A Robust Captcha Scheme for Web Security

Yash Raut

*Department Of Computer Engineering Ramrao Adik Institute of Technology* Nerul, Navi Mumbai, India [rautyash2000@gmail.com](mailto:rautyash2000@gmail.com)

Harshank Boricha *Department Of Computer Engineering Ramrao Adik Institute of Technology*

Nerul, Navi Mumbai, India [harshboricha1997@gmail.com](mailto:harshboricha1997@gmail.com)

Shreyash Pote *Department Of Computer Engineering Ramrao Adik Institute of Technology*

Nerul, Navi Mumbai, India [10shre](mailto:10shreyashpote@gmail.com)[yashpote@gmail.com](mailto:yashpote@gmail.com)

Prathmesh Gunjgur *Department Of Computer Engineering Ramrao Adik Institute of Technology*

Nerul, Navi Mumbai, India [prathmesh.gunjgur@rait.ac.in](mailto:prathmesh.gunjgur@rait.ac.in)

***Abstract*—The internet has grown increasingly important in everyone’s everyday lives due to the availability of numerous web services such as email, cloud storage, video streaming, music streaming, and search engines. On the other hand, attacks by computer programmes such as bots are a common hazard to these internet services. Captcha is a computer program that helps a server-side company determine whether or not a real user is requesting access. Captcha is a security feature that prevents unauthorised access to a user’s account by protecting restricted areas from automated programmes, bots, or hackers. Many websites utilise Captcha to prevent spam and other hazardous assaults when visitors log in. However, in recent years, the complexity of Captcha solving has become difficult for humans too, making it less user friendly. To solve this, we propose creating a Captcha that is both simple and engaging for people while also robust enough to protect sensitive data from bots and hackers on the internet. The suggested captcha scheme employs animated artifacts, rotation, and variable fonts as resistance techniques. The proposed captcha technique proves successful against OCR bots with less than 15% accuracy while being easier to solve for human users with more than 98% accuracy.**

***Index Terms*—CAPTCHA, CAPTCHA attacks, OCR, Bot, Web security, Synthetic artifacts, Rotation**

1. INTRODUCTION

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), an automated security method that identifies whether or not a user is a human or a dangerous bot is known as Captcha. This application develops and analyses basic tests/tasks that are easy for humans to complete but difficult for malicious computer programs to conduct and analyze. It is a challenge-response test that determines whether or not a user is a natural person.

A Captcha is used to prevent spam bots from filling out forms and stealing data. Spam-bots are algorithms that harvest email addresses and other data from public websites. On most websites, visitors must enter in a sequence of distorted characters. However, bots fail to interpret distorted visuals that humans may rapidly solve. Since people try to cheat the system by exploiting computer problems, a test to distinguish humans from bots was established. Using free email could overburden

them with account requests. Spammers are continually up- grading their algorithms to detect and scan altered messages. Robust Captcha’s must be created to prevent attacks. Weak Captcha’s cause usability and scalability issues. A Captcha must be powerful to be user-friendly and secure against malicious bots. Computer vision and pattern recognition have lately solved numerous well-known Captcha’s. As a result, security experts have been motivated to build new Captcha’s that are complex for computers to beat yet easy for people to decipher. This work tries to produce a more secure and efficient captcha set that may be less likely to be hacked by existing captcha bots but stays simple for humans.

The synthetic artifacts have been integrated with the captcha to make it challenging for bots. Hats, hands, spectacles, and other supplementary items are instances of artificial objects. According to a study [1], synthetic artifacts can be utilized to fool a machine learning based recognition system. Recently,

1. demonstrated a misclassification attack on the current state- of-the-art; this study intended to physically place eyeglasses on a person’s face in an image, causing a deep neural network- based facial recognition system to misclassify the subject. This method can also deceive the recognition systems by adding synthetic artifacts over text Captcha’s.

The key contributions of this work is summarized as fol- lows:

* + Highlight the vulnerability of the presently used text Captcha schemes by websites.
  + Highlight that existing text-based captchas are less user- friendly and difficult to understand for human users.
  + Introduces a new type of text-based image Captcha scheme that is both secure and user-friendly.
  + Analyses the robustness and user friendliness and robust- ness of proposed Captcha scheme.

The remainder of this paper is organized as follows. In Section II, the most relevant related works are reviewed. Section III introduces to the proposed system and discusses the designing of the proposed Captcha. Section IV presents the

performance evaluation of the proposed Captcha and discusses the results, and finally, Section V concludes the paper.

1. LITERATURE SURVEY

In this section, we present some recent research undertaken in the Captcha based security.

Y. Zi et al. [1] describe a no-preprocessing, simple, uni- versal, and efficient end-to-end assault on text Captchas. The results show that deep learning attacks can ultimately defeat the anti-segmentation principle without segmentation or preprocessing steps. A convolutional neural network and an attention-based recurrent neural network were used in their assault.

In this paper, F. Liu et al. [2] describe a text-based Captcha cracking solution based on convolutional neural networks (CNN). They propose combining CNN and conditional deep convolutional generative adversarial networks (cDCGAN) to overcome the small sample problem and achieve remarkable accuracy gains. They also choose different models for the majority voting ensemble with low Pearson correlation co- efficients, which improves accuracy even more. Experiments show that the system has significant advantages and provides a novel method for breaking Captchas.

In this suggested technique, Nayeem et al. [3] tried to balance readability and security by introducing additional contextual information to a natural dialogue while reducing distortion and noise. To obtain detailed user views of current Captcha systems like Google’s reCAPTCHA and Microsoft’s CAPTCHA, a case study involving 110 users was conducted. As a result, the system was deployed primarily through the internet.

Text-based Captchas have become highly vulnerable to machine learning-based assaults as a widely deployed security system. In this paper, C. Li et al. [4] present a simple and ef- fective end-to-end attack based on cycle-consistent generative adversarial networks (Cycle-GANs). The findings also show that combining different anti-recognition actions can enhance Captcha security.

Computer vision technology becomes more vulnerable to attack as it advances. H. Weng et al. [5] provide simple yet effective attack methods for each popular type of picture Captcha. They also investigate the underground market for captcha-solving solutions, discovering 152 and comparing them to data from these services. Finally, they point out some design flaws in these widely used systems and some best procedures and ethics for creating more secure captchas.

A Captcha is a security device used to prevent computer programs from abusing internet services intended for peo- ple. Many well-known Captcha’s have recently been solved using computer vision and pattern recognition techniques. A study by N. Roshanbin and J. Miller [6] introduces modern Captcha’s and attacks against them and analyzes their robust- ness and usability. They also talk about making Captcha’s that are more robust and applicable in real-world circumstances.

Text-based Captcha’s are still frequently employed as a security technique despite various proposed attacks. Most of

those recent attacks, on either hand, are strategies and require a tedious process to build. However, G. Ye et al. [7] propose a generative adversarial network-based text captcha solution that is otherwise general and efficient. It can solve a captcha in 0.05 seconds using a desktop GPU.

Adversarial generative nets (AGNs) are proposed by M. Sharif et al. [8] as a generic approach for training a generator neural network to generate malicious samples that satisfy specified objectives. They show tangible adversarial instances, such as eyeglass frames meant to deceive facial recognition, that is more robust, unobtrusive, and scalable than earlier efforts and a novel attack to trick handwritten-digit classifier. Gao et al. [9] describe a primary, cheap, but robust assault that successfully defeats a wide variety of text Captcha’s with varying design factors, even those used by Google, Microsoft, Yahoo!, Amazon, and other internet behemoths. Moreover, based on Log-Gabor filters, their approach had a better success rate varying from 5% to 77% for all schemes, with fewer than 15 seconds to solve a puzzle on a conventional desktop

computer.

A. Dionysiou and E. Athanasopoulos [10] analyze and categorize cutting-edge ML-based approaches for automated text-based Captcha cracking challenges. According to their findings, ML can significantly improve the Captcha solution’s accuracy, speed, and abstraction. Overall their research implies that different approaches to administering the reverse Turing test that is hassle-free for humans but tough for automated systems should be investigated.

DeepCAPTCHA is a novel but strong Captcha strategy based on adversarial scenarios, which addresses an intrinsic shortcoming of current deep learning networks. These adver- sarial cases are built from scratch either by adding a small and precise perturbation called adversarial noise to effectively classify items, causing the tailored DL network to misinterpret them. M. Osadchy et al. [11] demonstrate that conventional adversarial noise is insufficient for safe Captcha methods, prompting us to initiate constant adversarial noise.

Adversarial examples create an image by purposefully al- lowing a machine learning picture categorization to be incor- rect. Human readability is compromised as the character string Captcha adds distortion and noise to avoid being read by the computer. Adversarial instances generated with the traditional Fast Gradient Sign Method (FGSM) cannot misclassify strong nonlinear networks like CNN. This study by T. Azakami et al.

[12] suggests using the FGSM on character string Captcha’s and allowing CNN to misclassify them.

Captcha’s are rapidly being employed in various machine and human identification applications. However, Chinese char- acters have more complex characters making automatic recog- nition much more challenging. Zhang et al. [13] suggest a CNN technique to overcome this challenge. This method sig- nificantly enhances distortion, rotation, and background noise recognition accuracy. According to their findings, this method accomplishes over 95% accuracy for a single character and 84% accuracy for three forms of Chinese character Captcha’s of four characters.

Y. Gao et al. [14] used a holistic and modular assault, with 67.3% and 88.0% overall success rates on the Visual Turing Test (VTT) Captcha. The results reveal that visual reasoning Captcha’s is not as safe as it appears. However, given their assaults, they also advise developing more secure visual Captcha’s.

The Captcha was created to give a suitable level of secu- rity in situations where bots should be deterred from taking specific actions, i.e. signing up and downloading. Despite its numerous benefits, its use is fraught with security, usability, and accessibility issues. Sasmal et al. [15] attempted to present a complete study of various elements, state-of-the-art Captcha, and alternatives.

*A. Limitations of the Existing System*

Recent research suggests that most of the real-world Captcha documents are less secure and that existing methods of resistance are not as effective as expected. Here, we try to list some issues in this regard:

* Not easy to use - Complex Captcha’s created today have a high level of success against bots but are not easy for human users to interpret. For example, success rates for the most secure text Captcha systems, as shown in Figure 1 were only 7.7% and 3.3%, respectively, but these two programs were unfriendly and invisible to the public, with user accuracy of 9.9% user accuracy and 5.2% respectively, as shown in Figure 2, indicating that these two programs are ineffective to use.

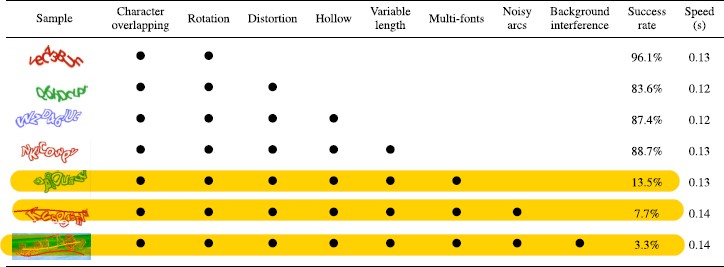


Fig. 1. Attack results on complex text captchas [1]

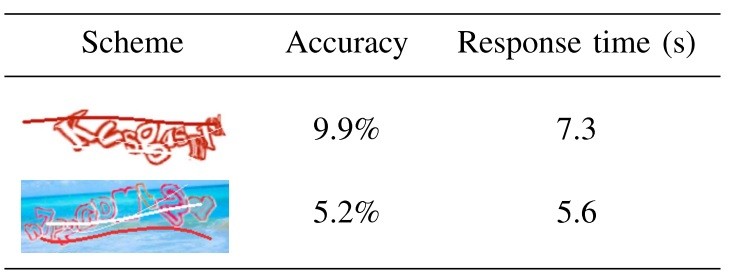


Fig. 2. Human readability analysis of two complex Captcha’s Accuracy & Response time [1]

* There are many problems with Captcha’s, significantly because they distort the text and images so that, some- times, it is difficult to even for people to read. Even an elementary yet effective Captcha, like math “What is the sum of three and five? can be painful for people with a mental disability [3].
* Some of the problems with specific fonts are: Distortion becomes a problem if done informally. Some letters such

as “d” can confuse “cl” or “m” with “rn”. It should also be easily mistaken for those who do not know the language well and maybe misunderstand [6].

1. PROPOSED METHODOLOGY

Captcha’s prevent bots from accessing many types of com- puter services or gathering sensitive information. In addition, they can help prevent bot-generated spam by compelling the (anonymous) sender to pass the Captcha test before the email message is delivered. Still, spammers can also use them to hinder optical character recognition (OCR) detection of spam from images attached to emails. Therefore, the proposed approach uses synthetic artifacts with a Captcha to make it hard for attacking bots to solve the Captcha.

This method is on creating a new type of captcha scheme that focuses more on the personal involvement of the user by introducing easy-to-understand Captcha by using simple animated distortions such as “Animated artifacts”. The 3D Cartoon Captcha characters created are aimed to be harder for bots to detect but still be easy for human users to interpret. The following modules are included in this work:

1. **Model molding**: This module is based upon creating interference objects (synthetic artifacts) and animated 3D text characters to create confusion for the captcha attacking systems. The artifacts and animated text char- acters will be created in this module.
2. **Integration**: The animated objects are then combined and aligned to create snapshots of captcha text as im- ages. These images are then integrated with the captcha generator. The captcha generator shows the captcha image chosen in random format from the set of uploaded captcha images.
3. **Captcha generator and testing**: This is the final part of the project. The 3d models and the web-based captcha generator integrated are tested by both real users and OCR attacking bots to judge the captcha’s strengths on various parameters like accuracy, readability, etc.

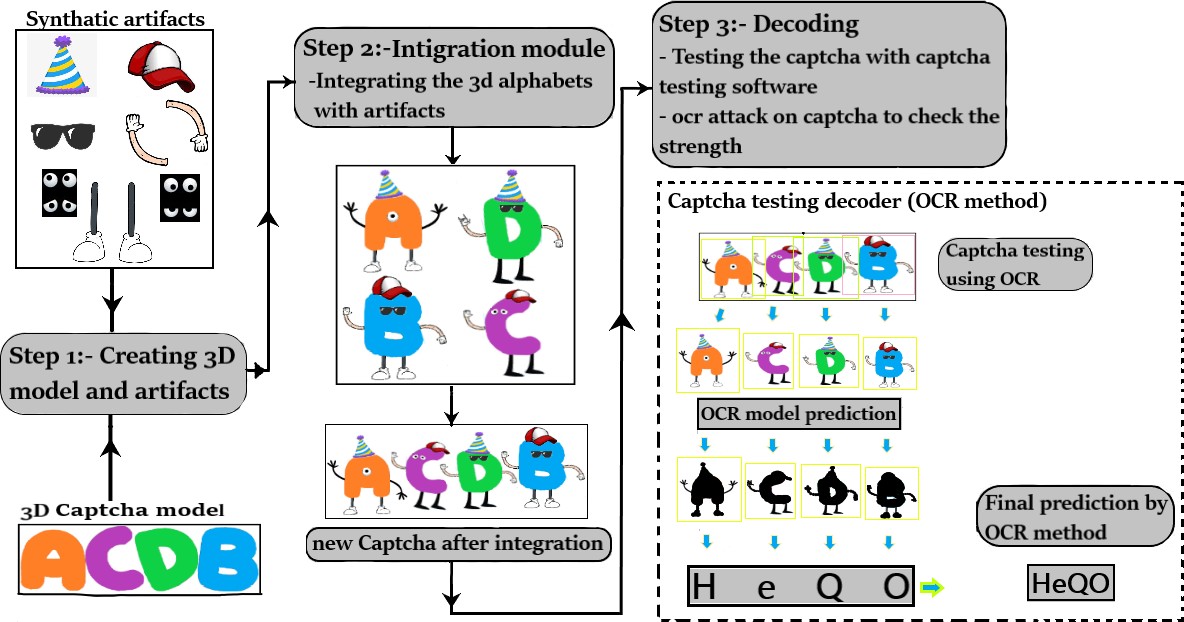


Fig. 3. System Architecture

The proposed goal of this study is to produce a unique and robust captcha by building 3D models of alphabets and syn- thetic artefacts like hands, spectacles, legs, etc., as interference objects, as seen in the system architecture in Figure 3. Next,

these animated objects are incorporated with the web-based captcha generator. Finally, the Captcha is evaluated on multiple Captcha cracking websites, which use the OCR technology to break captchas. Also, the Captcha is tested with real humans to evaluate how it operates in the real world.

*A. Model molding*

This module begins with developing the character model of the alphabet, which is a crucial aspect of this work. Using synthetic artifacts over the 3D alphabet models would cause OCR based algorithms to misclassify the subject. This task started with developing simple figure drawings as a base in the paint software, which would be used later for creating 3D models of the characters. The 3D model of the alphabet was then produced using the Blender application. Figure 4 displays the base drawings of the text characters generated using the Paint 3D software.

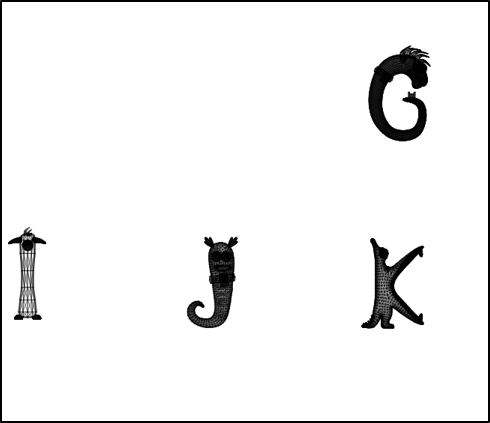


Fig. 4. Base drawings of model

were finalized, the next step was texturing and aligning the models. After taking screenshots of these aligned models, we moved to create a random Captcha generator. Next, we “integrated” the screenshots with the Captcha generator to display random Captchas in this module. Figure 5 shows the final set of text characters created on the blender tool. Figure 6 shows the captcha generator made using python tkinter. Figure 7 shows the artifacts created using the blender tool.

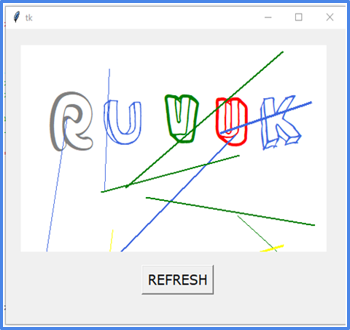


Fig. 6. Random Captcha generator

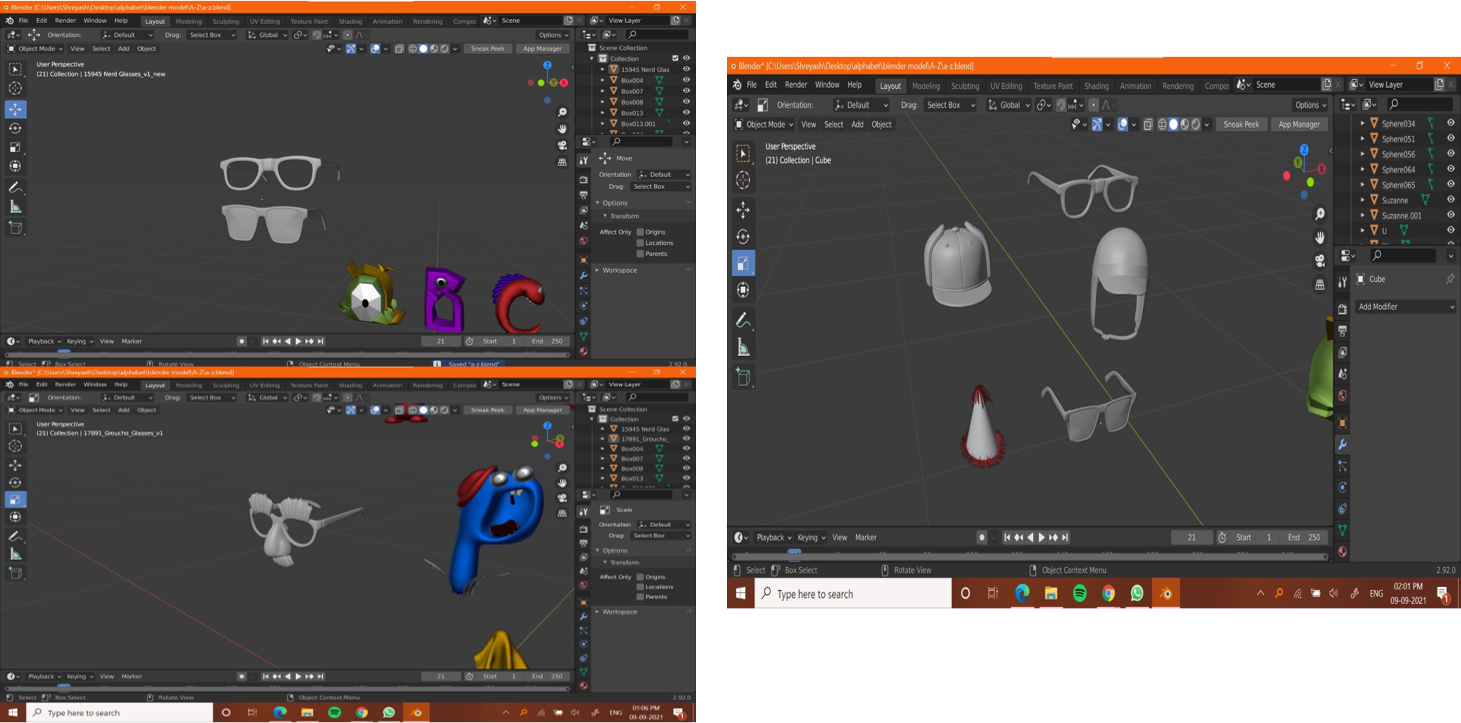
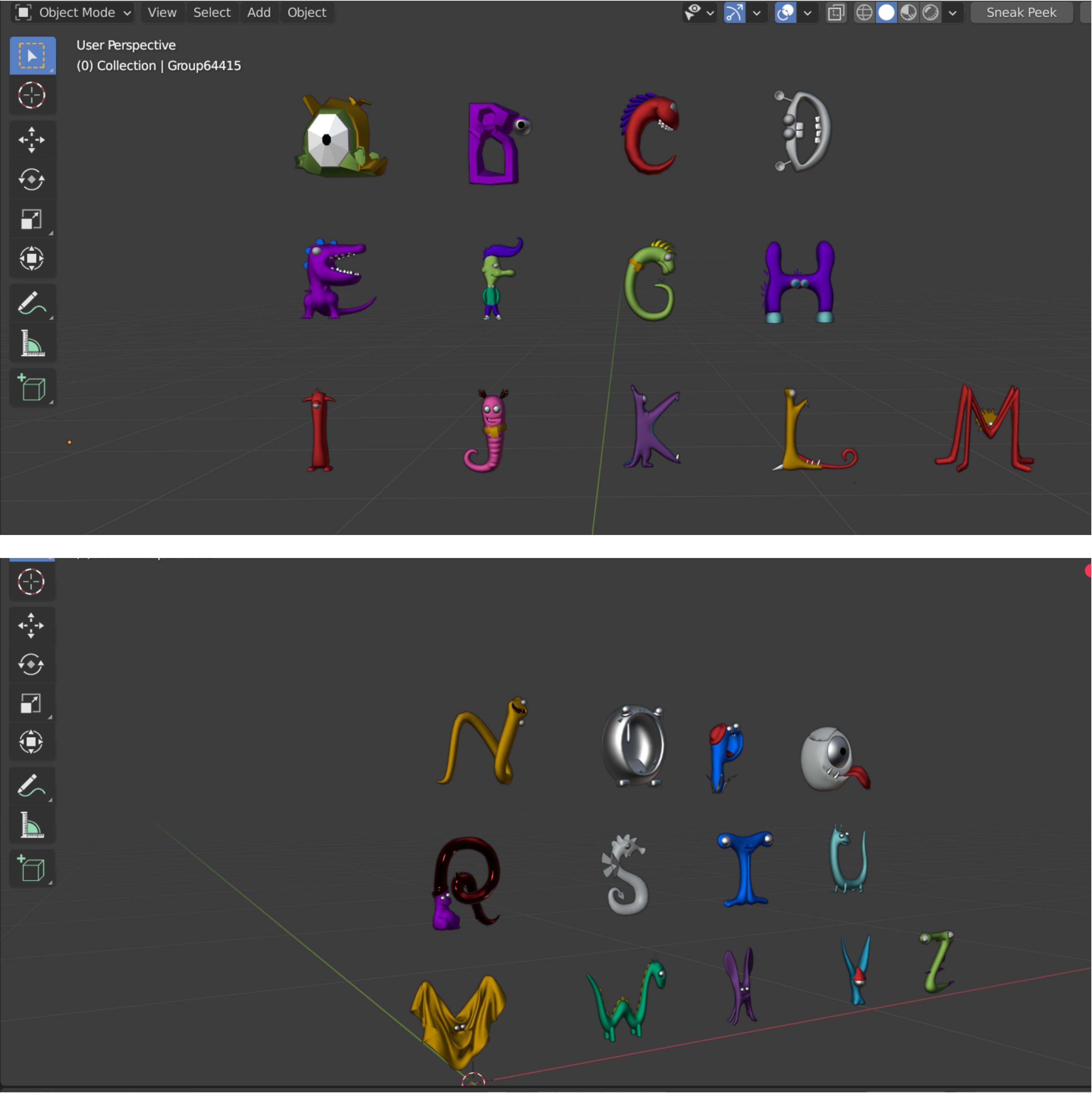


Fig. 7. Synthetic artifacts renders

*C. Captcha generator and testing*

In this module, we created the final state of the Captcha generator and performed testing. We surveyed around 200 users to test the various parameters of the proposed captcha scheme like readability, accuracy, response time, etc. Further, we tested the robustness of Captcha by using publicly available OCR bots.

*B. Integration*

Fig. 5. 3D model renders

1. RESULTS AND DISCUSSION

This section describes the evaluation of the proposed Captcha through various performance parameters and dis- cusses the results.

The efficiency of Captcha in rejecting and predicting the attacks of Bots is one of its greatest strengths. Therefore, we tested the proposed Captcha with more than 200 users to study how well the Captcha performed when real-world

In this module, we created the models of the alphabets from the sample drawings, which were already drawn using the Paint 3D software. Later, we designed the synthetic 3D artifacts for the model alphabets using the Blender application to make the Captcha more secure and robust. Once the models

users tried to solve the Captcha, and based on the generated responses and data through this test; we were able to analyze and grade the Captcha on various parameters like accuracy, response time, readability, etc. The most prevalent challenges reported by most Captcha are as follows:

1. **Readability**: The Captcha must be easily legible and decipherable by humans to be effective. In our survey, more than 200 persons participated, and the findings are shown in the form of a pie chart in Figure 8. This result indicates that 98% of the users found the Captcha easily accessible and suitable for captcha recognizability and readability.

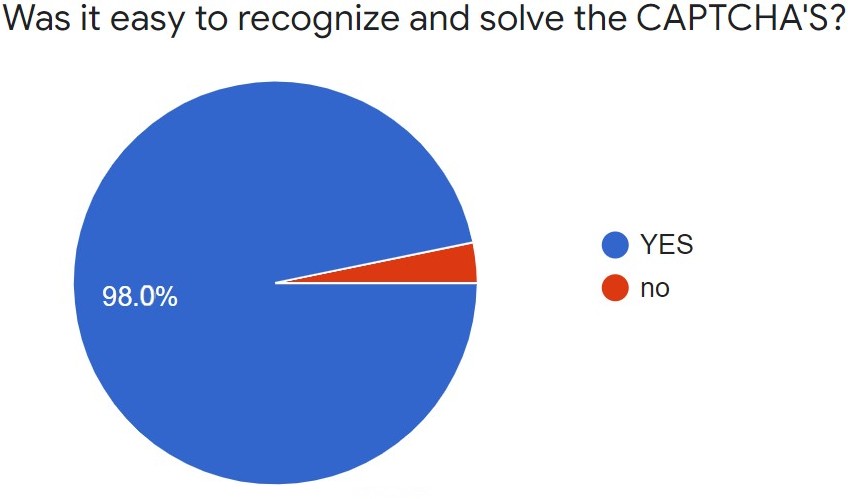


Fig. 8. Pie chart of readability

1. **Unguessability**: There’s no way to estimate the Captcha at random and be confident about the outcome. The Captcha should not be detectable by the OCR technol- ogy to function successfully. If OCR software could read the characters in the Captcha image, it would render the Captcha worthless to prevent malicious assaults. The below graph seen in Figure 9 shows the percentage of how humans were able to recognize and solve the Captcha compared to attacker bots which were using the OCR technique to break the Captcha. Figure 10 shows the accuracy percentage and guessablity of the proposed Captcha by the OCR technique.

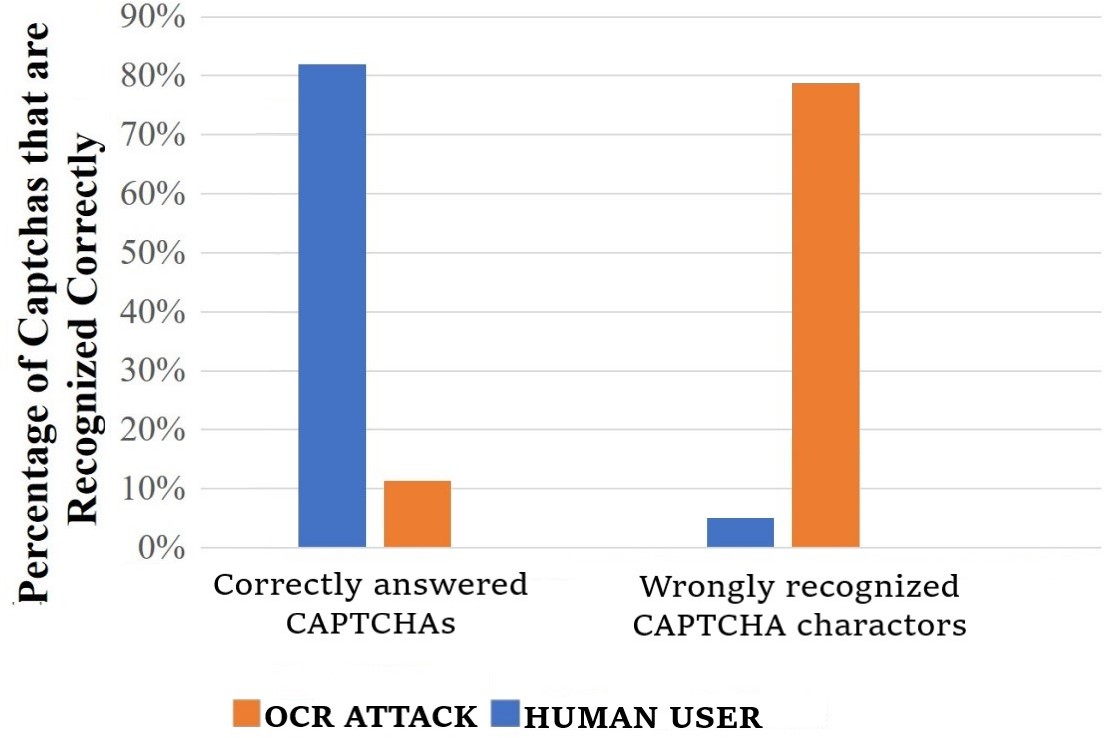


Fig. 9. Unguessability graph comparing between Bot and Human

1. **Accuracy**: Accuracy is the user’s ability to pass the Captcha challenge. Here the users were asked to rate the Captcha based on how easy/satisfying it was to solve them; based on this; we estimated the accuracy of the Captcha. So the users rated out of 5, where 5 is the highest rating and 1 is the lowest, and according to the pie chart shown in Figure 11, which depicts how easy the Captcha was to solve for humans, 85.7% chose 5



Fig. 10. OCR Accuracy for the Proposed Captcha

and 14.3% chose 4, which is very good for the captcha accuracy or solvability.

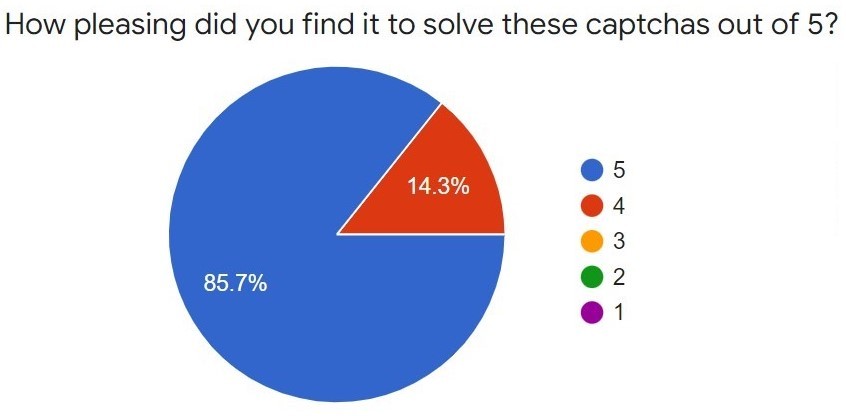


Fig. 11. Human Captcha Solvability

1. **Response time**: It is average time it takes for a user to pass the test. People differ in their perception of how tough it is to use a Captcha. The less the time taken to recognize and solve the Captcha, the better is the Captcha. Figure 12 shows the human accuracy and the average response time to solve the proposed Captcha.

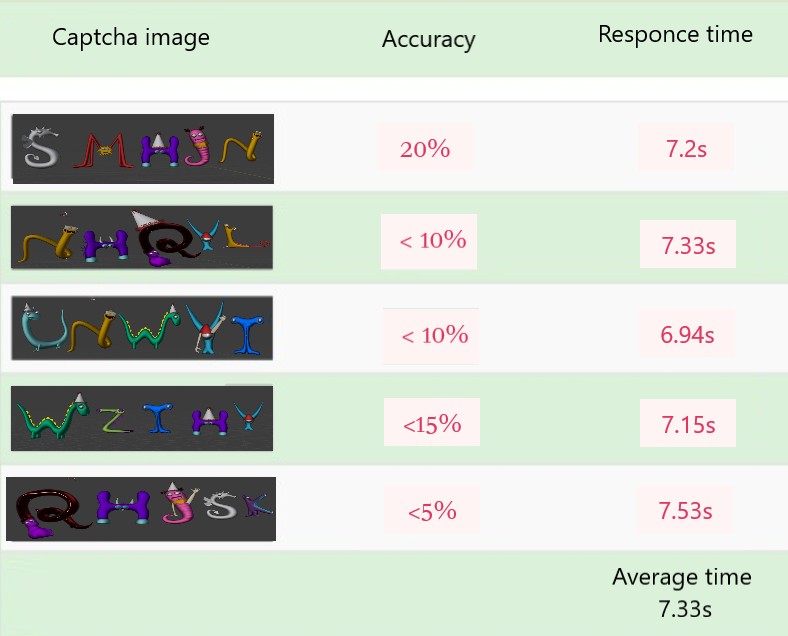


Fig. 12. Human Accuracy and Response Time for the Proposed Captcha

*A. Types of Noise used*

* **Use of Artifacts**: The Captcha text contains synthetic artifacts for noise creation; the artifacts cover or block the text to create confusion for the Captcha cracking bots.
* **Rotation**: The captcha text has used rotation to add more difficulty for Captcha cracking bots.
* **Variable Font**: The fonts used in Captcha text are en- tirely unpredictable and unique. Existing bots will find it challenging to identify the Captcha set due to its variable font size.

1. CONCLUSION

As the quantity of web-based services rises, so does the number of website attacks, putting both the user and the website at risk. Captchas, as they exist currently, are worthless in countering these attempts. Attackers can swiftly defeat most captchas on major websites using OCR or CNN techniques to crack text Captcha schemes, exposing those sites to vul- nerability. As a result, the suggestion is to construct a more robust and more powerful captcha. However, although difficult for bots, text captchas typically employed nowadays are less desired and excessively complex. Even real humans find some captchas frustrating and challenging to complete since they are demanding and time-consuming. Hence, the proposed system seeks to address all of these issues.

The proposed strategy combines 3D models and interference objects called synthetic artifacts, to build a new, more resilient sort of captcha scheme that is entertaining and simple for the user but difficult for bots to crack, hence tricky for attackers to penetrate. It established an innovative strategy by constructing interference objects with easy to understand synthetic objects such as spectacles, a set of hands and legs, caps, and sunglasses. Our test findings prove that our Captcha was resistant to the OCR technique of assault, which is the most often exploited by attackers to crack captchas and can break the majority of captchas globally. The survey’s findings indicate that more than 98% of human users had an easier time answering this Captcha. On the other hand, the OCR- based bots struggle to recognize the text in this Captcha and fail to react or detect on an average of less than 15% accuracy.

REFERENCES

1. Y. Zi, H. Gao, Z. Cheng and Y. Liu, “An End-to-End Attack on Text CAPTCHAs,” in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 753-766, 2020.
2. F. Liu, Z. Li, X. Li, and T. Lv, “A text-based CAPTCHA cracking system with generative adversarial networks,” 2018 IEEE International Symposium on Multimedia (ISM), pp. 192–193, 2019.
3. M. T. Nayeem, M. R. Akand, N. Sakib, and W. U. Kabir,“Human Cognition in Automated Truing Test Design,” International Journal of Software Science and Computational Intelligence (IJSSCI), vol. 6, no. 4, pp. 1–19, 2014.
4. C. Li, X. Chen, H. Wang, P. Wang, Y. Zhang, and W. Wang, “End-to-end attack on text-based CAPTCHAs based on cycle-consistent generative adversarial network,” Neurocomputing, vol. 433, pp. 223–236, 2021.
5. H. Weng et al. “Towards understanding the security of modern image captchas and underground captcha-solving services,” Big Data Mining and Analytics, vol. 2, no. 2, pp. 118–144, 2019.
6. N. Roshanbin and J. Miller, “A survey and analysis of current CAPTCHA approaches,” Journal of Web Engineering, vol. 12, no. 1–2, pp. 001–040, 2013.
7. G. Ye et al., “Yet another text CAPTCHA solver: A generative adver- sarial network based approach,” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 332–348, 2018.
8. M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, “A general framework for adversarial examples with objectives,” ACM Trans. Priv. Secur., vol. 22, no. 3, 2019, doi:10.1145/3317611.
9. H. Gao et al., “A Simple Generic Attack on Text Captchas,” NDSS Symposium, 2016.
10. A. Dionysiou and E. Athanasopoulos, “SoK: Machine vs. machine

– A systematic classification of automated machine learning-based CAPTCHA solvers,” Computers & Security, vol. 97, p. 101947, 2020.

1. M. Osadchy, J. Hernandez-Castro, S. Gibson, O. Dunkelman and D. Pe´rez-Cabo, “No Bot Expects the DeepCAPTCHA! Introducing Im- mutable Adversarial Examples, With Applications to CAPTCHA Gen- eration,” in IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2640-2653, 2017.
2. T. Azakami, C. Shibata, R. Uda and T. Kinoshita, “Creation of Adversar- ial Examples with Keeping High Visual Performance,” 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), pp. 52-56, 2019.
3. X. Zhang, J. Zhang, and S. Zhang, “Chinese Character CAPTCHA Recognition Based on Convolutional Neural Network,” Proceedings of the 2019 International Conference on Robotics Systems and Vehicle Technology, pp. 108–112, 2019.
4. Y. Gao et al., “Research on the security of visual reasoning CAPTCHA,” 30th USENIX Security Symposium (USENIX Security 21), pp. 3291–3308, 2021.
5. M. Sasmal, P. Ray, M. Sen, R. Mukherjee and S. Bandyopadhyay, “A Brief Review on Text and Image CAPTCHA,” Turkish Journal of Computer and Mathematics Education, vol. 11, pp. 508–526, 2020.