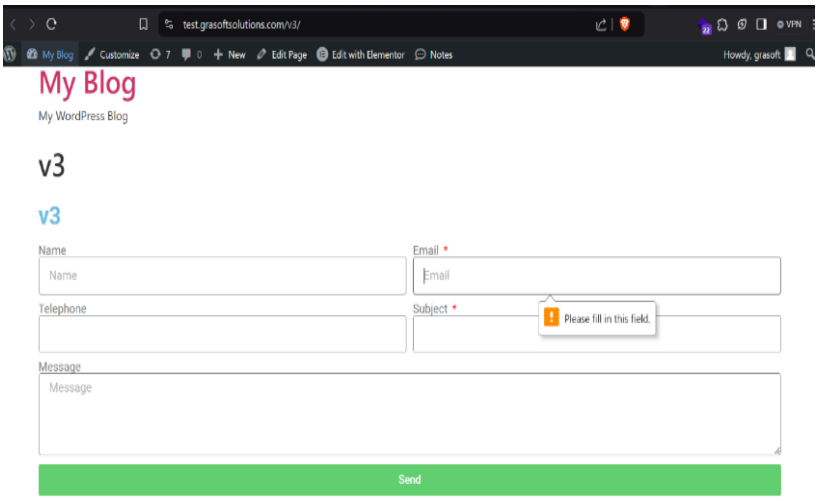

Figure 3. Form Validation Alert on Contact Page Submission in Word Press

Figure 3, the form displays a validation alert prompting the user to fill in the required "Subject" field before submitting.

Form with Hidden Fields: This particular form contains hidden fields that are normally interacted with by bots, however, they are not revealed and cannot be filled by any human. When the bot enters into these concealed fields, it makes its presence known and thus the submission can be categorized as spam.

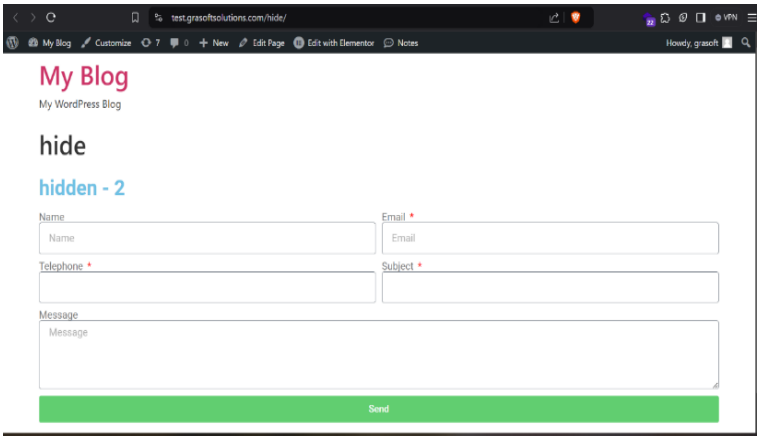

Figure 4. Contact Form Layout on 'Hide' Page of Word Press Site

Figure 4, a contact form is presented on the 'hide' page, where all required fields including Email, Telephone, and Subject must be filled before submission.

Form (Absence of Anti-Spam Mechanisms): This is a basic shape with no safeguards against the automated bot programs. It is used to measure and compare their vulnerability to such parasitic forms as undesired automatic spam submission

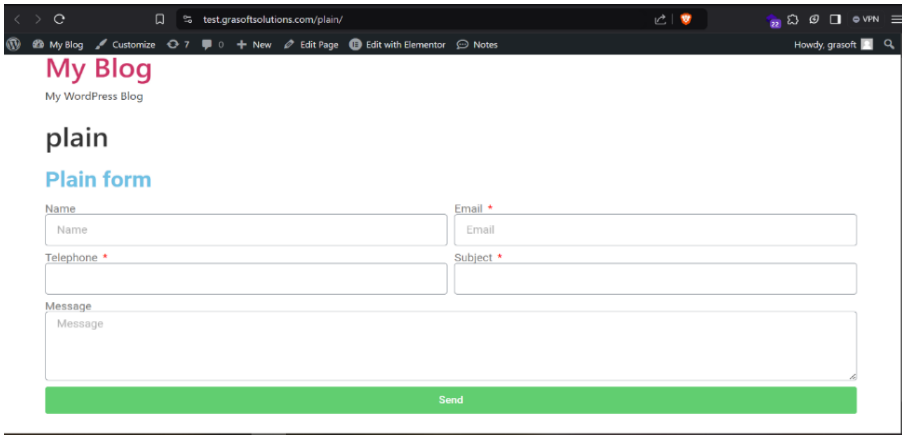

Figure 5. Plain Contact Form Display on Word Press Page

Figure 5, the 'plain' page features a basic contact form with standard input fields and a green "Send" button for user submissions.

Testing

Programming Bots

Bots were setup to start to send spam to complete these form in order to provide a simulation of a spam attack. The range of the activities of the bots were from filling the plain form to the complex bots that attempt to solve such methods as hidden fields.

Submissions Recording

The count of successful bot submissions by each form of the four forms were kept. This in turn enables the tester to determine how efficient each of the anti-spam method is in preventing automation entries. Essentially, the more instances successful bots are submitted, the less efficient that process is and also, the methods that reveal less number of successful submission are more effective for preventing bots.

4. RESULTS AND DISCUSSION

The results show the number of successful bot submissions for each type of form, providing a clear comparison of the effectiveness of various anti-spam techniques: Containing the submission of each form Table 1, the Plain and Hidden Fields Forms received the most submissions, whereas the reCAPTCHA V3 form had zero, suggesting possible configuration or user interaction issues.

Table 1. Comparison of Form Submissions Based on Form Type

Form	No of Submissions
Hidden Fields Form	121
Plain Form	130
reCAPTCHA V2	26
reCAPTCHA V3	0

Hidden Field Form: 121 Entries.

Analysis: Out of the ones with hidden fields, 121 submissions were completed by the bots, which means that this strategy is only somewhat helpful. It can effectively prevent some of the easier bots that change with hidden fields but more complex bots are able to recognize these fields and operate around them, there for resulting into a large number of successful spam entries.

Effectiveness: Moderate. This method is slightly better than a complete absence of protection; however it's less effective against the more evolved bots.

Plain Form: 130 Entries

Analysis: As demonstrated in the results, the plain form that has no anti-spam measures at all had the most number of successful bot submission of 130. This method does not offer any form of protection which means that bots are capable of detecting the form and submitting all forms of data and thus not useful in combating spam.

Effectiveness: Low. Not surprisingly, plain forms are very susceptible to spam invasions.

reCAPTCHA v2 Form: The 26 Entries

Analysis: A reCAPTCHA form where it asks the users to complete a certain action such as identifying images enabled 26 bots to submit their entry. As this suggests, reCAPTCHA v2 works despite the fact that some advanced bots or some types of approaches, including CAPTCHA-solving services, can get through the system.

Effectiveness: Moderate to high. While it has quite a lot of security measures, it is not immune to complex bots or various CAPTCHA cracking tools.

reCAPTCHA v3 Form: No entry

Analysis: There was no successful attempt by bots to fill the reCAPTCHA v3 form that was implemented on the website; all the entries were from bots. It appeals to a behavioral analysis that puts a risk score on each user so that the bots can be easily blocked without the users' intervention. The lack of any entries also show that reCAPTCHA v3 protects better among the various methods used in the research.

Effectiveness: Very high. It is very efficient with regard to the detection and prevention of bot submissions particularly against other evolved bot programs.

Table 2. Bot Submission Rates

CAPTCHA Method	Total Attempts	Successful Bot Submissions	Detection Success Rate (%)
Plain Form	130	130	0%

Hidden Fields	130	121	7%
reCAPTCHA v2	130	26	80%
reCAPTCHA v3	130	0	100%

Below is the bar chart and line graph representation of the bot submissions results.

Table 2, reCAPTCHA v3 achieved a 100% detection success rate by blocking all bot submissions, while the plain form failed to prevent any, allowing all 130 bot attempts through.

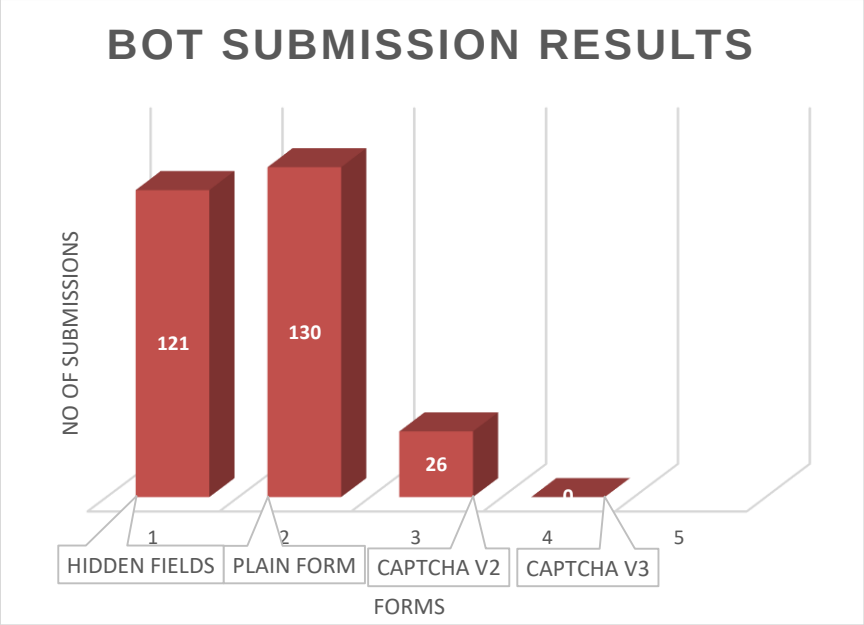

Figure 6. Bot Submission Comparison across Different Form Security Methods

Figure 6, the plain form had the highest number of bot submissions, followed by hidden fields, while reCAPTCHA v3 blocked all bot entries, indicating its superior effectiveness.

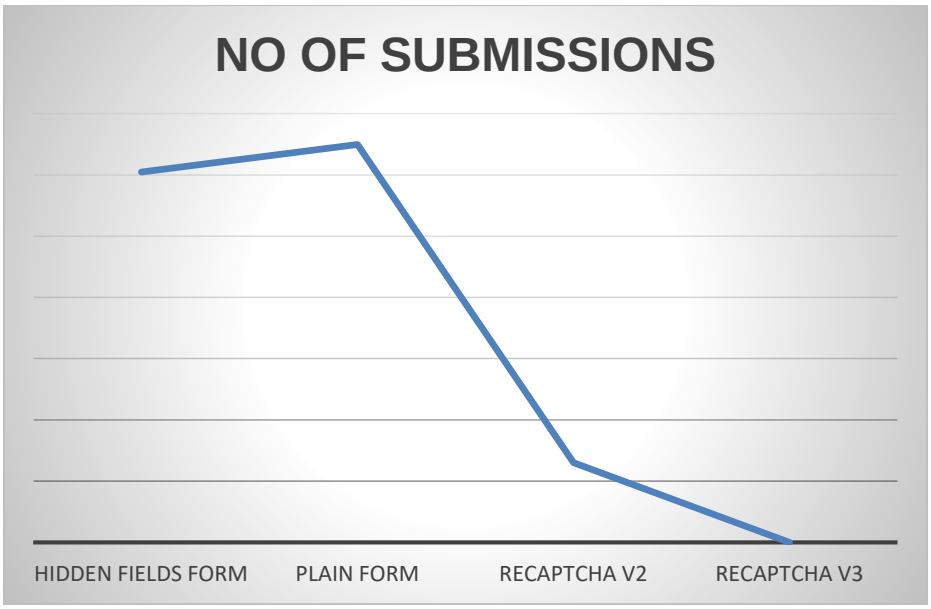

Figure 7. Trend of Bot Submissions across Various Form Types

Figure 7, bot submissions decreased significantly from the plain and hidden fields forms to reCAPTCHA v2 and dropped to zero with reCAPTCHA v3, highlighting its effectiveness in blocking bots.

The results obtained from the experiment show that there are distinctions regarding the efficacy of the anti-spam approaches used. Just as important is its capability to disallow automated bot submission in order to assess the effectiveness of common anti-spam measures.

This findings form the bases for the discussion and comparative analysis below.

1. Security Effectiveness

As for the anti-spam methods namely plain form, hidden fields, reCAPTCHA v2 and reCAPTCHA v3, the test for their level of security was conducted on the basis of count of bot submission. This metric directly shows how effectively each method allows to avoid automated attack and guarantee the forms' purity.

Plain Form: This was despite the plain form with no anti-spam measures and methods being able to receive 130 successful bot submissions. This implies that forms without protection are very much at the mercy of these form grubbing bots thus agreeing with the fact that bots can easily identify these forms and flood them with various data. According to Stasiuk and Kopylov [10], unprotected forms are often completed with bots and therefore cannot be used in practice.

As can be expected, there are no limitations with plain forms; thus, bots take advantage of them and distort the platform by continuously spamming and posing security threats, including identity theft. This result highlights the necessity of applying anti- spam measures to any web-based form that takes user input especially in the situations that require customization and secrecy of the input data.

Hidden Fields: Some of the most fundamental methods that were employed were hidden fields which gave a moderate level of protection; although the program was able to capture some bots, 121 were able to submit their entries. This technique operates by incorporating other form fields that are not easily noticeable, and cannot be interacted with by real users. Despite this, bots tend to complete all fields, including hidden ones, which could be easily identified as bots' activity. Even if this method helps capture a few bots, the outcome clearly shows that it is rather simple to overcome by sophisticated bots which are designed to look for concealed fields [11].

A large number of successful bot entries are indicative of the fact that hidden fields do not present any significant barrier to controlling spamming and should not be over relied on in this regard. This method may be useful for typical bare-bone bots, but it is inadequate against the new and improved spam bots that are capable of detecting these traps and avoiding them.

reCAPTCHA v2: With reCAPTCHA v2, the number of bot registrations was cut down to 26 after enhancing the system against bots. reCAPTCHA v2 is quite popular with which the user needs to pass a challenge—captchas, for example, where the user is required to point to some objects displayed in pictures or click on the checkbox to confirm that the user is not a robot. Nevertheless, the presence of 26 submissions that was successful proves that the new generation of bots is developing and some of them are able to pass CAPTCHA using technologies such as machine learning and AI algorithms [12].

Although this method still offers high immunity against most of the bots, it is highly vulnerable to certain complex attacks such as those involving CAPTCHA-solving services as well as other forms of high-tier automation. This has a hint on the fact that though reCAPTCHA v2 provides adequate security, it might require other measures to combat more complex threats.

reCAPTCHA v3: reCAPTCHA v3 proved to be the most efficient and none of the bots were able to pass through. As opposed to reCAPTCHA v2 which requires users to solve Captcha, v3 works in the background, and assess users' behavior to award them a risk score. This technique would make it nearly

impossible for bots to replicate human activity as it takes into consideration features like the movement of the mouse pointer, the typing speed or any other activity that a user might carry out [6]. Moreover, no submissions that should be allowed were blocked, which confirms that reCAPTCHA v3 is almost perfect in detecting and preventing automated attacks, and thus is the most effective technique among the tested ones. This is a better form of defense especially in environments where little user interface interferences are wanted since the procedure utilizes advanced behavioral analysis. However, due to its focus on data-driven changes in behaviors, it has issues of privacy, as will be explained later.

2. User Experience

Another closely related factor based on the designation of anti-spam solutions is the effects that occur on the user experience. Security is important but collecting too much information from the users tends to cause a lot of irritation to users and ultimately harm the user experience.

Plain Form

The plain form is, in contrast, very insecure but it provides the best user experience since no additional actions are required or any identity check. This means that the users can filled their information without any obstructions. But the complete lack of protection really makes it impossible to use in the normal everyday life.

Hidden Fields

Hidden fields are exceptional because they offer a good proportion between the reliability of data protection and the convenience of users interacting with a website or an application. As these fields are hidden from the user interface there are no effects on the submission process. Normal users will be able to use the form as they would under normal circumstances, bots in turn will be recognized and refused access. It is friendly to the end-user, especially when it comes to websites with un-interrupted form interaction without hitches.

reCAPTCHA v2

reCAPTCHA v2 may aggravate the user experience because of the need for interacting with a human. For example, users may be offered choices of images, or to complete puzzles which can be very irritating, especially for a disabled person or a person who is using a rather slow connection to the internet site [13]. Although specifically, the 'I am not a robot' checkbox is not that invasive at all, image based CAPTCHAs could at times create a hindrance as they take time to complete and at times forms are abandoned in the process. This challenge shows that there is a dilemma with respect to security and usability in employing reCAPTCHA v2.

reCAPTCHA v3: As the result, reCAPTCHA v3 gives the best user experience among the tested methods because it works in the background. This means that there is no interference from the user thus eliminating any hindrances that may be found in the submission of forms [7]. This does make the reCAPTCHA v3 very suitable to those websites that want to measure the experience of the end user without compromising on the high security measures put in place. The clients remain ignorant of the measures being taken to protect their data and thus the various interactions can be easily executed without the frustrations that come with the standard CAPTCHA processes.

3. Privacy Concerns

As a protection measure against spam, censorship is important in form protection although some methods work side by side with data collection and analysis thus subjecting user's privacy to compromise as well.

Plain Form & Hidden Fields:

They both has no effect on user privacy since it does not collect or capture the behavior of the users of the application, like the hidden fields do not as well. These methods are perfect for the sites and applications that care about web privacy and do not want to violate the user's rights or gather more data than necessary.

reCAPTCHA v2

Here, the reCAPTCHA v2 entails some extent of data gathering since the system monitors how the users are handling the CAPTCHA test. While this data is mostly applied to check whether the user is a human or a robot, it does cause some privacy issues. Nevertheless, the amount of collected data is lower in comparison to reCAPTCHA v3.

reCAPTCHA v3

Overall, reCAPTCHA v3 poses a huge threat to individuals' right to privacy because of the manner in which it tracks users across the internet. In reCAPTCHA v3, the behavior of the mouse, scrolling speed, and amount of time one spends on a site is assessed and a lot of data is collected to decide if the user is a bot [14].

The level of tracking that social media platforms are capable of can also give rise to some ethical issues regarding the use of users' data without their consent especially in jurisdictions that observe high standards of data protection as pointed out by Lomas [7]. Thus, though, reCAPTCHA v3 is more secure compared to reCAPTCHA v2, website owners have to think of these consequences in relation to the ability to differentiate between bots and actual users more effectively.

4. Implementation Complexity

Another important consideration when informing the decision is the relative simplicity/complexity of implementing each of the anti-spam techniques especially to small websites or ones with low technological capabilities.

Plain Form

Over Internet, the plain form can be used without installation of other forms and thus, can be used as the easiest form. But it means that this system has no security at all, which makes it non-applicable for most web sites.

Hidden Fields

There is also one more interesting field type – hidden fields; to implement them, even simple coding will suffice to place hidden fields in a form. This places them as an excellent choice among websites that lack technical know-how and or are constrained in terms of resources [15]. They are easy to use and for simple bots pose a real threat for bigger websites but for small, less visited and or less-risky websites can serve as a good solution.

reCAPTCHA v2

Compared to the previous version, reCAPTCHA v2 imposes moderate difficulty in terms of integration, but there are extensive choices of plugins and third-party additional services supported by Google reCAPTCHA v2, especially for content management systems such as WORDPRESS [6]. Since pre-built solutions are available, it is not very complicated to integrate reCAPTCHA v2 in almost all sites for even inexperienced developers.

reCAPTCHA v3

reCAPTCHA v3 is the most difficult way to integrate on the webpage. It calls for connectivity with

Google's API and back end for scoring the users' activities [14]. This actually encompasses a workflow that includes installing the API, analyzing traffic and tuning risk scores to enhance bot identification. One could easily credit reCAPTCHA v3 for being more difficult to implement but this version comes with a lot of extra attributes to make web protection as tight as possible which makes it worth using where security is a priority.

Table 3, while reCAPTCHA v3 ranks highest in effectiveness and user experience, it also raises privacy concerns and is harder to implement compared to simpler methods like the plain form. Ask

Table 3. Comparative Analysis

Parameter	Plain Form	Hidden Fields	Recaptcha V2	Recaptcha V3
Effectiveness	Low	Moderate	High	Very High
User Experience	High	High	Moderate	Very High
Privacy Concerns	None	None	Moderate	High
Ease Of Implementation	Very Easy	Easy	Moderate	Difficult

5. CONCLUSION

This paper compares all the methods that may be used to prevent spamming which include plain forms, hidden fields, reCAPTCHA v2, and reCAPTCHA v3 showing the merits and demerits of each in trying to eliminate bots from accessing the various websites. The plain forms have no protection mechanism to safeguard the emails hence a major downfall for spam and, therefore, can hardly be used in daily practice. There is the use of hidden fields which brings a poor level of protection but which are easily penetrated by other advanced bots. reCAPTCHA v2 gives better security than ReCAPTCHA v1 but some advanced bots can pass through it and its user interactivity is somehow disruptive.

Meanwhile reCAPTCHA v3 appears to be the most effective one that safely filters out all bots and does not allow any more submissions from bots without the interference of the user. Because of its deep behavioral analysis, it is one of the most secure bot platforms to use, providing the best bot identification without compromising the use experience of the end-users. But it is based on data collection to differentiate bots from the real users that causes privacy issues in my view. Also, since reCAPTCHA becomes v3, the process of its integration is more complicated than in previous cases and involves further connecting to Google API as well as traffic analysis.

Finally, although reCAPTCHA v3 provides the greatest protection, it is essential to consider the costs of protection and the impact of the solution on users' privacy and web page usability and complexity in terms of its implementation.

Acknowledgments

The authors have no specific acknowledgments to make for this research.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Tracy Fitz-Inteseful	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Joshua Sunkwa		✓		✓		✓			✓			✓		
Dr. William Asiedu	✓	✓	✓		✓			✓		✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

Conflict of Interest Statement

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Informed Consent

All participants were informed about the purpose of the study, and their voluntary consent was obtained prior to data collection.

Ethical Approval

The study was conducted in compliance with the ethical principles outlined in the Declaration of Helsinki and approved by the relevant institutional authorities.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCE

[1] X. Ling-Zi and Z. Yi-Chun, 'A case study of text-based CAPTCHA attacks', in Cyber- Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on, IEEE, 2012, pp. 121-124. doi.org/10.1109/CyberC.2012.28

[2] P. Uma, K. Siddivinayak, and P. Ramachandra, Smart Captcha to Provide High Security against Bots. 2019.

[3] S. Vaithyasubramanian, D. Lalitha, and C. K. Kirubhashankar, 'Enhancing website security against bots, spam and web attacks using lCAPTCHA', Int. J. Comput. Appl., vol. 45, no. 1, pp. 63-69, Jan. 2023. doi.org/10.1080/1206212X.2019.1702285

[4] Y.-W. Chow, W. Susilo, and P. Thorncharoensri, 'CAPTCHA Design and Security Issues', in Advances in Cyber Security: Principles, Techniques, and Applications, Singapore: Springer Singapore, 2019, pp. 69-92. doi.org/10.1007/978-981-13-1483-4_4

[5] N. T. Dinha and V. T. Hoang, Recent advances of Captcha security analysis: a short literature review. 2023. doi.org/10.1016/j.procs.2023.01.229

[6] Google Developers. (2020). reCAPTCHA v2 and v3. Retrieved from https://developers.google.com/recaptcha

[7] N. Lomas, Google's Invisible reCAPTCHA: Convenient or Creepy? *TechCrunch*, 2018.

[8] K. Gupta and R. Gupta, 'An analysis of various CAPTCHA techniques to resist bot attacks', _International Journal of Computer Science, 2017.

[9] Brown, K., & Williams, P. (2019). Web form vulnerabilities and mitigation strategies.

[10] P. Stasiuk and V. Kopylov, Bot Interaction with Plain Forms: Vulnerability Assessment. 2020.

[11] Gupta, S., & Gupta, A. (2017). Anti-spam techniques in web applications.

[12] S. Sivakorn, I. Polakis, and A. Keromytis, 'I Am a Robot: CAPTCHA Breaking via Deep Learning', in IEEE Symposium on Security and Privacy, 2016, pp. 45-60.

[13] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, 'The web never forgets: Persistent tracking mechanisms in the wild', Proceedings of the ACM on Web Science, pp. 105-116, 2018.

[14] Google Developers. (2020). reCAPTCHA developer's guide. Retrieved from https://developers.google.com/recaptcha

[15] V. Klyuev, 'Honeypot Techniques for Web Forms: Efficiency and Security', Journal of Information Security, vol. 10, no. 1, pp. 1-12, 2018.

How to Cite: Tracy Fitz-Inteseful, Joshua Sunkwa, Dr. William Asiedu. (2025). A comparative analysis of the effectiveness of recaptcha v3 against recaptcha v2, hidden fields, and other anti-spam techniques. International Journal of Information Technology and Computer Engineering (IJITC), 5(1), 1-14. https://doi.org/10.55529/ijitc.51.1.14

BIOGRAPHIES OF AUTHORS

	**Tracy Fitz-Inteseful** Tracy Fitz-Inteseful is a lecturer at the Department of Information Technology Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED), Kumasi, Ghana. Her research interests include cybersecurity, web application security, and user experience in digital systems. She has worked extensively on web-based anti-spam technologies and automation detection techniques. Email: tracyadjoa@yahoo.com
	**Joshua Sunkwa** Joshua Sunkwa is an academic researcher in the Department of Information Technology Education at AAMUSTED, Ghana. His primary areas of expertise are software engineering, automation testing, and the development of secure web applications. He has contributed to several studies on web security protocols and AI-driven solutions for spam detection. Email: hellosunkwa@gmail.com
	**Dr. William Asiedu** Dr. William Asiedu is a senior lecturer and cybersecurity specialist at AAMUSTED, Kumasi, Ghana. He holds extensive experience in network security, ethical hacking, and information assurance. His academic contributions include several published works on data privacy, cybercrime prevention, and advanced security mechanisms for web applications. Email: wasiedu@aamusted.edu.gh