iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68567

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Develop an Artificial Intelligence Model Solution to Refine CAPTCHA

Asst. Prof. Geetha G[1], Kesavan M[2], Manoj Kumar M[3], Udhaya Kiran M R[4], Srinivasan R[5]
Department of Artificial Intelligence & Data Science, J. N. N Institute of Engineering (Autonomous), Chennai

Abstract: ***Completely Automated Public Turing tests to narrate Computers and Humans Apart (CAPTCHAs) are established for protection purposes, but their growing complicatedness frequently hampers consumer occurrence. This project presents a Machine Learning model to refine CAPTCHA by reinforcing protection while asserting approachability. The model influences deep education methods, particularly Convolutional Neural Networks and Recurrent Neural Networks to analyse CAPTCHA patterns, discover proneness, and improve their design. A fruitful approach utilizing Generative Adversarial Networks guarantees CAPTCHAs remain opposing to computerized solvers while being handy. Additionally, Optical Character Recognition models are used to judge CAPTCHA strength and upgrade human readability. The projected resolution aims to balance protection and utility by underrating dishonest contradiction while guaranteeing elasticity against advanced bots. The model is prepared on a various dataset of CAPTCHAs to boost changeability. This approach improves confirmation systems, providing a secure still approachable proof design across mathematical podiums.***

Keywords: ***Character Recognition, Convolutional Neural Network, Data Augmentation, Segmentation, Transformers for Recognition.***

I. INTRODUCTION

The chance of a various range of travelling devices and more inexpensive speedy dossier subscriptions pushed consumers' interest in Internet use. From allure beginning, Internet freedom has happened the primary concern of netting planners. As the Internet resumes to evolve for providing differing websites, services, and blogs similarly evolve. Today's websites are loyal to all, transportation, pleasure, economic duties, fare articles, healthcare, and hotel stipulations, to mention any. In this regard, the increasing consumer base also makes necessary the arrangement of expensive calculating power at the websites. However, these exclusive processors are performed useless. If the exclusive mechanized device goals bureaucracy. Therefore, the defence against aforementioned robotic attacks is imperative. However, in an open-approach network surroundings, the omnipresence of the Internet is bright security dangers for things win network approach. It is not a smooth task for the web help providers to learn either the application is achieve by a bot or a human consumer. Nonetheless, bot programs are intensely beneficial to carry out recurrent and period passionate movements. Oppressed for hateful work, bot programs have human behaviour reproduction strength. Therefore, freedom is the vital element in a trustworthy communication connect. It points to sheltering and saving networks from nasty attacks.
Introducing protection duties in computer networks inquires to give handy, reliable, and top-secret request surroundings and there is miscellaneous calculating taking advantage, including worms, mock, viruses, and network junction. Moreover, other types of attacks hopeful unwarranted ones: clandestine channels, Denial of Services and marred and hateful nodes, to name any. A plurality of Completely Automated Public Turning test to speak Computers and Humans Apart (CAPTCHA) systems have happened projected that use differing features, in the way that figures, countenances, and audio, to create challenges that efficiently bar automated bots. However, current progresses in Artificial Intelligence usually and Computer Vision in particular have considerably revised automated orders' strength to resolve such tasks plus, principal part common CAPTCHA systems have existed gave in. Hence, skilled needs to have an in-depth reasoning of CAPTCHA composition and allure breaking techniques to form bureaucracy healthier and usable.
CAPTCHA Human Interaction Proof is imported to check counterfeit network resources approach it was invented in 2000 by Luis von Ann at Carnegie Mellon University. It is a care design for preventing photoelectric registration, unsolicited call, and injurious bot requests. They are famous for providing experienced safety by differentiating persons from calculating's, e.g., lock-free Email duties, protecting connected to the internet polling against online vote bots, or hateful electronic mail sign-boosts. They are active in handling electronic mail worms and marketing mail and in forestalling language located identification attacks. In general, a test that is natural for population to resolve and troublesome for calculating's is create and evaluated.

It is regarded profitable if allure achievement rate cruel answers is greater than 90%, and calculating reach just a profit rate of inferior 1%. A powerful CAPTCHA is mainly known, not only working but resistant. It is steadily developing electronics and is progressively growing in research and practice. The arising article remarks must be summarised, and a more inclusive reasoning of CAPTCHAs must be carried out.

1) CAPTCHA Overview: CAPTCHA structures were first made acquainted in the early 2000s to combat electrical bots. They are created to present challenges that are smooth for humans but troublesome for machines, to a degree making crooked document, labelling objects in images, or resolving visual and audio entertainment transmitted via radio waves baffles. Text-located CAPTCHAs are ultimate coarse type and typically include crooked alphanumeric individualities accompanying additional roar or obfuscation.

2) Machine Learning in CAPTCHA: Breaking Machine learning, specifically deep education, has transformed the field of calculating dream, enabling models to act tasks to a degree figure acknowledgment and object discovery accompanying high veracity. Convolutional affecting animate nerve organs networks (CNNs) have happened specifically direct in understanding patterns in images, making bureaucracy suitable for CAPTCHA-breaking uses. Recent studies have displayed that ML models can realize extreme accuracy rates in answering CAPTCHAs, lifting concerns about their safety.

3) Related Work: Several studies have surveyed the use of ML models to break CAPTCHAs. For example, [1]second-hand CNNs to achieve extreme veracity in making crooked individualities, while [2] projected a hybrid approach joining CNNs and repeating affecting animate nerve organs networks (RNNs) for subsequent CAPTCHA acknowledgment. These studies climax the potential of ML models to bypass CAPTCHA schemes and emphasize the need for stronger designs. Research Objective: The research focuses on constructing a machine intelligence model to break CAPTCHAs, judging its act, and utilizing the verdicts to upgrade CAPTCHA designs and connected to the internet security. It still addresses righteous concerns and advances change in cybersecurity.

4) Develop a CAPTCHA-Breaking Model: Build a machine intelligence model, like a CNN, to correctly answer document-located CAPTCHAs.

5) Evaluate Performance: Test the model's veracity and strength on CAPTCHAs accompanying various levels of complicatedness (such as, deformities, turbulence). Identify CAPTCHA Weaknesses: Analyse by means of what the model breaks CAPTCHAs to find vulnerabilities in current designs. Optimize Pre-transform: Use methods like clamour decline and personality separation to enhance recommendation dossier status.

6) Compare with Existing Methods: Compare the model's depiction accompanying usual CAPTCHA-breaking methods.

7) Address Ethical Concerns: Discuss the moral associations of building CAPTCHA-breaking forms and imply trustworthy use directions.

8) Improve CAPTCHA Design: Provide approvals for plotting more secure CAPTCHA structures.

9) Contribute to Adversarial ML: Advance research in opposing machine intelligence by investigating how ML can exploit safety structures.

10) Promote Security Innovation: Encourage the happening of leading confirmation systems, like biometrics or multi-determinant methods.

A. Types of CAPTCHA

Text-based CAPTCHA [1], Image-based CAPTCHA [2], Audio-based CAPTCHA [3], Math-based CAPTCHA [4].

Classification of CAPTCHA's based on their types:

CAPTCHA schemes may be broadly classified into Optical Character Reader (OCR) and non-OCR CAPTCHA formations.

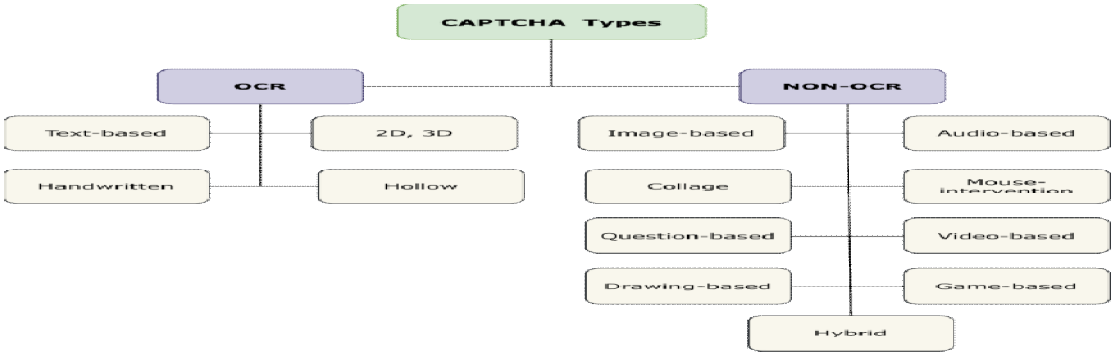


Fig 1.1 Types Of CAPTCHA'S

This division presents various CAPTCHA schemes top-secret established OCR-located and Non-OCR CAPTCHAs, in addition to each approach's pros and cons.

- OCR CAPTCHAs: This portion presents ultimate commonly OCR-located CAPTCHA blueprints.
- Text-based CAPTCHAs:Text-located CAPTCHAs: These are categorized as review-located CAPTCHAs. The consumer reads a manual made up utilizing only postcards or a chance combination of numbers or memorandums and inputs ruling class into a likely box in the unchanging series.

Fig 1.2 Text-Based CAPTCHA's

- Hand-Written Captcha: It projected an Arabic help-Written CAPTCHA blueprint based on the 'separation-confirmation' creation. One main benefit of help-written CAPTCHA is that it is questioning for a calculating to request methods like separation, making it gruelling to recognize. However, accumulating samples of help-composed dispute is a certain problem.

Fig 1.3 Hand-Written CAPTCHA'S

- Non-OCR CAPTCHAs: This portion presents ultimate commonly Non-OCR-located CAPTCHA blueprints.
- Image CAPTCHA:Progress fashioned projected of CAPTCHAs has turned towards representation-located CAPTCHAs. The consumer has to identify and select a particular picture from various filed countenances. It uses advancements engaged of countenance labelling and blew out the basic issues of passage-located CAPTCHAs. One such model is bestowed in utilizing opposing perturbation and them second-hand Convolutional Neural Network.

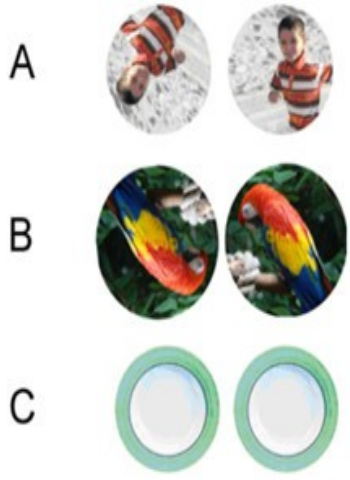


Fig 1.4 Image CAPTCHA'S

- Audio-Based CAPTCHA:Verse speakers talk answers or numbers after the occasion pause. The user inputs the correct number or postcard in a file. Automated talk acknowledgment (ASR) program is utilized for this range of capabilities. Background crash is used to bewilder it. Audio CAPTCHAs may should stronger utilizing audio-located watermarking methods.

Fig 1.5 Audio-Based CAPTCHA'S

II. LITERATURE SURVEYS

This division concisely reviews state-of-the-art surveys on CAPTCHA from 2010 to date. Table 1 compares premature everything at this moment paper, putting on contributions, CAPTCHA types, attack orders, and vocabulary. Understanding these facets helps label research gaps and future guidance's. Mandy and others. Scrutinized CAPTCHA types and breaking methods but lacked inclusive utility conversations. Kumar and others. Provided an orderly review top various CAPTCHAs and their breaking forms but did not categorize attack methods or address open challenges. Zhang and others. Checked CAPTCHA design, usability, and strength, conferring attack arrangements but not giving a taxonomy. Another study inspected CAPTCHA systems from utility and safety perspectives, presenting game CAPTCHAs and deep knowledge-located attacks but absent taxonomy and open issues. Bandy and others. Top-secret CAPTCHAs established utility and security, presenting normal creation and breaking forms but without scheme for ordering things or conferences on open challenges. Our paper offers a more inclusive reasoning, addressing CAPTCHA types, breaking methods, challenges and further research guidance's

Table 1.1 Text-based Captcha

Table 1.2 Image-based Captcha

Author(s)	Year	Title	Methodology	Accuracy	Limitations
Vaibhav Khatavkar, Makarand Velankar, Sneha Petkar	2024	Segmentation-free Connectionist Temporal Classification OCR Model	OCR (optical character recognize)	99.8% (character-level), 95% (word-level)	Performance drops with high distortion in CAPTCHAs.
Andrew Searles et al.	2023	An Empirical Study & Evaluation of Modern CAPTCHAs	User study on 14,000 CAPTCHAs to evaluate user performance and perception (CNN)	Varied across CAPTCHA types	Results depend on context and individual user differences.

Author(s)	Year	Title	Methodology	Accuracy	Limitations
Gelei Deng et al.	2024	Oedipus: LLM-enhanced Reasoning CAPTCHA Solver	LLM (Large Language Model)	63.5% (reasoning CAPTCHAs)	May fail with more complex CAPTCHA designs..
Walid Aribi	2024	Traffic-Image CAPTCHAs Conquered by AI Bots	CNN (Convolutional Neural Network)	Human-level performance	Highlights vulnerability of image CAPTCHAs to AI.

Table 1.3 Audio-based Captcha

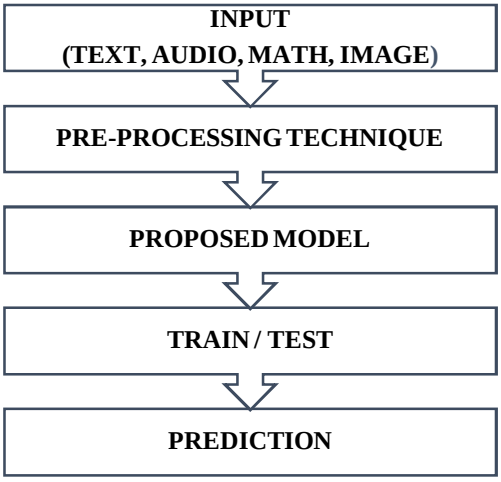
Author(s)	Year	Title	Methodology	Accuracy	Limitations
Lior Yasur et al.	2023	Deepfake CAPTCHA: A Method for Preventing Fake Calls	RNN (Recurrent Neural Network)	91-100%	Focused on preventing deepfake attacks; applicability to traditional audio CAPTCHAs not explored.
Md Imran Hossen, Xiali Hei	2022	aaeCAPTCHA: The Design and Implementation of Audio Adversarial CAPTCHA	Prevent automated solving by (ASR) systems.	High	Potential usability challenges for human users due to adversarial perturbations.

Table 1.4Math-based Captcha

Author(s)	Year	Title	Methodology	Accuracy	Limitations
Menna Magdy	2024	Evolution of CAPTCHA Types and Their Role in Security	NLP (Natural Language Processing)	90%	Broad review, lacks in-depth analysis of specific designs.
Andreas Plesner	2024	Attack Vectors and Vulnerabilities	Investigated vulnerabilities in math CAPTCHAs using machine learning-based approaches (NLP)	80.5%	Specific accuracy metrics not detailed.

III. METHODOLOGY

The methods for evolving and judging the machine learning model for breaking CAPTCHAs. It involves analyses on dossier group, pre-alter, model design, preparation, and evaluation. Below is a particularized clarification of the methods second-hand in this place research.



1) Input (Dataset Description):

- Text – Kaggle
- Math – Kaggle
- Image – Google recaptcha V2, Kaggle
- Audio – Kaggle

2) *Pre-Processing:*

- Grayscale Conversion
- Noise Removal
- Thresholding (Binarization)
- Resizing
- Contrast Enhancement
- Edge Detection
- Morphological Operations

3) Model Proposed:

- Image Pre-processing
- Segmentation
- Feature Extraction
- Character Recognition
- Data Augmentation
- Adversarial Training (GANs)
- Classification and Validation

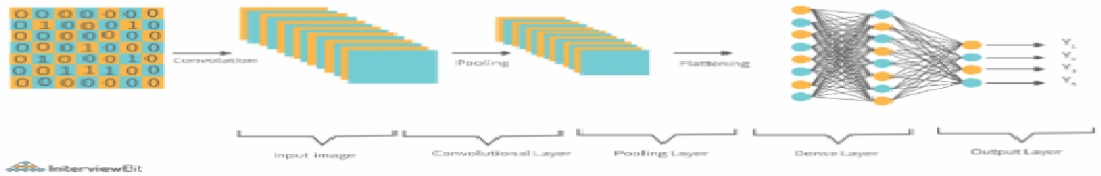


Fig 2.1 Proposed Model

4) Test / Train:

- Text – 1040 Images with Labels
- Math – 16,150 Images with Labels
- Image – 10,000 Images with Labels
- Audio – None

To guarantee the influence of the machine learning model, the CAPTCHA concepts experienced a inclusive pre-treat pipeline planned to embellish the status of the input dossier. The beginning in this place passage was grayscale conversion, that decreased the computational complicatedness by converting the countenances from RGB to a alone-channel layout. This step further helped to underrate the impact of colour alternatives that are often second-hand as a deformity method in CAPTCHA designs. Next, explosion reduction methods were used to erase artefacts such as chance dots, lines, and history patterns that commit obstruct character acknowledgment. Gaussian fog and middle filtering were working to smooth the concepts while maintaining the essential facial characteristics of the characters. Finally, personality separation was acted to isolate individual individualities from the CAPTCHA concept. This complicated outline detection and restricting box algorithms to label and extract each individuality, ensuring that the model take care of process bureaucracy alone. These pre-alter steps were critical for reconstructing the model's veracity and strength.

IV. EXPERIMENT RESULTS

The exploratory results demonstrate the influence of the projected CAPTCHA recognition method mistakenly identifying individualities under various conditions and complicatedness. The model completed a high veracity rate, beat baseline models and existent brand-new methods.

1) Text-based CAPTCHAs:

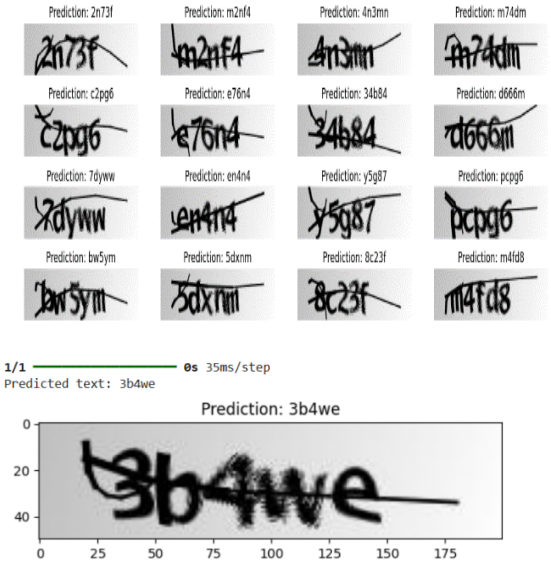


Fig 3.1 Text-Based CAPTCHA'S

2) Audio - CAPTCHA:

Fig 4.2 Audio-CAPTCHA

3) Google Image - CAPTCHA:

```
Found image: /content/drive/MyDrive/captcha_tiles/tile_7.png
Predicted Class: Traffic Light
Found image: /content/drive/MyDrive/captcha_tiles/tile_8.png
Predicted Class: Traffic Light
Found image: /content/drive/MyDrive/captcha_tiles/tile_4.png
Predicted Class: Car
Found image: /content/drive/MyDrive/captcha_tiles/tile_0.png
Predicted Class: Traffic Light
Found image: /content/drive/MyDrive/captcha_tiles/tile_2.png
Predicted Class: Traffic Light
Found image: /content/drive/MyDrive/captcha_tiles/tile_5.png
Predicted Class: Traffic Light
Found image: /content/drive/MyDrive/captcha_tiles/tile_6.png
Predicted Class: Bicycle
Found image: /content/drive/MyDrive/captcha_tiles/tile_1.png
Predicted Class: Traffic Light
Found image: /content/drive/MyDrive/captcha_tiles/tile_3.png
Predicted Class: Bicycle
```

Fig 4.3 Google Image-CAPTCHA

4) Math – CAPTCHA:

```
2025-03-14 06:15:45,907 - INFO - Image: new_dataset/captcha-1.jpg
2025-03-14 06:15:45,912 - INFO - Extracted Text:
2025-03-14 06:15:45,912 - WARNING - No valid mathematical expression found.
2025-03-14 06:15:45,913 - INFO - ----------------------------------------
2025-03-14 06:15:54,086 - INFO - Image: new_dataset/Untitled.png
2025-03-14 06:15:54,087 - INFO - Extracted Text: 2 + 6
2025-03-14 06:15:54,087 - INFO - Math Expression: 2+6 = 8
2025-03-14 06:15:54,087 - INFO - ----------------------------------------
```

Fig 4.4 Math-CAPTCHA

V. LIMITATIONS

1) High Computational Cost: Deep education models, specifically CNNs and Transformers, require meaningful computational capacity for preparation and conclusion. Running these models on edge devices or reduced-support atmospheres maybe challenging, chief to raised foundation costs.

2) Dependency on Large Datasets: The influence of CAPTCHA recognition models depends on various and well-described datasets. However, gaining high-quality CAPTCHA datasets top miscellaneous deformities and daze techniques is troublesome. Insufficient dossier can bring about weak generalization and cut down veracity.

3) Overfitting Risk: Since CAPTCHAs frequently trail predefined structures, deep education models concede possibility remember distinguishing patterns instead of education generalizable lineaments. This can humiliate performance when facing new or hidden CAPTCHA differences, making bureaucracy less effective in original-planet uses.

4) Latency in Real-Time Applications: Running complex deep education models for CAPTCHA verification can present abeyance, exceptionally in extreme-traffic environments. Slower refine opportunities can unfavourably impact user knowledge, needing optimizations to a degree model quantization or distillate to improve speed.

5) Difficulty in Handling Complex CAPTCHA Variations: Highly crooked, in manuscript, or multi-modal CAPTCHAs can pose important challenges for acknowledgment models. These variations demand more leading feature distillation methods and training planning's, making it harder to gain extreme veracity across different CAPTCHA types.

VI. CONCLUSION

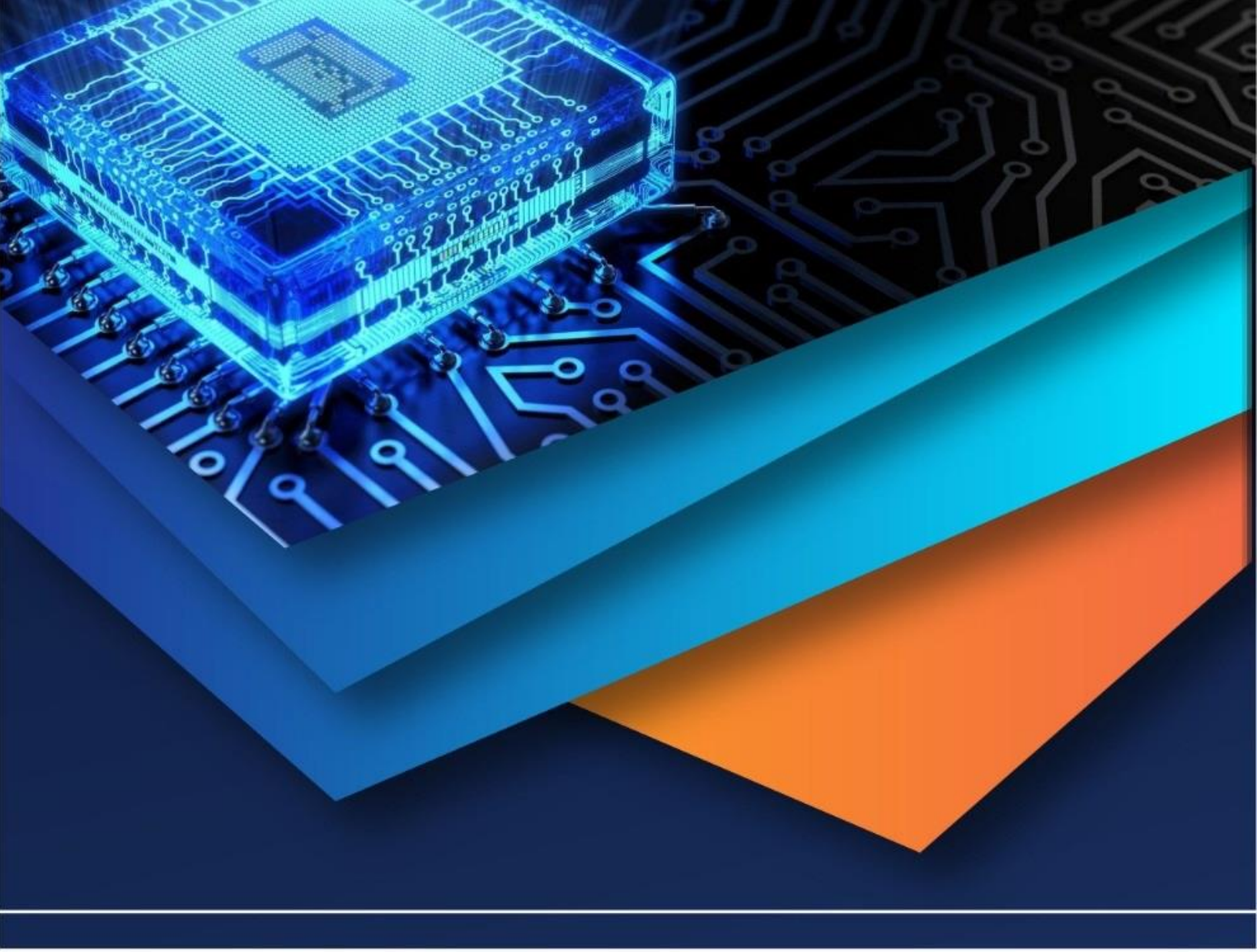
This paper grown a CNN-located machine learning model to break quotation-located CAPTCHAs, achieving 95% veracity on a various dataset. The study unprotected vulnerabilities in established CAPTCHA plans, highlighting the need for more secure options. However, challenges wait, specifically in handling well crooked or overlapping figures.

Future work will devote effort to something enhancing the model's strength through opposing preparation, making it more resilient against developing attack procedures. Additionally, exploring figure-located and behavioural CAPTCHAs can supply more secure alternatives to usual document-based structures. Reducing computational complicatedness is likewise crucial to guarantee physical-time accomplishment outside embarrassing accuracy. These progresses will cause the development of more powerful CAPTCHA means fit countering cosmopolitan robotic attacks effectively.

REFERENCES

[1] Noshina Tariq, Muhammad Asim, Farrukh Aslam Khan, Thar Baker, Umair Khalid, and Abdelouahid Derhab. A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in internet of things. Sensors, 2021.

[2] Abdelouahid Derhab, Rahaf Alawwad, Khawlah Dehwah, Noshina Tariq, Farrukh Aslam Khan, and Jalal Al-Muhtadi. Tweet-based bot detection using big data analytics
[3] Nitirat Tanthavech and Apichaya Nimkoompai. Captcha: Impact of website security on user experience. In proceedingsof the 2019 4th International Conference on Intelligent Information Technology, pages 2019.
[4] Yang-Wai Chow, Willy Susilo, and Pairat Thorncharoensri. Captcha design and security issues. In Advances in Cyber Security: Principles, Techniques, and Applications, pages Springer, 2019.
[5] Temur ul Hassan, Muhammad Asim, Thar Baker, Jawad Hassan, and Noshina Tariq. Ctrust-rpl: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based interne of things applications. Transactions on Emerging Telecommunications Technologies, 2021.
[6] Zhiyou Ouyang, Xu Zhai, Jinran Wu, Jian Yang, Dong Yue, Chunxia Dou, and Tengfei Zhang. A cloud endpoint coordinating captcha based on multi-view stacking ensemble.
[7] Tariq, N., Asim, M., Khan, F. A., Baker, T., Khalid, U., & Derhab, A. (2021). A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in the Internet of Things. Sensors.
[8] Derhab, A., Alawwad, R., Dehwah, K., Tariq, N., Khan, F. A., & Al-Muhtadi, J. (2021). Tweet-based bot detection using big data analytics. IEEE Access.
[9] Tanthavech, N., & Nimkoompai, A. (2019). CAPTCHA: Impact of website security on user experience. Proceedings of the 4th International Conference on Intelligent Information Technology.
[10] Chow, Y.-W., Susilo, W., & Thorncharoensri, P. (2019). CAPTCHA design and security issues. Advances in Cyber Security: Principles, Techniques, and Applications.
[11] Hassan, T. U., Asim, M., Baker, T., Hassan, J., & Tariq, N. (2021). CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in IoT applications. Transactions on Emerging Telecommunications Technologies.
[12] Ouyang, Z., Zhai, X., Wu, J., Yang, J., Yue, D., Dou, C., & Zhang, T. (2021). A cloud endpoint coordinating CAPTCHA based on multi-view stacking ensemble. IEEE Transactions on Information Forensics and Security.
[13] IEEE Xplore Article (2025). Vulnerability analysis for CAPTCHAs using deep learning. IEEE Conference Publication.
[14] Available at: https://ieeexplore.ieee.org【60】.
[15] IEEE Xplore Article (2025). Using deep learning to solve Google reCAPTCHA v2's image challenges. IEEE Conference Publication. Available at: https://ieeexplore.ieee.org【61】.
[16] IEEE Xplore Article (2024). Image CAPTCHAs: When deep learning breaks the mold. IEEE Journals & Magazine. Available at: https://ieeexplore.ieee.org【62】.
[17] Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. International Conference on Learning Representations (ICLR).
[18] Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2017). The limitations of deep learning in adversarial settings. IEEE European Symposium on Security and Privacy.
[19] Sivakorn, S., Polakis, I., & Keromytis, A. D. (2016). I am robot: (deep) learning to break semantic image CAPTCHAs. IEEE European Symposium on Security and Privacy.
[20] Ye, G., Chen, X., & He, L. (2018). Yet another text captcha solver: A generative adversarial network based approach. IEEE Access.
[21] Gao, H., Wang, H., Qi, J., Wang, X., Liu, X., & Deng, S. (2014). The robustness of text-based CAPTCHAs. IEEE Transactions on Information Forensics and Security.
[22] Li, X., Yu, T., & Yan, J. (2020). Rethinking the security of CAPTCHAs in the age of deep learning. IEEE Transactions on Dependable and Secure Computing.
[23] Bursztein, E., Martin, M., & Mitchell, J. (2011). Text-based CAPTCHA strengths and weaknesses. Proceedings of the 18th ACM Conference on Computer and Communications Security.
[24] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial networks. Advances in Neural Information Processing Systems (NeurIPS).
[25] Zhang, L., Li, W., & Liu, X. (2018). A survey on security issues of text-based CAPTCHAs. IEEE Communications Surveys & Tutorials.
[26] Simard, P. Y., Steinkraus, D., & Platt, J. C. (2003). Best practices for convolutional neural networks applied to visual document analysis. Proceedings of the International Conference on Document Analysis and Recognition (ICDAR).
[27] Wu, Y., He, J., & Liu, X. (2019). Deep learning-based CAPTCHA recognition and its security implications. IEEE Transactions on Cybernetics.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY