International Journal of
Computational Learning & Intelligence
Vol. 04 | Issue 01 | 2025

RESEARCH ARTICLE OPEN ACCESS

Forgery Detection in Digital Media using Neural Networks

G Anvesh Reddy . G Srikanth Reddy . C Sree Rama Raju . D Padmaja . J Sreenivasulu

Department of Computer Science and Engineering,
Annamacharya Institute of Technology and Sciences,
Kadapa, Andhra Pradesh, India.

DOI: **10.5281/zenodo.15163295**
Received: 27 January 2025 / Revised: 21 February 2025 / Accepted: 27 March 2025

Abstract – The widespread availability of digital image editing tools has led to an increase in manipulated media, making advanced forgery detection techniques essential. This project presents a robust approach to identifying forged images by utilizing Python and a Convolutional Neural Network (CNN). The CNN acts as the core of the detection system, achieving remarkable accuracy with a training performance of 98% and a validation accuracy of 92%. These results demonstrate the model's ability to effectively differentiate between authentic and tampered images. For this study, a dataset comprising 12,615 images was used, including 7,492 genuine images and 5,123 altered ones. This diverse dataset ensures a comprehensive assessment of the model's performance. To improve detection accuracy, the system integrates Error Level Analysis (ELA) as a preprocessing technique. Each image is resized to a standardized resolution of 256x256 pixels before applying ELA, which helps reveal inconsistencies in compression artifacts. Ideally, unedited images should display uniform compression, whereas discrepancies in compression levels may suggest potential alterations. The processed images are converted into NumPy arrays for further analysis. By integrating deep learning with CNNs and leveraging the subtle variations identified through ELA, the proposed system not only achieves high detection accuracy but also pinpoints areas within an image that may have been manipulated. Implemented using Python and a structured CNN framework, this project significantly enhances digital media forgery detection, with promising applications in fields requiring image authenticity verification.

Index Terms – Digital image forgery detection, Convolutional Neural Network, Image authentication, MobileNetV2, Authentic images, Tampered images.

I. INTRODUCTION

With the widespread availability of advanced editing tools, the manipulation of digital images has become a growing concern. Altered images are often used to spread misinformation, making it difficult to verify their authenticity. Social media platforms have accelerated the dissemination of such content, increasing the risk of misleading visual information. Sophisticated editing software like Adobe Photoshop, GNU, and GIMP enables users to create highly realistic forgeries that are nearly undetectable by the human eye. As a result, ensuring image integrity has become essential in various fields, including forensic investigations, journalism, legal proceedings, and medical diagnostics, where accuracy and trustworthiness are paramount.

Conventional forgery detection methods, such as manual inspection and metadata analysis, have limitations in identifying advanced tampering techniques. Recently, computational approaches like Error Level Analysis (ELA) have gained attention due to their effectiveness in identifying inconsistencies within an image. ELA evaluates variations in compression levels, revealing regions that may have been manipulated. As a passive detection technique, ELA does not require an original reference image, making it highly suitable for real-world applications. Image forgeries generally fall into three primary categories: copy-move forgery, image splicing, and image retouching. In copy-move forgery, a section of an image is duplicated and placed elsewhere within the same image, making detection difficult due to identical pixel properties. Image splicing, on the other hand, involves merging components from multiple images to create a new, manipulated version. This type of forgery often includes alterations in lighting, texture, and color balance to maintain visual consistency. Image retouching is a more subtle manipulation technique, where certain features of an image are modified—such as adjusting brightness, contrast, or background details—to enhance or conceal specific information. Detecting these types of tampering requires advanced analytical models capable of identifying minute inconsistencies.

To improve detection capabilities, this study proposes a hybrid approach combining Error Level Analysis with deep learning-based classification using MobileNetV2. Initially, ELA is applied to identify compression inconsistencies and highlight potential forgery regions. The processed images are then analyzed using MobileNetV2, a lightweight convolutional neural network known for its efficiency in feature extraction and image classification. MobileNetV2 is particularly advantageous due to its ability to achieve high accuracy while operating in resource-constrained environments. The model is evaluated using the CASIAV2 dataset, which includes a diverse collection of forged images, such as those involving splicing and copy-move techniques across various formats and resolutions.

The objective of the study is to:

1. Develop an image forgery detection system by integrating Error Level Analysis with MobileNetV2.
2. Assess the impact of ELA as a preprocessing step for deep learning-based forgery detection.
3. Enhance accuracy and computational efficiency for passive image forgery detection in practical applications.

Section II reviews existing literature on forgery prediction and digital media images with deep learning techniques. Section III describes the methodology used, including data collection, preprocessing, and model development. Section IV presents the results and analysis, highlighting the model's prediction accuracy. Section V discusses the findings, their implications, and future research directions. Finally, Section VI concludes the study by summarizing the contributions and potential applications of Forgery detection in digital media.

II. LITERATURE SURVEY

Ensuring the authenticity of digital images is crucial in preventing fraudulent manipulations across various fields such as journalism, forensics, and social media. Image forgery detection methods aim to identify alterations in digital media using image processing, machine learning, and deep learning techniques. This study explores the application of MobileNetV2 and Error Level Analysis (ELA) in combination with Convolutional Neural Networks (CNNs) for identifying forged images. Machine learning techniques are widely applied to detect forged images by analyzing attributes such as texture, colour, and statistical variations. Feature extraction techniques like Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG) help in identifying inconsistencies within images. Traditional classifiers such as Support Vector Machines (SVM), Random Forest, and Decision Trees process these extracted features to differentiate between authentic and altered images. However, these conventional approaches often struggle to detect complex and advanced forgeries, making deep learning models a more effective solution.

Deep learning, particularly CNNs, plays a significant role in improving forgery detection by learning intricate spatial patterns. CNNs efficiently highlight manipulated regions, while ELA assists in identifying inconsistencies in compression artifacts, which serve as indicators of image tampering. MobileNetV2, a lightweight yet efficient neural network architecture, enhances detection performance by achieving high accuracy with reduced computational demands. Its depthwise separable convolutions allow for faster processing, making it well-suited for real-time detection applications. To assess the effectiveness of forgery detection methods, datasets such as CASIA v2 provide a diverse collection of authentic and manipulated images, allowing models to be trained and evaluated comprehensively. The performance of detection models is typically measured using evaluation metrics such as accuracy, precision, recall, and F1-score. The combination of ELA preprocessing and CNN-purity continues to be a growing concern, research in forgery detection focuses on enhancing model reliability and adaptability to combat evolving manipulation techniques. By leveraging MobileNetV2, ELA, and CNNs, researchers can develop robust solutions for detecting image forgery. Future developments in neural network architectures and advanced image analysis techniques will further strengthen these MobileNetV2 models has shown improved accuracy in detecting high-quality forged images.

Despite recent advancements in forgery detection, challenges persist. The increasing sophistication of forgery techniques makes detection more difficult, and models often struggle to generalize to new forms of image tampering. Additionally, the high computational costs of deep learning models create limitations for large-scale and real-time implementations. Addressing these issues requires further optimization of lightweight architectures like MobileNetV2 and enhanced preprocessing

techniques such as ELA to improve efficiency and accuracy in forgery detection. As digital media see accuracy and reliability of forgery detection systems, ensuring the integrity of digital content.

III. METHODOLOGY

This study employs a deep learning technique, MobileNetV2 to predict forgery images using real-time digital images. The methodology consists of data collection, error level analysis, model development, performance analysis and model deployment.

1. Data Collection

The dataset used for training and testing the model is CASIA v2, which consists of 12,615 digitally manipulated images along with their corresponding authentic versions. The dataset is essential for building an effective deep-learning model for image forgery detection. To ensure consistency, each image is preprocessed by resizing it to (200,200) pixels, converting it into NumPy arrays, and normalizing pixel values. This preprocessing step enhances the efficiency of the learning process. To create a reliable training and testing pipeline, the dataset is split into an 80:20 ratio, ensuring that the model learns from diverse examples while being tested on unseen images. The training set helps the model understand different patterns of forgeries, while the testing set evaluates its accuracy and generalization ability. Proper dataset preparation is crucial as it directly impacts the model's performance in detecting manipulated images.

2. Error Level Analysis

This system utilizes Error Level Analysis (ELA) to detect inconsistencies in digital images. When an image undergoes editing and is resaved, different regions experience varying degrees of compression, which ELA effectively reveals. By converting an image into a JPEG file with a predefined compression rate and then comparing it with the original, a difference map is generated. This map reveals possible alterations by displaying tampered regions with brighter colours. The advantage of ELA lies in its ability to make even minor modifications noticeable. Since human eyes may struggle to detect subtle changes in an image, ELA enhances the forgery detection process by making discrepancies more prominent. The processed images serve as valuable inputs for the neural network, assisting in the accurate classification of authentic and manipulated images.

3. Model Development

The deep learning model used for forgery detection is built using a Convolutional Neural Network (CNN), specifically leveraging the MobileNetV2 architecture. CNNs are highly effective for image processing tasks as they extract critical spatial features from images. The architecture consists of multiple convolutional layers, max-pooling layers to reduce dimensions, and fully connected layers for classification. Dropout layers are incorporated to prevent overfitting and ensure better generalization. The model is trained using categorical cross-entropy loss along with the Adam optimizer to ensure effective and efficient convergence. A batch size of 32 is used during training, allowing the model to learn efficiently over multiple epochs. Data augmentation techniques, such as image rotation, flipping, and brightness adjustments, are applied to enhance model performance. These techniques help in making the

model robust against variations in image forgery, improving its ability to detect tampering under different conditions.

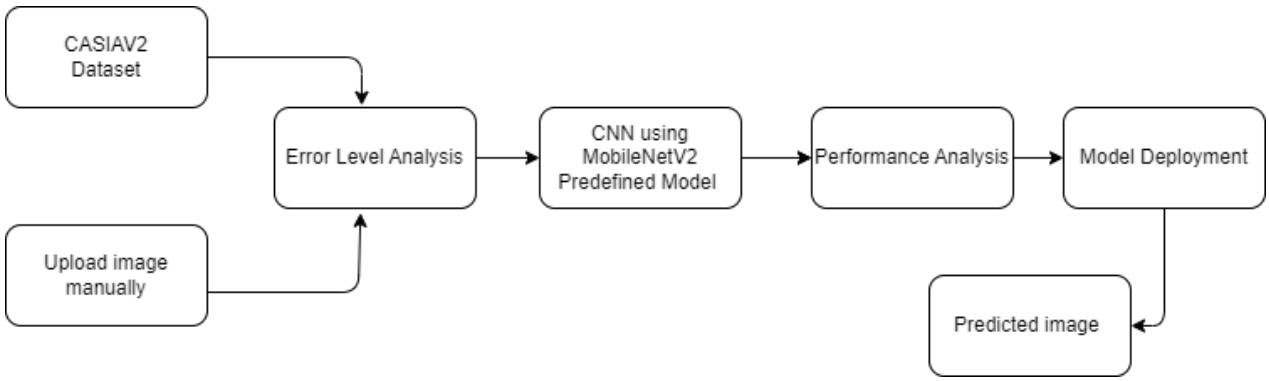

Fig. 1: System Architecture

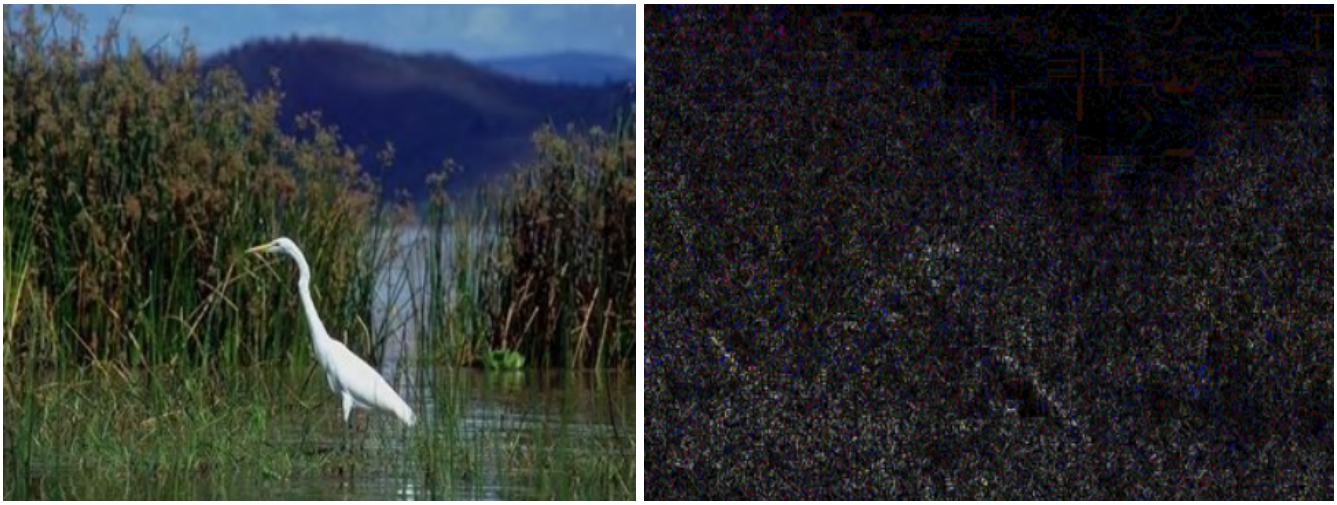

Fig. 2: converting an image into grey scale image

4. Performance Analysis

The dataset was divided into training (80%) and testing (20%) sets. The model was trained using the MobileNetV2. Performance was evaluated using the following metrics:

- **Accuracy:** Measures the overall prediction correctness.
- **Precision & Recall:** Evaluate the model's ability to identify image authenticity correctly.
- **F1-score:** Ensures a balance between precision and recall.
- **Confusion Matrix:** Analyzing misclassification patterns.

The model loss and model accuracy is given below:

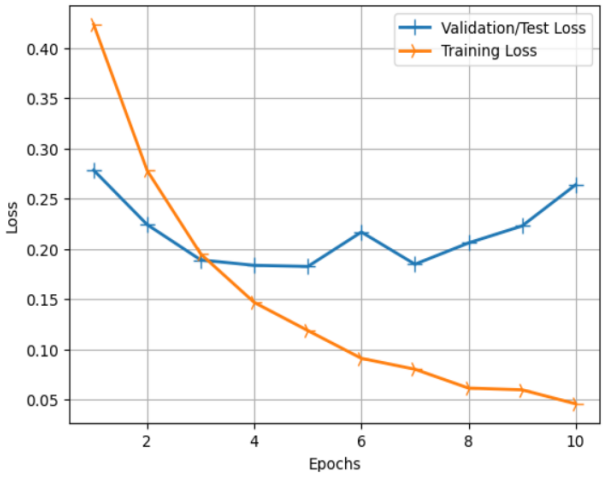

Fig 3: Model loss

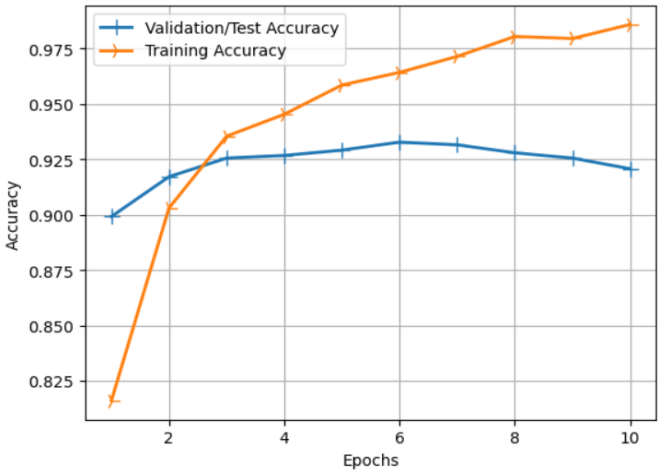

Fig 4: Model accuracy

5. Model Deployment

Once the model reaches a satisfactory level of accuracy, it is stored in a .h5 format, making it suitable for deployment in a fully functional web application. This web-based system enables users to upload images for forgery detection, delivering instant results. The backend is developed using frameworks like Flask ensuring smooth interaction between the user interface and the forgery detection model. The frontend is designed with a user-friendly interface, presenting forgery detection outcomes in a clear and comprehensible manner. Additionally, the system includes an interactive dashboard that offers in-depth analysis through visual tools such as confusion matrices, accuracy graphs, and precision-recall curves. To ensure the system performs efficiently under high user traffic, stress testing is conducted, assessing its reliability and responsiveness. With these integrated components, the forgery detection system serves as an effective tool for identifying digital image manipulations, making it valuable in forensic investigations, media authentication, and fraud prevention.

IV. RESULT & DISCUSSION

The implemented system, utilizing Convolutional Neural Networks (CNNs) combined with Error Level Analysis (ELA), achieved an accuracy of 92%, precision of 89%, recall of 92%, and an F1-score of 92% in detecting altered images. The evaluation conducted using the CASIA v2 dataset demonstrated the model's ability to effectively identify inconsistencies in image artifacts. By incorporating the MobileNetV2 architecture, the system improved computational efficiency, enabling faster and more reliable detection. The results indicate that deep learning-based approaches outperform traditional machine learning techniques in identifying manipulations. However, further enhancements, like expanding the dataset and refining model architectures, are necessary to improve generalization and adaptability to evolving image alteration methods.

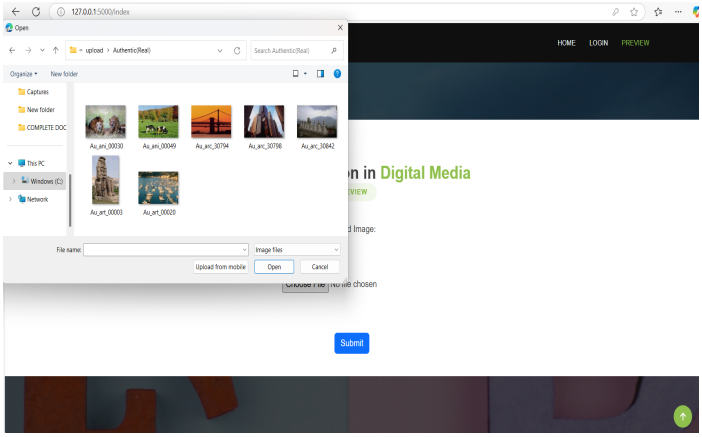

Fig. 9: Uploading an image

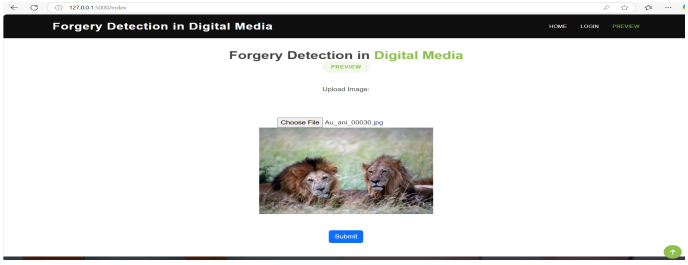

Fig. 10: Uploaded image for forgery detection

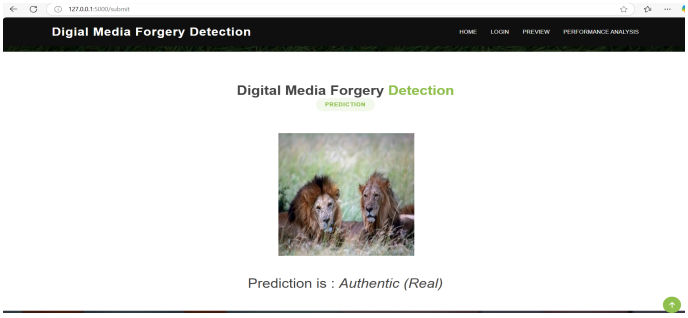

Fig 11: Result of the image (Authentic)

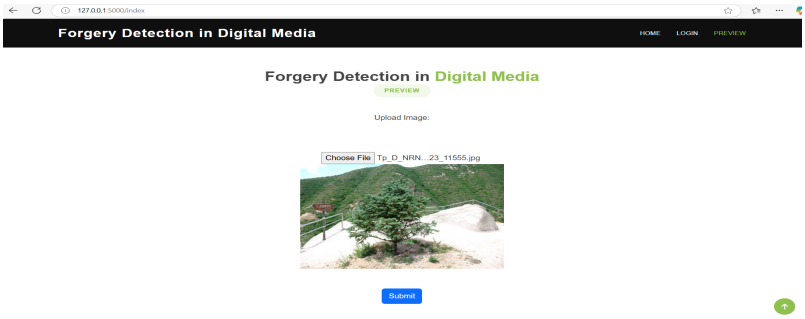

Fig 12: Uploading another for forgery detection

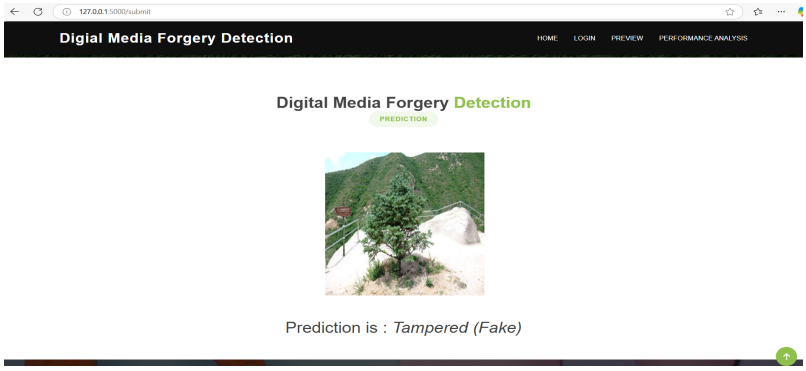

Fig 13: Result of the image (Tampered)

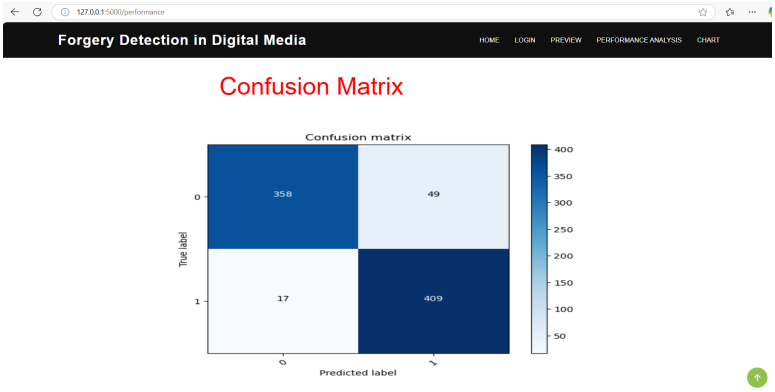

Fig 14: Performance Analysis through Confusion Matrix

V. CONCLUSION AND FUTURE WORK

The growing prevalence of digital image manipulation presents challenges in maintaining authenticity and trustworthiness in media. The project, "Digital Image Forgery Detection Using CNN and Error Level Analysis (ELA)," introduces an effective approach to identifying altered images. By leveraging Convolutional Neural Networks (CNNs) in combination with ELA, the system accurately detects inconsistencies caused by forgeries. This integration enhances the identification of manipulated regions while ensuring computational efficiency. With the ability to recognize both basic and complex forgeries, the proposed system serves as a valuable asset for forensic experts, content moderators, and individuals aiming to validate digital content. Furthermore, its potential for real-time implementation broadens its applicability across fields such as journalism, social media, and security. To further enhance detection capabilities, various improvements can be explored. Implementing advanced deep learning models, including transformers and ensemble learning, could improve the system's adaptability to diverse forgery techniques. Utilizing transfer learning on large datasets would refine generalization, while real-time optimization would allow efficient deployment on devices with limited resources. Additionally, improving interpretability through explainable AI techniques can provide clearer insights into model decisions, assisting forensic investigations. Expanding the dataset with emerging manipulation methods

and extending detection techniques to videos and other multimedia formats would further strengthen the robustness of the system.

Beyond technological advancements, integrating the forgery detection system into forensic analysis tools, content moderation platforms, and social media frameworks can help mitigate the spread of manipulated content. Developing intuitive user interfaces and APIs would make the technology more accessible to journalists, law enforcement agencies, and general users. Ethical considerations, including privacy concerns and bias mitigation, must be carefully addressed to ensure responsible use of forgery detection technologies. Additionally, raising public awareness about digital image authenticity through educational initiatives would promote more informed media consumption. By continuously refining and expanding its capabilities, this system contributes to the broader goal of preserving the reliability and security of digital content.

References

1. Hosny, K. M., Mortda, A. M., Lashin, N. A., & Fouda, M. M. (2023). A new method to detect splicing image forgery using convolutional neural network. *Applied Sciences, 13*(3), 1272. https://doi.org/10.3390/app13031272
2. Li, F., Pei, Z., Wei, W., Li, J., & Qin, C. (2022). Image forgery detection using tamper-guided dual self-attention network with multiresolution hybrid feature. *Security and Communication Networks, 2022*, Article 3568934. https://doi.org/10.1155/2022/3568934
3. Li, Q., Wang, C., Zhou, X., & Qin, Z. (2022). Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN. *Scientific Reports, 12*, 14987. https://doi.org/10.1038/s41598-022-19418-8
4. Koul, S., Kumar, M., Khurana, S. S., Mushtaq, F., & Kumar, K. (2022). An efficient approach for copy-move image forgery detection using convolution neural network. *Multimedia Tools and Applications, 81*(8), 11259–11277. https://doi.org/10.1007/s11042-021-11587-5
5. Ali, S. S., Ganapathi, I. I., Vu, N.-S., Saxena, N., & Werghi, N. (2022). Image forgery detection using deep learning by recompressing images. *Electronics, 11*(3), 403. https://doi.org/10.3390/electronics11030403
6. Qazi, E. U. H., Zia, T., & Almorjan, A. (2022). Deep learning-based digital image forgery detection system. *Applied Sciences, 12*(6), 2851. https://doi.org/10.3390/app12062851
7. Gu, A.-R., Nam, J.-H., & Lee, S.-C. (2022). FBI-Net: Frequency-based image forgery localization via multitask learning with self-attention. *IEEE Access, 10*, 62751–62762. https://doi.org/10.1109/ACCESS.2022.3179629
8. Kadam, K. D., Ahirrao, S., & Kotecha, K. (2021). Multiple image splicing dataset (MISD): A dataset for multiple splicing. *Data, 6*(10), 102. https://doi.org/10.3390/data6100102
9. Agarwal, R., Verma, O. P., Saini, A., Shaw, A., & Patel, A. R. (2021). The advent of deep learning-based forgery detection. In *Innovative Data Communication Technologies and Application*. Springer. https://doi.org/10.1007/978-981-16-1694-3_13
10. Elaskily, M. A., Alkinani, M. H., Sedik, A., & Dessouky, M. M. (2021). Deep learning-based algorithm (ConvLSTM) for copy-move forgery detection. *Journal of Intelligent & Fuzzy Systems, 40*(3), 4385–4405. https://doi.org/10.3233/JIFS-202203
11. Mohassin, A., & Farida, K. (2021). Digital image forgery detection approaches: A review. In *Applications of Artificial Intelligence in Engineering*. Springer. https://doi.org/10.1007/978-981-16-7005-1_7
12. Meena, K. B., & Tyagi, V. (2021). *Image splicing forgery detection techniques: A review*. Springer. https://doi.org/10.1007/978-3-030-77692-1
13. Gupta, S., Mohan, N., & Kaushal, P. (2021). Passive image forensics using universal techniques: A review. *Artificial Intelligence Review, 55*(3), 1629–1679. https://doi.org/10.1007/s10462-020-09915-8
14. Khoh, W. H., Pang, Y. H., Teoh, A. B. J., & Ooi, S. Y. (2021). In-air hand gesture signature using transfer learning and its forgery attack. *Applied Soft Computing, 113*, 108033. https://doi.org/10.1016/j.asoc.2021.108033
15. Abhishek, & Jindal, N. (2021). Copy-move and splicing forgery detection using deep convolutional neural network and semantic segmentation. *Multimedia Tools and Applications, 80*(3), 3571–3599. https://doi.org/10.1007/s11042-020-09765-9

16. Qureshi, M. M., & Qureshi, M. G. (2021). Image forgery detection & localization using regularized U-Net. Springer. https://doi.org/10.1007/978-981-16-3982-7_12
17. Haipeng, C., Chang, C., Zenan, S., & Yingda, L. (2021). Hybrid features and semantic reinforcement network for image forgery detection. *Multimedia Systems, 28*(2), 363–374. https://doi.org/10.1007/s00530-021-00824-2
18. Jaiswal, A. K., & Srivastava, R. (2021). Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model. *Neural Processing Letters, 54*(1), 75–100. https://doi.org/10.1007/s11063-021-10438-1
19. Kadam, K. D., Ahirrao, S., & Kotecha, K. (2021). Detection and localization of multiple image splicing using MobileNetV1. *IEEE Access, 9*, 162499–162519. https://doi.org/10.1109/ACCESS.2021.3076429
20. Rao, Y., Ni, J., & Zhao, H. (2020). Deep learning local descriptor for image splicing detection and localization. *IEEE Access, 8*, 25611–25625. https://doi.org/10.1109/ACCESS.2020.2971061
21. Madapuri, R. K., & Mahesh, P. C. S. (2017). HBS-CRA: Scaling impact of change request towards fault proneness: Defining a heuristic and biases scale (HBS) of change request artifacts (CRA). *Cluster Computing, 22*(S5), 11591–11599. https://doi.org/10.1007/s10586-017-1424-0
22. Dwaram, J. R., & Madapuri, R. K. (2022). Crop yield forecasting by long short-term memory network with Adam optimizer and Huber loss function in Andhra Pradesh, India. *Concurrency and Computation: Practice and Experience, 34*(27). https://doi.org/10.1002/cpe.7310
23. Reddy, B. S. H. (2025). Deep learning-based detection of hair and scalp diseases using CNN and image processing. *Milestone Transactions on Medical Technometrics, 3*(1), 145–155. https://doi.org/10.5281/zenodo.14965660
24. Reddy, B. S. H., Venkatramana, R., & Jayasree, L. (2025). Enhancing apple fruit quality detection with augmented YOLOv3 deep learning algorithm. *International Journal of Human Computations & Intelligence, 4*(1), 386–396. https://doi.org/10.5281/zenodo.14998944
25. Kumar, A., Satheesha, T. Y., Salvador, B. B. L., Mithileysh, S., & Ahmed, S. T. (2023). Augmented Intelligence enabled Deep Neural Networking (AuDNN) framework for skin cancer classification and prediction using multi-dimensional datasets on industrial IoT standards. *Microprocessors and Microsystems, 97*, 104755.
26. Patil, K. K., & Ahmed, S. T. (2014, October). Digital telemammography services for rural India, software components and design protocol. In *2014 International Conference on Advances in Electronics Computers and Communications* (pp. 1–5). IEEE.
27. Sreedhar Kumar, S., Ahmed, S. T., Flora, P. M., Hemanth, L. S., Aishwarya, J., GopalNaik, R., & Fathima, A. (2021, January). An improved approach of unstructured text document classification using predetermined text model and probability technique. In *ICASISET 2020: Proceedings of the First International Conference on Advanced Scientific Innovation in Science, Engineering and Technology* (p. 378). European Alliance for Innovation.
28. Ahmed, S. T., Sandhya, M., & Shankar, S. (2018, August). ICT's role in building and understanding Indian telemedicine environment: A study. In *Information and Communication Technology for Competitive Strategies: Proceedings of Third International Conference on ICTCS 2017* (pp. 391–397). Springer.
29. Singh, K. D., & Ahmed, S. T. (2020, July). Systematic linear word string recognition and evaluation technique. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 545–548). IEEE.