

DETECTOO: AI-Based Image Forgery Detection Using Error Level Analysis, Edge Detection and Noise Analysis

Anisha Sathe¹, Prof. Manisha Darak², Sneha Pawar³, Shravani Sonawane⁴

Department of Computer Engineering, RMD Sinhgad School of Engineering, Warje, Pune, Maharashtra, India

Abstract - Digital image manipulation has become increasingly common due to the widespread availability of image editing software and artificial intelligence tools. The ability to alter images without leaving obvious visual traces poses significant challenges in fields such as journalism, digital forensics, law enforcement, and social media verification. This paper presents **DETECTOO**, a web-based image forgery detection system designed to identify potentially manipulated regions in digital images using multiple forensic analysis techniques. The proposed system employs Error Level Analysis (ELA), Edge Detection, and Noise Analysis to detect inconsistencies that may indicate image tampering. The system generates heatmaps, overlay visualizations, confidence scores, tamper percentage metrics, and downloadable PDF reports to assist users in forensic examination. The frontend is developed using React.js, while FastAPI, OpenCV, and Python are used for backend processing and image analysis. Experimental results demonstrate that the system effectively highlights suspicious regions and provides users with intuitive visual evidence of possible manipulation. The proposed approach offers an accessible, user-friendly, and efficient solution for image forgery detection in real-world applications.

Key Words: Image Forgery Detection, Error Level Analysis, Edge Detection, Noise Analysis, Digital Forensics, FastAPI.

1. INTRODUCTION

The rapid growth of digital communication and social media platforms has significantly increased the sharing and distribution of digital images. Images are widely used in journalism, legal investigations, social networking, advertising, and educational content. However, the availability of advanced image editing software and artificial intelligence tools has made image manipulation easier than ever before. As a result, forged images can be created and distributed without leaving obvious visual evidence, making it difficult for users to determine the authenticity of digital content.

Image forgery has become a major concern in digital forensics because manipulated images can be used to spread misinformation, create false evidence, and influence public opinion. Traditional methods of image

verification often require forensic expertise and specialized software tools, which may not be accessible to ordinary users. Therefore, there is a growing need for automated systems capable of detecting image tampering efficiently and accurately.

This paper presents **DETECTOO**, a web-based image forgery detection system designed to identify suspicious modifications in digital images using multiple forensic analysis techniques. The proposed system utilizes Error Level Analysis (ELA), Edge Detection, and Noise Analysis to examine image inconsistencies and detect potentially manipulated regions. The system further generates heatmaps, overlay visualizations, confidence scores, tamper percentage metrics, and downloadable PDF reports to assist users in forensic examination.

The frontend of the system is developed using React.js, while FastAPI, OpenCV, Pillow, and Python are used for backend processing and image analysis. The objective of **DETECTOO** is to provide an accessible, efficient, and user-friendly platform that enables users to verify image authenticity without requiring advanced forensic knowledge. The proposed solution contributes to the field of digital image forensics by combining multiple analysis techniques with intuitive visualization and reporting features.

2. LITERATURE SURVEY

Digital image forgery detection has become an important research area in the field of digital forensics due to the increasing availability of image editing tools and artificial intelligence technologies. Various techniques have been proposed by researchers to identify manipulated images and verify their authenticity.

Error Level Analysis (ELA) is one of the most widely used passive image forgery detection techniques. It works by identifying variations in JPEG compression levels within an image. When an image is edited and saved multiple times, manipulated regions often exhibit different compression characteristics compared to the original image. ELA highlights these inconsistencies and assists in detecting suspicious areas.

Edge-based forgery detection methods focus on identifying abnormal boundaries and structural inconsistencies within an image. Edge Detection algorithms such as the Canny Edge Detector are commonly used to extract image edges and locate regions that may have undergone modification. Manipulated regions frequently contain irregular edge patterns that differ from surrounding areas.

Noise Analysis is another effective forensic technique used to detect image tampering. Every digital image contains sensor noise introduced during image acquisition. Editing operations often disturb this natural noise distribution, creating inconsistencies that can be detected through noise analysis. This technique is particularly useful for identifying copy-move and splicing forgeries.

Recent research has also explored the use of machine learning and deep learning techniques for image forgery detection. Convolutional Neural Networks (CNNs) have demonstrated promising results in identifying manipulated regions automatically. However, deep learning approaches generally require large datasets, high computational resources, and complex model training procedures.

Although existing methods provide valuable solutions for forgery detection, many systems rely on a single detection technique and offer limited visualization capabilities. Furthermore, several tools require forensic expertise for result interpretation. To overcome these limitations, the proposed DETECTOO system combines Error Level Analysis, Edge Detection, and Noise Analysis with heatmap generation, overlay visualization, and automated PDF reporting to provide a more comprehensive and user-friendly image forgery detection solution.

3. RESEARCH GAP

The literature survey reveals that numerous image forgery detection techniques have been developed to identify manipulated digital images. However, several limitations still exist in current approaches. Many existing systems rely on a single forensic technique such as Error Level Analysis, Edge Detection, Noise Analysis, or Machine Learning-based classification. While these methods can detect certain types of image manipulation, their effectiveness may decrease when used independently.

Most available image forgery detection tools provide limited visual interpretation of the detected results. Users often receive only a classification result without sufficient evidence explaining why an image is considered authentic or tampered. This makes it difficult for non-technical users to understand and verify the analysis outcome. In addition, many advanced forensic systems require specialized knowledge, expensive software, or high computational resources, making them less accessible to ordinary users.

Another significant limitation is the lack of integrated reporting functionality. Existing solutions rarely provide automated forensic reports that summarize analysis results, detected regions, confidence scores, and supporting visual evidence. Furthermore, several research approaches focus primarily on accuracy while overlooking usability, user experience, and real-time accessibility through web-based platforms.

To address these limitations, the proposed DETECTOO system integrates multiple forensic techniques including Error Level Analysis (ELA), Edge Detection, and Noise Analysis within a single platform. The system enhances result interpretability through heatmap generation, overlay visualization, confidence scoring, tamper percentage calculation, and automated PDF report generation. This integrated approach aims to provide an efficient, accessible, and user-friendly solution for digital image forgery detection.

4. PROBLEM STATEMENT

With the rapid advancement of image editing software and artificial intelligence technologies, digital image manipulation has become increasingly common. Tampered images can be created easily and distributed through social media, news platforms, and online communication channels. Such manipulated images can spread misinformation, create false evidence, damage reputations, and influence public opinion. Detecting image forgery through visual inspection alone is often difficult because modern editing tools can produce highly realistic modifications that are not easily noticeable to the human eye.

Existing image forgery detection solutions often require forensic expertise, expensive software, or complex analysis procedures. Many available systems focus on a single detection technique and provide limited explanation of the detected results. As a result, ordinary users face challenges in verifying the authenticity of digital images and understanding the evidence behind the detection process.

Therefore, there is a need for an efficient, accessible, and user-friendly image forgery detection system capable of identifying manipulated regions in digital images and presenting the results in an understandable manner. The proposed DETECTOO system addresses this problem by utilizing Error Level Analysis (ELA), Edge Detection, and Noise Analysis to detect suspicious image modifications. The system further provides heatmap visualization, overlay visualization, confidence scores, tamper percentage metrics, and automated PDF reports to assist users in forensic image verification.

5. OBJECTIVES OF THE SYSTEM

The primary objective of the proposed DETECTOO system is to develop an efficient and user-friendly platform for detecting image forgery using digital forensic techniques. The system aims to assist users in verifying the authenticity of digital images and identifying potentially manipulated regions through automated analysis.

The specific objectives of the system are as follows:

1. To detect manipulated regions in digital images using forensic image analysis techniques.
2. To implement Error Level Analysis (ELA) for identifying compression inconsistencies that may indicate image tampering.
3. To apply Edge Detection techniques for locating abnormal boundaries and suspicious structural modifications within images.
4. To perform Noise Analysis for identifying inconsistencies in image noise patterns caused by editing operations.
5. To generate heatmap visualizations that highlight potentially tampered regions for easy interpretation.
6. To create overlay visualizations by superimposing detected suspicious regions on the original image.
7. To calculate tamper percentage and confidence scores that provide quantitative information about image authenticity.
8. To generate downloadable PDF reports containing analysis results, forensic metrics, and visual evidence.

9. To provide a simple and accessible web-based interface that can be used by both technical and non-technical users.
10. To improve awareness and accessibility of digital image forensic analysis through an automated and user-friendly solution.

6. PROPOSED SYSTEM

The proposed system, DETECTOO, is a web-based image forgery detection platform designed to identify suspicious modifications in digital images using multiple forensic analysis techniques. The system combines Error Level Analysis (ELA), Edge Detection, and Noise Analysis to improve the accuracy and reliability of image forgery detection. The primary objective of the system is to provide users with an accessible and efficient method for verifying image authenticity without requiring specialized forensic expertise.

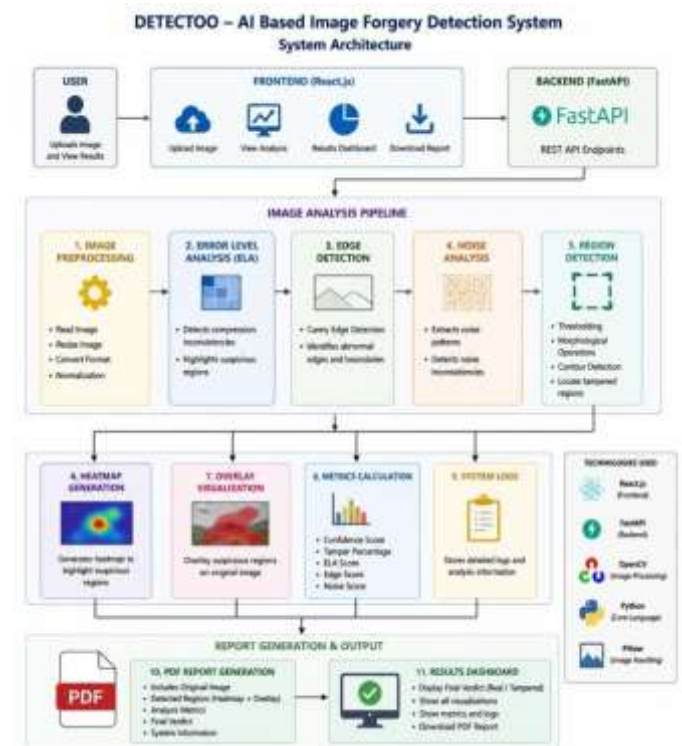
The system follows a client-server architecture consisting of a React.js frontend and a FastAPI backend. Users upload an image through the web interface, and the backend performs forensic analysis using OpenCV and Python-based image processing techniques. The uploaded image undergoes multiple stages of analysis, including Error Level Analysis for compression inconsistency detection, Edge Detection for identifying abnormal boundaries, and Noise Analysis for detecting irregular noise patterns.

After processing, the system generates a binary mask to identify suspicious regions. Contour detection techniques are then applied to locate and extract potential tampered areas. The detected regions are highlighted using bounding boxes and visualized through heatmaps and overlay images. The system further calculates tamper percentage, confidence score, ELA score, Edge score, and Noise score to provide quantitative information regarding the authenticity of the image.

To improve result interpretation, DETECTOO provides side-by-side image comparison, heatmap visualization, and system logs displaying detailed forensic metrics. Additionally, the system generates downloadable PDF reports containing analysis results, detected regions, visual evidence, and performance metrics. This integrated approach enables users to efficiently analyze images and understand the forensic evidence supporting the final verdict.

The proposed system offers a practical solution for digital image verification and can be applied in areas such as journalism, digital forensics, law enforcement, social media verification, and academic research.

7. SYSTEM ARCHITECTURE



7.1 System Architecture Description

The DETECTOO system follows a client-server architecture consisting of a React.js frontend and a FastAPI backend. Users upload images through the web interface, which are sent to the backend for forensic analysis. The system performs Error Level Analysis (ELA), Edge Detection, and Noise Analysis to identify suspicious regions within the image. The detected regions are further processed to generate heatmaps, overlay visualizations, confidence scores, and tamper percentage metrics. Finally, the results are displayed on the dashboard and included in a downloadable PDF forensic report.

8. ALGORITHMS USED

The proposed DETECTOO system utilizes multiple image forensic analysis techniques to identify suspicious modifications in digital images. These techniques analyze compression artifacts, image boundaries, and noise inconsistencies to detect potentially tampered regions. The algorithms used in the system are described below.

8.1 Error Level Analysis (ELA)

Error Level Analysis (ELA) is used to identify compression inconsistencies within an image. The uploaded image is recompressed at a predefined quality level and compared with the original image. Regions that have been edited often exhibit different compression characteristics and therefore appear brighter in the ELA output. These inconsistencies help identify potentially manipulated areas.

8.2 Edge Detection

Edge Detection is performed using the Canny Edge Detection algorithm. This technique identifies abrupt changes in pixel intensity and extracts significant image boundaries. Manipulated regions frequently contain irregular edge

structures, making edge detection useful for locating suspicious modifications.

8.3 Noise Analysis

Noise Analysis examines variations in image noise patterns. A Gaussian Blur is applied to the image, and the difference between the original and blurred image is calculated. Inconsistencies in the resulting noise distribution may indicate image tampering.

8.4 Heatmap Generation

A heatmap is generated from the analysis results to visually highlight suspicious regions. The heatmap enables users to quickly identify areas that require further forensic investigation.

8.5 Overlay Visualization

The detected suspicious regions are highlighted on the original image using bounding boxes and overlay techniques. This visualization provides clear evidence of potential image manipulation and improves result interpretation.

9. RESULTS AND DISCUSSION

The proposed DETECTOO system was successfully developed and tested using various original and manipulated images. The system performs image forgery detection using Error Level Analysis (ELA), Edge Detection, and Noise Analysis techniques. Experimental results demonstrate that the system can effectively identify suspicious regions and provide visual evidence of potential image tampering.

The user uploads an image through the web interface, after which the system processes the image and generates forensic analysis results. The detected suspicious regions are highlighted using overlay visualizations and heatmaps, allowing users to easily identify areas that may have been manipulated. The system also calculates important forensic metrics such as confidence score, tamper percentage, ELA score, edge score, noise score, and the number of detected regions.

The generated results are displayed on an interactive dashboard that includes side-by-side image comparison, heatmap visualization, system logs, and forensic metrics. In addition, the system automatically generates a downloadable PDF report containing analysis results and visual evidence. The results obtained indicate that the proposed approach provides an efficient and user-friendly solution for digital image forgery detection.

Result Screens

Fig. 2. Home Page of DETECTOO



Fig. 3. Image Upload Interface

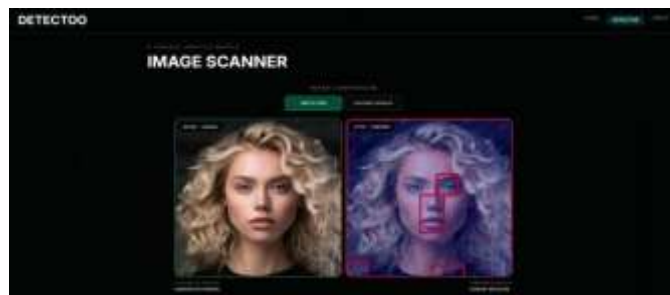


Fig. 4. Analysis Result Dashboard



Fig. 5. Heatmap Visualization of Suspicious Regions

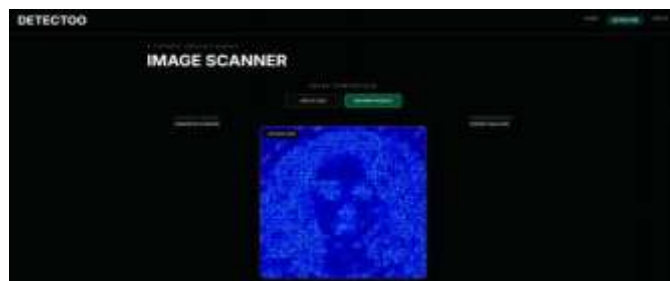
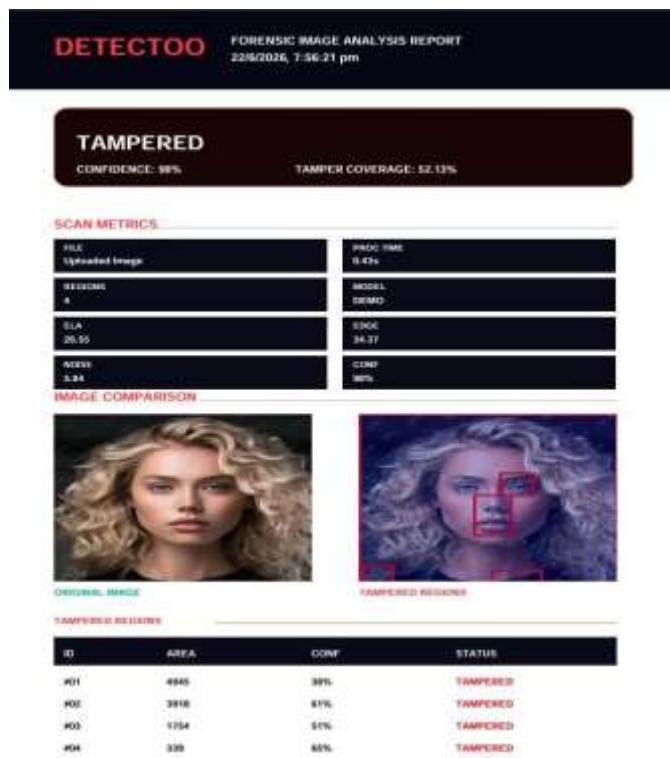


Fig. 6. Generated PDF Forensic Report



10. CONCLUSIONS

In this paper, DETECTOO, a web-based image forgery detection system, was successfully developed and implemented using Error Level Analysis (ELA), Edge Detection, and Noise Analysis techniques. The system effectively identifies suspicious regions in digital images and provides visual evidence through heatmaps and overlay visualizations. In addition, forensic metrics such as confidence score, tamper percentage, ELA score, edge score, and noise score are generated to support the analysis process. The developed system offers an intuitive user interface and automated PDF report generation, making image forgery detection accessible to both technical and non-technical users. The experimental results demonstrate that the proposed system provides an efficient and reliable solution for digital image authenticity verification.

11. FUTURE SCOPE

The functionality of DETECTOO can be further enhanced by incorporating advanced deep learning techniques for improved forgery detection accuracy. Future developments may include support for video forgery detection, detection of AI-generated images, batch processing of multiple images, and cloud-based deployment for large-scale analysis. Mobile application integration and real-time social media image verification can also be explored to increase accessibility and practical applicability of the system in various domains.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our guide, and the faculty members of the Department of Computer Engineering, RMD Sinhgad School of Engineering, for their valuable guidance, support, and encouragement throughout the project. We also thank our mentors and staff members for their assistance and cooperation during the successful completion of this work.

REFERENCES

- [1] M. Zanardelli, F. Guerrini, R. Leonardi, N. Adami, "Image forgery detection: a survey of recent deep-learning approaches," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1–43, 2023.
- [2] M.A. Anwar, A. Liz-Lopez, S. Bonomi, "Image forgery detection by transforming local descriptors into deep-derived features," *Applied Soft Computing*, vol. 138, pp. 110933, 2023.
- [3] Z.J. Barad, R. Tewari, M. Tiwari, "Image Forgery Detection using Deep Learning: A Survey," in *Proc. 2020 International Conference on Computing, Communication, and Intelligent Systems*, pp. 225–231, 2020.
- [4] K. Lee, H. Kumar, "Hybrid GAN-based data augmentation for image forgery detection," *IEEE Access*, vol. 12, pp. 42279–42292, 2024.
- [5] B. Rahman, S. Parveen, M. S. Khan, "Transfer Learning-based Localisation of Image Forgeries in Social Media," *International Journal of Computer Vision and Image Processing*, vol. 15, no. 3, pp. 99–113, 2022.
- [6] D. Alves, A. Pinto, A. Ferreira, "Unsupervised deep anomaly detection for image tampering identification," *Pattern Recognition Letters*, vol. 180, pp. 88–97, 2025.
- [7] M. Liz-Lopez, S. Bonomi, "Recent Advances in Image Forgery Detection and Localization," *Journal of Imaging*, vol. 10, no. 1, pp. 1–21, 2024.
- [8] S. Gupta, S. Singh, "State-of-the-Art Techniques for Image Forgery Detection," *International Journal of Engineering Research and Applications*, vol. 15, no. 1, pp. 106–120, 2025.
- [9] Y. Hamed, F. Ibrahim, R. Adepoju, "Challenges and Future Directions in Image Forgery Detection for Fake News," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 1234–1249, 2023.
- [10] J. Smith, F. Wang, "A full-image, full-resolution end-to-end trainable CNN framework for image forgery detection," *IEEE Access*, vol. 8, pp. 12260–12277, 2020.
- [11] A. Rehman, Z. Wang, "Digital Image Forgery Detection and Localization Using Deep Learning Approaches," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 18, no. 3s, pp. 1–22, 2022.
- [12] L. Bondi, S. Lameri, D. Guera, P. Bestagini, E. J. Delp, S. Tubaro, "Tampering Detection and Localization through Clustering of Camera-based Image Patches," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3219–3231, 2020.
- [13] P. Deb, S. Deb, A. Das, N. Kar, "Image Forgery Detection Techniques: Latest Trends and Key Challenges," *IEEE Access*, vol. 12, pp. 124578–124595, 2024.
- [14] H. Farid, "Image Forgery Detection: A Survey," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 47–53, 2020.
- [15] R. C. Gonzalez, R. E. Woods, "Digital Image Processing," 4th Edition, Pearson, 2018.
- [16] J. Cozzolino, G. Poggi, L. Verdoliva, "Splicebuster: A new blind image splicing detector," in *Proc. IEEE International Workshop on Information Forensics and Security*, pp. 1–6, 2015.
- [17] H. Huang, W. Guo, Y. Zhang, "Detection of copy-move forgery in digital images based on DWT and SVD," in *Proc. IEEE International Conference on Computer Science and Automation Engineering*, pp. 423–427, 2021.
- [18] A. C. Popescu, H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," *Technical Report TR2004-515*, Dartmouth College, 2004.