Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Forensics AI: Next-Gen Digital Forensics with AI

KVemuri Chandana, Dudekula Abdul Salam, Adoni Althaf, Komme Kavya Sree, Degalpadu Afrid

Department of Computer Science and Engineering, Gates Institute of Technology, Andhra Pradesh, India.

Abstract

Crime Scene Investigation (CSI) has become increasingly challenging due to the massive growth of digital evidence across devices, cloud platforms, and online activities. Traditional digital forensic methods are slow, manually intensive, and prone to human error, making them ineffective for handling large and complex datasets. The proposed system introduces an AI-integrated digital forensic framework that applies Machine Learning, Deep Learning, Natural Language Processing (NLP), and Computer Vision to automate key forensic tasks. These include anomaly detection in log files, rapid text classification, and object or scene identification in images and videos. The framework follows a human-in-the-loop model, ensuring AI handles data processing while experts make final decisions, maintaining accuracy and legal admissibility. By integrating Machine Learning, Deep Learning, NLP, and Computer Vision, the system helps investigators identify patterns, anomalies, and critical evidence quickly.

Correspondence

Vemuri Chandana

Department of Computer Science and Engineering, Gates Institute of Technology, Andhra Pradesh, India.

- Received Date: 11 Feb 2026
- Accepted Date: 02 Apr 2026
- Publication Date: 25 Apr 2026

Keywords

Artificial Intelligence, Crime Scene Investigation, Digital Forensics, Legal Admissibility, Machine Learning, Metadata Analysis

Introduction

Traditional methods of handling crime scenes involve meticulous identification, collection, and analysis of evidence. These methods are often time-consuming, labor-intensive, and physically demanding.

However, the adoption of digital forensics has transformed these processes by introducing new techniques that improve the retrieval of evidence from electronic devices and digital trails. Among these advancements, Artificial Intelligence (AI) stands out as a revolutionary force reshaping crime scene investigations.

AI enhances digital forensic investigations by enabling efficient and accurate analysis of large datasets. Traditional methods often fail to keep up with the increasing volume of digital evidence from smartphones, computers, cloud storage, and social media platforms. Machine learning algorithms and neural networks help process this data, identify patterns, and derive insights that might otherwise go unnoticed.

Automation is another major advantage of AI in digital forensics. Tasks that once required hours of manual work can now be completed quickly, allowing forensic experts to focus on complex analytical tasks. For example, AI can extract metadata such as authorship, timestamps, and modification history from digital files, which is crucial in investigations.

AI also improves the reliability of forensic findings by minimizing human errors caused by bias, fatigue, or oversight. It applies consistent parameters across cases and can validate findings using historical data and crime patterns.

Additionally, predictive analytics enables investigators to anticipate potential crimes by analyzing trends in large datasets. AI-driven image and video analysis techniques, such as facial recognition and object detection, further enhance the ability to extract meaningful insights from multimedia evidence.

Despite its advantages, AI raises ethical and legal concerns, including privacy issues and algorithmic bias. Furthermore, the admissibility of AI-generated evidence in court remains a challenge, requiring clear standards and regulatory frameworks. Continuous training and collaboration among technologists, legal experts, and forensic professionals are essential for the effective adoption of AI in this field.

Related Work

This study explores the role of digital forensics and the importance of machine learning techniques in analyzing large volumes of data. Various models are evaluated for processing digital evidence such as emails, chat logs, and files.

The research also focuses on integrating data from multiple sources, including mobile devices, personal computers, and cloud storage. Automation is highlighted as a key factor in improving efficiency and reducing manual effort.

Special attention is given to multimedia analysis using AI, including facial recognition, object detection, and video analysis. The study also discusses challenges such as image manipulation and the need for high-quality training datasets.

Ethical concerns, including privacy and algorithmic bias, are examined alongside legal

Citation: Vemuri C, Dudekula AS, Adoni A, Komme KS, Degalpadu A. Forensics AI: Next-Gen Digital Forensics with AI. GJEIIR. 2026;6(4):231.

challenges related to the admissibility of AI-generated evidence. The importance of transparency, reliability, and reproducibility in AI systems is emphasized.

The paper also explores predictive modeling techniques for crime forecasting and highlights the role of metadata analysis in understanding digital evidence.

Proposed System

The initial process is to acquire electronic data from computer systems, mobile devices, the cloud, and social media. It is, therefore, usually big and unstructured, hence it demands anxious preprocessing. It simply involves bio- cleaning the data by cancelling the noisy input and reformatting it in order for it to fit the correct layout for analysis. It is also important to perform activities that will make the data set cleaned ,tidy, and ready for analysis which include data normalization, deduplication, and noise reduction activities.

In this regard, feature selection is important in redefining the raw data into meaningful features that A. I models can work on. Extracting features from the digital evidence that may include time stamp, I. P address, activities that have been carried out and other meta-data. Attribute discretization takes these characteristics further and settles on choosing only those most relevant in the study. It is very important for the enhancement of the existing algorithm, make better and exact models of Artificial Intelligence, decrease computational load and concentrate on important evidence.Indeed which, by having a clean and clearly defined dataset, many machine learning algorithms can be applied. Classification and regression are two types of supervised learning models where the institution creates learning algorithms and predictive models from large initial datasets by learning from sample labels. Other forms of machine learning are clustering ,where it forms groups of similar data and anomaly detection where the system is able to identify unusual data patterns, all done without prior knowledge of the data set. The use of a certain algorithm depends on the circumstantial proposed the investigation and kind of Digital evidence available as shown in Fig 1.

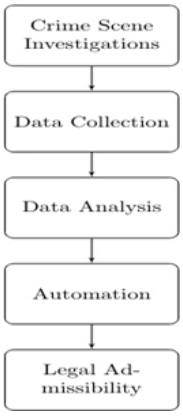

Fig1.Proposed Methodology Architecture

AI is very beneficial to digital forensics since it can help in cutting down the amount of work needed to be done by handler son regular tasks .Automatic tools as per. It can also involve other recurrent processes like keyword search, recognition of meta data, creation of reports and so on. The use of the automated work in the area of forensic leads to bringing more focus and concentration of the expert in the analytical and decision-making tasks, which in turn leads to the enhancement of efficiency and accuracy of the field work.

The capabilities of AI to use superior mathematics to understand the data collected as evidence. Criminal pattern recognition can therefore be achieved by use of Predictive modeling approaches after analyzing the accumulated data and coming up with empirically forged patterns that may be useful in determining likely future criminal activities. For instance, using the proactive approach, predictive models that may anticipate possible cyber-attacks or people most likely to commit crimes can be developed. Such information can be of great use to police departments and other related authorities in order to find ways of preventing the occurrence of more crimes and making the society more secure. LA solutions involving deep learning and neural networks are particularly useful to process multimedia evidence. Some of the key examples of features that can be extracted from images and videos include those as facial recognition, object detection, and scene reconstruction which can provide vital information that might be overlooked by an analyst. This is especially required in forensic applications of the technology as in cases were surveillance videos or pictures are used, AI has the ability to quickly recognize and track down culprits, analyze the footage for key points of interest, as well as have near perfect accuracy in recreating the crime scene. Text in form of EMAILS, CHAT logs Conversations and any other SOCIAL MEDIA POSTS formulate the input data on which NLP techniques are applied to. Use of the AI-based NLP tools can also parse the text and find key phrases, sentiment, and relationships between people, which is quite helpful when analyze behavior and intentions of others. These tools can also decode concealed messages or any messages that are encrypted and these are matters of great use in criminal activities. Despite the benefits of using AI in digital forensic processes, guidelines like ethical and legal ones should be followed. These include measures that assure the protection of individuals' privacy and their freedoms while using AI, the safety of data collected so as not to influence certain results while using AI and the elimination of bias in the same. Stakeholders within the legal profession should work toward making AI as transparent and replicable as possible to ensure that judiciaries accept the AI-produced evidence as valid or allow the principles of due process to prevail.

As technologies advance and forensic sciences expand, artificial intelligence and digital forensics are two contemporary disciplines. It indicates that forensic professionals have to embark on continuing professional development schemes and updates with the latest innovations of artificial intelligence. Periodic revision and seminars should be held to make sure that the forensic staff is fully trained on the use of Artificial Intelligence alongside ensuring that it is in touch with developments in the field. Applying AI innovations in the field of digital forensics is only possible through synergistic approaches involving technology specialists, forensic professionals, lawyers, and legislators. This allows for a focus on both the technical and legal aspects relevant to forensic investigations while having AI developed and designed in a meaningful way. The key finding for the current research is that through the use of consultations and capable partnerships, it is possible to establish strong structures that promote the use of AI while minimizing useful risks.

In this regard, the following has been identified as an optimal solution for the integration of AI in the digital forensic processes: A diverse and comprehensive dataset should be gathered from multiple sources in a variety of organizations. The data or the samples gathered for this study includes electronic evidence extracted from computers, mobile devices, cloud storage, and

social media. The data in this set a real so diverse in their formats and content and may include text files, emails and chat, pictures ,videos, as well as metadata. The datasets that are freely available to the public must also be used to train and validate AI systems such as, the Enron Email Dataset, and the Million Image Dataset. Further, for the practical purposes of real-world employed models, data sets from the cases of ongoing investigations, which have been anonymized to ensure privacy of the involved parties, are used. This large and varied data base helps to make sure that the AI algorithms have been trained on a broad spectrum of frequencies, thus being effective in real world forensic work as shown in fig 2.

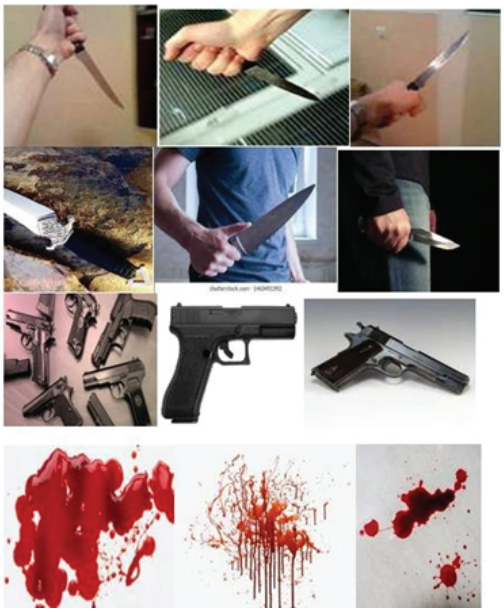

Fig 2.Crime Scene Dataset

The tools applied in the course of the study to analyze the data, learn from the data, and perform digital forensics are open source and commercial .Deep learning libraries ranging from TensorFlow and Torch to Py torch are employed in the development and training of the models. These frameworks include respective giant hefty libraries for ensemble of Neural networks, Deep learning and other facts of Machine learning respectively. In digital forensics, there are applications which are used in data investigation, data recovery, and data evidence including the Autopsy and the Sleuth Kit. Besides, the rare specific programs, for instance, FTK (Forensic Toolkit) and EnCase which are intended for hard and deep forensic, including abilities to work with the recovered data and search for new data. Text analysis is done through Natural Language Processing (NLP) tools that include NLTK and spaCy that are deposited in the project whereas OpenCV is developed for image and video manipulation. This integration of application guarantees durability, optimal performance ,and integrality in the fusion of AI in the digital forensic context.

Task	Traditional Method Time(hours)	AI-Enhanced Method Time(hours)	Improvement(%)
Meta data Extraction	10	2	80%
Keyword Search	15	1	93%
Image Analysis	20	5	75%
Video Analysis	30	8	73%

Results

The new techniques table 1 embrace the use of artificial intelligence and come with the added advantage of improving the duration involved in performing several essential forensic activities. For instance, a project aimed at extractingmetada tarecordeda80%enhancementwhilethe keyword search had 93% enhancement. These reductions demonstrate significant AI possibilities as a tool for enhancing the efficacy of digital forensic determinations as shown in fig 3.

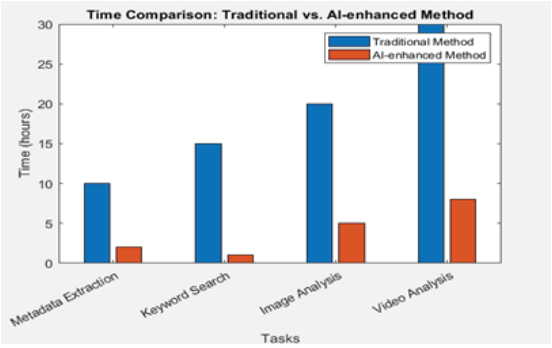

Fig 3. Comparison of Efficiency

ACCURACY ENHANCEMENT

Task	Traditional Method Accuracy(%)	AI- Enhanced Method Accuracy(%)	Improvement(%)
Metadata Analysis	85	95	12%
Keyword Detection	78	92	18%
Facial Recognition	70	88	26%
Object Detection in Videos	65	90	38%

The use of superior Table 2 AI enhanced methods presents improved similarities in accuracy in completed forensic tasks. For instance, the identification accuracy of faces was made better by 26% while the detection of objects in videos got better by 38%. These addendums bear the importance which AI technologies offer towards reliability and precision in digital forensic services as shown in fig 4.

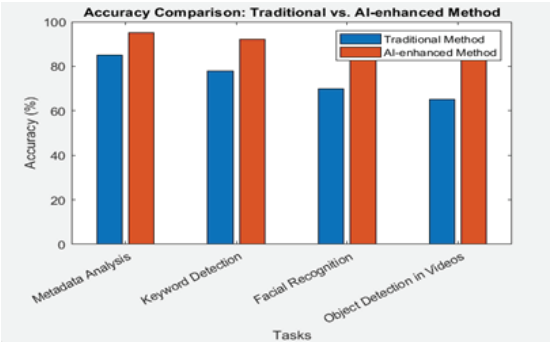

Fig 3. Accuracy Comparison

Task	Manual Effort(hours)	Automated Effort(hours)	Reduction(%)
Data Preprocessing	12	3	75%
Feature Extraction	10	2	80%
Report Generation	8	1	88%
Anomaly Detection	14	4	71%

It is obvious table 3 that automation has contributed to a substantial decrease in the amount of work that is manually done in the forensic field for various tasks. For instance, report generation saw a decrease in the manual effort required for the task by 88% while feature extraction recorded a manual effort reduction by 80%. This is a clear indication that the incorporation of AI can go a long way in the FP by dispensing routine tasks to enable forensic experts to attend to more complicated issues fig 5.

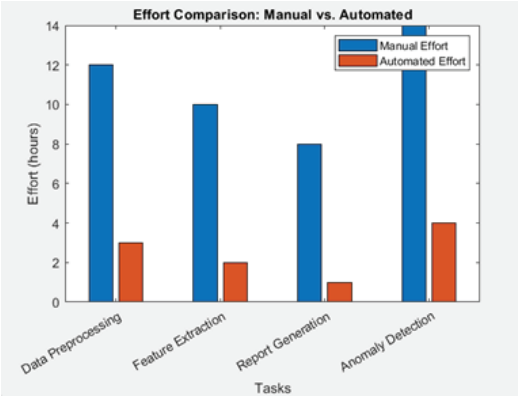

Fig5.Comparison of Effort

LEGAL ADMISSIBILITY OF AI-GENERATED EVIDENCE

Evidence Type	Traditional Method	Automated Effort(hours)	Reduc-tion(%)
Admissibility(%)	AI-Enhanced Method	3	75%
Admissibility(%)	Improve-ment(%)	2	80%
Textual Evidence(Emails, Logs)	90	95	5%
Multimedia Evi-dence	14	4	71%
(Images, Videos)	85	92	8%
Metadata Analysis	80	88	10%
Predictive Analytics	70	85	21%

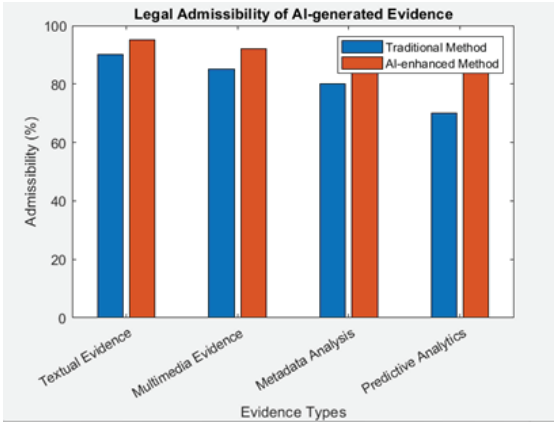

Fig6.Comparison of legal Admissibility of AI-Generated Evidence

The discussed table 4 AI-enhanced methods prove that they are effective in increasing legal admissible presence of evidence. For example, the assessment of multimedia evidence was enhanced by 8% and the analytics prediction was enhanced by 21%. Based on these findings, it can be therefore concluded that apart from improving the analytical approach to AI technologies, the support for legal legitimacy of forensic information is also ascertainable as shown in fig 6.

Conclusion And Future Work

AI is transforming traditional forensic practices by making them faster, more reliable, and scalable. Its integration enhances both investigative outcomes and legal credibility in modern crime analysis. Address ethical and legal challenges such as data privacy, bias-free algorithms, and responsible AI use in evidence analysis. Expand research in advanced analytics and collaborative efforts to develop AI systems that can proactively detect and prevent crimes.

- **Real-Time Forensic Analysis** – Extend the system to analyze live data from IoT devices, cloud platforms, and social media for faster crime detection and response.
- **Explainable AI Integration** – Implement Explainable AI (XAI) to make AI decisions transparent and legally acceptable in court proceedings.
- **Blockchain for Evidence Security** – Use blockchain technology to ensure secure storage, integrity, and proper chain of custody of digital evidence.
- **Adaptive & Scalable Models –** Develop self-learning AI models that continuously adapt to new cybercrime patterns and support multiple platforms and languages.

References

1. J. Suarez-Paez et al., "A novel low processing time system for criminal activities detection applied to command and control citizen security centers," Inf., vol. 10, no. 12, 2019, doi: 10.3390/info10120365.
2. S. Jang, L. Battulga, and A. Nasridinov, "Detection of Dangerous Situations using Deep Learning Model with Relational Inference," J. Multimed. Inf. Syst., vol. 7, no. 3, pp. 205–214, 2020, doi: 10.33851/jmis.2020.7.3.205.
3. T. J. Nandhini and K. Thinakaran, "Optimizing Forensic Investigation and Security Surveillance with Deep Reinforcement Learning Techniques," 2023 Int. Conf. Data Sci. Agents Artif. Intell., pp. 1–5, 10.1109/ICDSAAI59313.2023.10452551. 2023, doi:
4. K. V Shivthare, P. D. Bhujbal, A. P. Darekar, and Y. N. N, "Suspicious Activity Detection Network for Video Surveillance Using Machine Learning," vol. 6, no. 4, pp. 2456–0774, 2021.
5. K. Thinakaran, "Visual HOG-Enabled Deep ResiNet for Crime Scene Object Detection," 2023.
6. D. S. Devishree, K. M. Divakar, K. A. Ashini, A. S. Bhardwaj, and S. M. Younis, "Crime scene prediction and analysing its accuracy with frames using deep neural network," vol. 5, no. 2, pp. 860–867, 2019.
7. Y. Wu, X. Dong, G. Shi, X. Zhang, and C. Chen, "Crime Scene Shoeprint Image Retrieval: A Review," Electron., vol. 11, no. 16, pp. 1–15, 2022, doi: 10.3390/electronics11162487.
8. P. Li, L. Prieto, D. Mery, and P. J. Flynn, "On Low-Resolution Face Recognition in the Wild: Comparisons and New Techniques," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 8, pp. 2000–2012, 2019, doi: 10.1109/TIFS.2018.2890812.
9. D. Devasenapathy, M. Raja, R. K. Dwibedi, N. Vinoth, T. Jayasudha, and V. D. Ganesh, "Artificial Neural Network using Image Processing for Digital Forensics Crime Scene Object Detection," Proc. 2nd Int. Conf. Edge Comput. Appl. ICECAA 2023, no. Icecaa, pp. 652–656, 10.1109/ICECAA58104.2023.10212302.
10. A. Rizwanbasha, "Real Time Object Detection Based on RCNN Technique," 2023 3rd International Conference On Pervasive

Computing And Social Networking (ICPCSN),,Doi: 10.1109/Icpcsn58827.2023.00121
11. V. Rekha and K. Natarajan, “Foreground algorithms for detection and extraction of an object in multimedia,” Int. J. Electr. Comput.
12. Eng., vol. 10, no. 2, pp. 1849–1858, 2020, doi: 10.11591/ijece.v10i2.pp1849-1858. R. R. A. Hussein, S. M. Al-Qaraawi, and M. S. Croock, “Viterbi optimization for crime detection and identification,” Telkomnika (Telecommunication Comput. Electron. Control., vol. 18, no. 5, pp. 2378–2384, 10.12928/TELKOMNIKA.V18I5.13398.
13. G. Uganya, F. D. Shadrach, I. Sudha, P. M. Krishnammal, V. Lakshmanan, and T. J. Nandhini, “Crime Scene Object Detection from Surveillance Video by using Tiny YOLO Algorithm,” 2023 3rd Int. Conf. Pervasive Comput. Soc. Netw., no. October, pp. 654–659, 2023, doi: 10.1109/ICPCSN58827.2023.00114.
14. D. V. Ganesh and R. M. Bommi, “Neural Network based Predictive Analysis of Surface Roughness using Bayesian Regularization in Turning of Monel K500,” 6th Int. Conf. Inven. Comput. Technol. ICICT 2023 - Proc., no. Icict, pp. 448–452, 2023, doi: 10.1109/ICICT57646.2023.10134220.
15. A. Rizwanbasha, “Simultaneous Simulation Study of Metal Product Design Based on Machine Learning Algorithm,” 2023 2nd Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2023, pp. 705–709,2023,doi:10.1109/SmartTechCon57526.2023.10391630
16. Nagesh, C., Chaganti, K.R. , Chaganti, S. , Khaleelullah, S., Naresh, P. and Hussan, M. 2023. Leveraging Machine Learning based Ensemble Time Series Prediction Model for Rainfall Using SVM, KNN and Advanced ARIMA+ E-GARCH. International Journal on Recent and Innovation Trends in Computing and Communication. 11, 7s (Jul. 2023), 353–358. DOI:https://doi.org/10.17762/ijritcc.v11i7s.7010.
17. S. Khaleelullah, P. Marry, P. Naresh, P. Srilatha, G. Sirisha and C. Nagesh, "A Framework for Design and Development of Message sharing using Open-Source Software," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 639-646, doi:10.1109/ICSCDS56580.2023.10104679.
18. Ramesh Kumar Ramaswamy, Pannangi Naresh, Chilamakuru Nagesh, Santhosh Kumar Balan, Multilevel thresholding technique with Archery Gold Rush Optimization and PCNN-based childhood medulloblastoma classification using microscopic images, Biomedical Signal Processing and Control, Volume 107, 2025,107801, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2025.107801.
19. K. R. Chaganti, B. N. Kumar, P. K. Gutta, S. L. Reddy Elicherla, C. Nagesh and K. Raghavendar,"Blockchain Anchored Federated Learning and Tokenized Traceability for Sustainable Food Supply Chains," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1532-1538, doi: 10.1109/ICUIS64676.2024.10866271.
20. Mohammed Inayathulla and Karthikeyan C, “Image Caption Generation using Deep Learning For Video Summarization Applications” International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http:// dx.doi.org/10.14569/IJACSA.2024.0150155.
21. Mohammed, I., Chalichalamala, S. (2015). TERA: A Test Effort Reduction Approach by Using Fault Prediction Models. In: Satapathy, S., Govardhan, A., Raju, K., Mandal, J. (eds) Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1. Advances in Intelligent Systems and Computing, vol 337. Springer, Cham. https://doi. org/10.1007/978-3-319-13728-5_25
22. Inayathulla, M., Karthikeyan, C. (2022). Supervised Deep Learning Approach for Generating Dynamic Summary of the Video. In: Suma, V., Baig, Z., Kolandapalayam Shanmugam, S., Lorenz, P. (eds) Inventive Systems and Control. Lecture Notes in Networks and Systems, vol 436. Springer, Singapore. https://doi.org/10.1007/978-981-19- 1012-8_18.
23. Mohammed and C. Karthikeyan, “Object detection in video summarization for video surveillance applications,” Yugoslav Journal of Operations Research, vol. 35, no. 3, pp. 523–546, 2025. doi:10.2298/YJOR240615010I.
24. Inayathulla Mohammed and K. R. Rao, “Enhancing real-time violence detection in video surveillance using hybrid deep learning model,” Journal of Web and User Applications, vol. 16, no. 1, 2025. doi:10.58346/JOWUA.2025.I1.021.
25. G. Raju, K. Sushmitha, M. Priyanka, E. Sai Leela, M. Vani Chowdary, and A. Yashwantha, “Real Time Hand Gesture Recognition Using CNN,” Global Journal of Engineering Innovations & Interdisciplinary Research (GJEIIR), vol. 5, no. 2, 2025, doi: 10.33425/3066-1226.1101.
26. G. Raju, K. Sattar Hadiya, K. Penna Obulesu, M. P. Pavan Raj, and M. Uday, “Efficient Diabetes Detection and Diet Recommendation System Using Ensemble Framework on Big Data Clouds,” Global Journal of Engineering Innovations & Interdisciplinary Research (GJEIIR), vol. 5, no. 2, 2025, doi: 10.33425/3066-1226.1108.
27. G. Raju, L. R. Buchupalli, A. Thudimela, K. Kodikondla, K. Palaku, and D. Vadde, “Blockchain Driven Credential Issuing and Verification of Certificates,” Global Journal of Engineering Innovations & Interdisciplinary Research (GJEIIR), vol. 5, no. 2, 2025, doi: 10.33425/3066-1226.1083.