IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Image Forgery Detection System

Mrs. Gujjala Usha[1], D Lahari[2], Ashwini[3], Muktha R[4], Yashashwini C. L[5]
Assistant Professor, Department of AI & ML[1]
Students, Department of AI & ML[2-5]
Proudhadevaraya Institute of Technology, Hospet, India
[1]laharid2005@gmail.com, [2] akhilashwini7@gmail.com, [3]rmuktha212@gmail.com
[4]Yashu28c5l@gmail.com

Abstract: *With the rapid expansion of digital media and online information sharing, ensuring the authenticity of digital images has become increasingly critical in journalism, legal investigations, cybersecurity, and social networking platforms. The availability of advanced image editing tools has made digital image manipulation easier and more sophisticated. This paper presents an Image Manipulation Detection System developed using Python that identifies forged or tampered images through digital forensic analysis techniques.*

The proposed system detects multiple types of image forgery, including copy–move manipulation, double JPEG compression artifacts, and Colour Filter Array (CFA) inconsistencies. Additionally, metadata analysis is performed to identify suspicious modifications in image properties. The system integrates these forensic techniques within a graphical user interface (GUI) to provide an efficient and user-friendly detection framework. Experimental results demonstrate the system's ability to accurately detect common image tampering methods while maintaining reliability and efficiency.

The proposed framework serves as a practical tool for digital image authentication and contributes to combating misinformation and digital fraud.

Keywords: Image Forgery Detection, Copy-Move Forgery, Double JPEG Compression, CFA Analysis, Digital Forensics, Metadata Analysis.

I. INTRODUCTION

Digital images play a critical role in modern communication, legal documentation, journalism, and online media. However, the ease of accessing advanced editing tools such as Photoshop, GIMP, and AI-based generative systems has significantly increased the risk of digital image manipulation. Image forgery can alter visual content in subtle ways, influencing public perception, spreading misinformation, and compromising evidentiary authenticity.

Image manipulations generally fall into categories such as copy-move forgery (cloning), image splicing, retouching, recompression, and hidden data embedding. Traditional active authentication methods such as watermarking and digital signatures require pre-embedded information, which is not feasible for already distributed images. Hence, passive image forensics techniques that analyse intrinsic image characteristics have gained significant importance.

This research proposes a multi-forensic Image Forgery Detection System that integrates several complementary detection methods. Each module in the system analyses different forensic traces left during manipulation. Spatial analysis detects duplicated regions; frequency-domain analysis identifies compression artifacts; sensor-level analysis examines CFA interpolation inconsistencies; statistical analysis detects noise irregularities; metadata inspection reveals contextual inconsistencies; and file-level investigation uncovers hidden data.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40441

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

II. LITERATURE SURVEY

1. Multi-Approach Survey and In-Depth Analysis of Image Forgery Detection Techniques:

This study presented a comprehensive survey of image forgery detection techniques by analysing traditional methods, deep learning approaches, and hybrid forensic models. The authors compared various algorithms based on accuracy, reliability, and computational efficiency. Traditional methods focused on statistical and frequency-based features, while deep learning models used convolutional neural networks for automatic feature extraction. Hybrid approaches combined both techniques to improve performance. The study concluded that hybrid models provide better detection accuracy and robustness. However, it also highlighted challenges such as high computational cost, lack of explainability, and difficulty in real-time implementation.

2. Image forgery Detection Comprehensive Review of Digital Forensics Approaches:

This research focused on digital forensic techniques for image forgery detection. It reviewed passive detection methods based on sensor noise patterns, JPEG compression artifacts, and colour filter array inconsistencies. The study emphasized the importance of explainable and interpretable models.

3. Deepfake Detection Enhanced Model for Image Forgery Detection to Combat Academic Misconduct:

This study introduced a deep learning-based enhanced model to detect deepfake images and prevent academic misconduct. The proposed model used multi-scale feature extraction and attention mechanisms to identify subtle forgery patterns. It achieved high detection accuracy on research and academic datasets. The model was particularly effective in detecting manipulated scientific images and fake experimental results. However, the study reported that the model requires large labelled datasets and high computational resources, which limits its practical implementation in small-scale systems.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed system follows a modular multi-forensic framework. Each detection technique operates independently and contributes to the final authenticity assessment.

1. Copy-Move Forgery Detection

The system divides the input image into overlapping blocks and extracts feature descriptors from each block. Lexicographic sorting is applied to detect similar feature vectors. Spatial offsets between matched blocks are calculated to identify duplicated regions. Suspicious areas are highlighted in the output.

2. Double JPEG Compression Detection

The image's DCT coefficients are analysed to detect periodic artifacts caused by multiple compression stages. Histogram inconsistencies indicate potential recompression.

3. CFA Artifact Detection

The system examines pixel interpolation consistency based on Bayer pattern analysis. Disrupted CFA patterns indicate tampered regions.

4. Noise Variance Analysis

High-pass filtering isolates noise components. Local variance is computed across image blocks, and statistically inconsistent regions are flagged.

5. Metadata Analysis

EXIF metadata is extracted and examined for editing software signatures, timestamp inconsistencies, or missing camera information.

6. Error Level Analysis (ELA)

The image is recompressed at a controlled quality level. Pixel-wise differences are computed to identify abnormal compression levels.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

7. String and Image Extraction

Binary-level scanning identifies hidden ASCII strings and embedded image files, detecting steganographic or appended data.

The integration of these techniques ensures comprehensive forgery detection.

IV. OBJECTIVES

To develop a multi-forensic Image Forgery Detection System that identifies various types of digital image manipulations using spatial, frequency-domain, statistical, sensor-level, metadata, and file-level analysis techniques.

- Copy-Move Forgery Detection: To identify duplicated regions within the same image used to hide or replicate objects.
- Double JPEG Compression Detection: To detect multiple JPEG compression artifacts that indicate possible image editing or recompression.
- CFA (Colour Filter Array) Artifact Detection: To analyse sensor interpolation inconsistencies caused by tampering or splicing.
- Noise Variance Analysis: To detect abnormal variations in noise patterns that suggest image manipulation.
- Metadata (EXIF) Analysis: To examine image metadata for editing traces, missing camera details, or timestamp inconsistencies.
- Error Level Analysis (ELA): To highlight regions with different compression levels that may indicate edited areas.
- String Extraction: To detect hidden textual or ASCII data embedded within the image file.
- Embedded Image Extraction: To identify and recover hidden or appended images within the file structure.

V. SYSTEM REQUIREMENTS

Software Requirements

1. Operating System

The system is cross-platform and can run on major operating systems without modification.

2. Coding Language: Python

The project is developed using Python 3.x for efficient image processing and forensic analysis.

3. IDE/Editor: VS Code

These tools are used to write, debug, and execute the Python code for the project.

4. Libraries Used:

- **NumPy –** Used for numerical computations and handling image pixel arrays as matrices.
- **OpenCV(cv2) –** Performs core image processing tasks such as reading, filtering, and analysing images.
- **Pillow (PIL) –** Handles image loading, format conversion, and metadata extraction.
- **Matplotlib –** Used to visualize images, histograms, and forensic analysis results.
- **Scikit-image –** Provides advanced image processing functions like feature extraction and filtering.

5. Package Manager: pip

Installs and manages all required Python libraries for the project.

6. Image Formats Supported: JPG, JPEG, PNG

The system processes common image file formats used in digital media.

7. Execution Mode: Python Script (.py files)

The program runs as executable Python script files from the command line or IDE.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

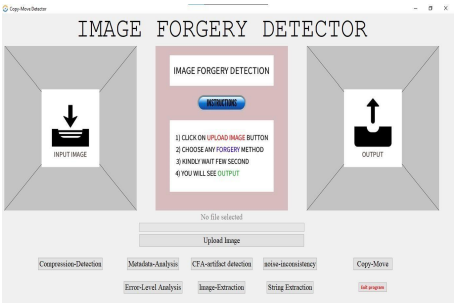
VI. IMPLEMENTATION AND WORKFLOW

Include:

1. Image Input
2. Preprocessing
3. Copy-Move Detection
4. Double JPEG Detection
5. CFA Analysis
6. Noise Analysis
7. Metadata Analysis
8. ELA Analysis
9. Hidden Data Detection
10. Final Authenticity Report

VII. RESULTS AND OUTCOMES

The proposed Image Forgery Detection System was successfully developed and tested using various digital forensic techniques. The system effectively detects image manipulations such as copy-move forgery, double JPEG compression, CFA inconsistencies, and metadata modifications. Error Level Analysis and Noise Variance Analysis helped identify suspicious regions within forged images. The metadata extraction module provided useful information about image origin and editing history. Experimental results showed that the combination of multiple forensic methods improves the accuracy and reliability of forgery detection. The user-friendly graphical interface enables easy image analysis and quick result generation. Overall, the system provides an effective solution for verifying the authenticity of digital images in forensic and security applications.



The Image Forgery Detector is a digital image forensics application that employs analytical and statistical techniques to detect image tampering. The system examines compression artifacts, noise inconsistencies, metadata anomalies, and copy-move regions to determine image authenticity

- **Compression Detection**
  Detects inconsistencies caused by multiple JPEG compressions. Tampered regions often show different compression patterns.
- **Error Level Analysis (ELA)**
  Highlights areas with varying compression errors. Modified regions appear brighter due to re-saving differences.
- **Metadata Analysis**
  Examines EXIF data to identify missing, altered, or suspicious image metadata.
- **CFA Artifact Detection**
  Detects irregularities in Colour Filter Array interpolation, common in manipulated images.
- **Noise Inconsistency**
  Analyses noise patterns across the image to detect unnatural variations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Copy-Move Detection

Identifies duplicated regions within the same image indicating copy-paste forgery.



Fig: Input image for Detection

The input image is a natural scene captured in a public environment, containing architectural structures and moving subjects.

It serves as the original image on which various forgery detection techniques are applied to examine authenticity and detect possible tampering.

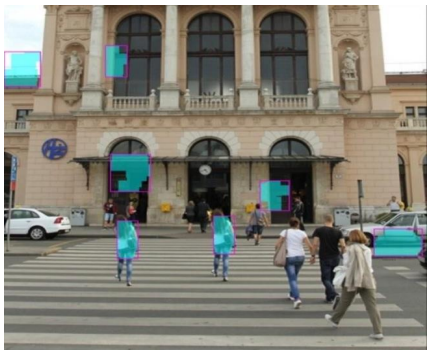


Fig: CFA analysis



Fig: CFA analysed output

CFA analysis detects forgeries by examining camera sensor colour filter array artifacts. Tampered regions show disrupted demosaicing patterns and inconsistent neighbour pixel correlations in R-G/B-G difference channels.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

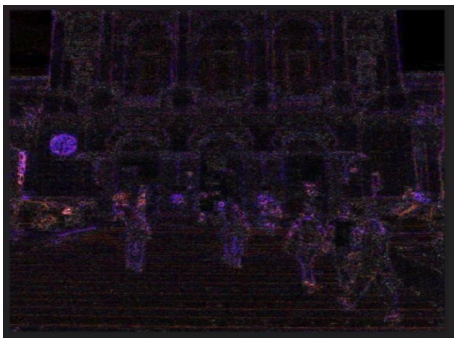


Fig: Error analysis

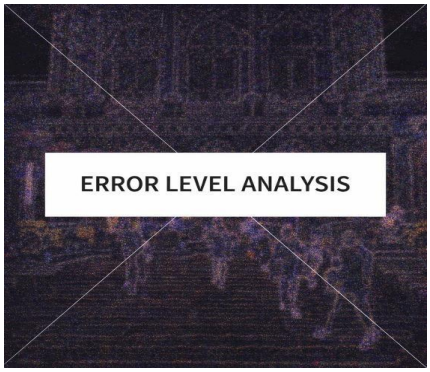


Fig:10.6 Error analysed output

ELA resaves the input JPEG at fixed quality (e.g., 90%), subtracts the recompressed image from the original to amplify compression differences. Tampered regions appear brighter (high error values >100) due to inconsistent JPEG levels from splicing/copy-move.

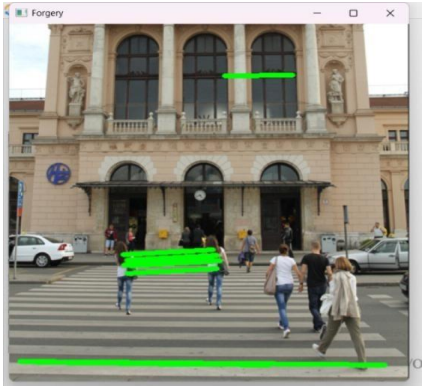


Fig: Copy-move analysis

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

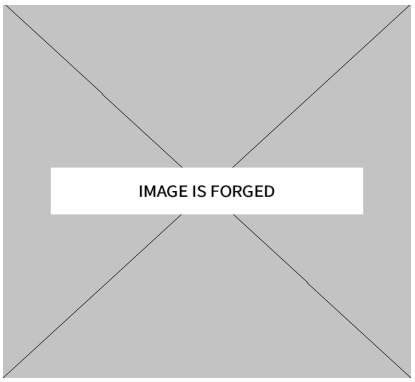


Fig: Copy-move analysed output

Divides image into overlapping blocks, extracts SIFT/DCT features, and matches similar regions to identify duplicated areas. Post-processing shifts vectors cluster matching blocks to precisely localize the source and forged regions.



Fig: Noise variance analysis

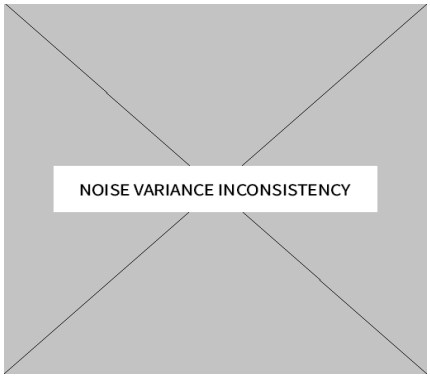


Fig: Noise variance analysed

Estimates local noise variance in image blocks using PCA or wavelet analysis to detect inconsistencies. Forged regions show significantly different noise levels from authentic areas due to post-processing artifacts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2



Fig: Metadata analysis

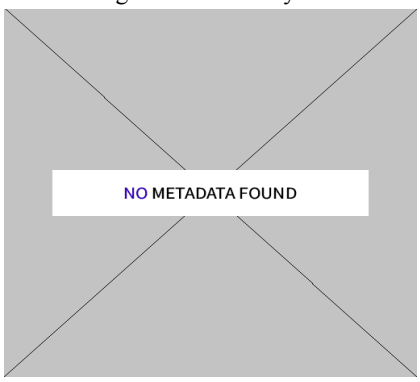


Fig: No Metadata

Extracts EXIF data (camera model, timestamp, GPS, Software tags) to detect tampering Inconsistencies. Edited images often show mismatched creation dates, editing software traces, or absent sensor fingerprints.

VIII. CONCLUSION

The Image Forgery Detection System developed in this project provides an efficient and reliable solution for identifying manipulated digital images using multiple forensic techniques.

By integrating methods such as Compression Detection, Metadata Analysis, CFA- Artifact Detection, Noise Inconsistency Analysis, Copy-Move Detection, and Error- Level Analysis into a single platform, the system ensures accurate and comprehensive verification of image authenticity.

The user-friendly interface makes the system easy to use, allowing users to upload images and obtain quick and clear results.

This project plays an important role in improving digital security and trust in various fields such as law enforcement, journalism, banking, education, and cybercrime investigation.

By detecting and localizing tampered regions and presenting visual evidence, the system increases the credibility of digital information. It also reduces the need for manual inspection, saves time, and minimizes human effort, making the verification process faster and more efficient.

REFERENCES

1. Image Forgery Detection: Survey and Future Directions KB Meena, V Tyagi - Data, Engineering and Applications: Volume 2, 2019 – Springer https://link.springer.com/chapter/10.1007/978-981-13-6351-1_14

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

2. Image Forgery Detection Using Deep Learning by Recompressing Images SSAli, II Ganapathi, NS Vu, SD Ali, N Saxena… - Electronics, 2022 - mdpi.com https://www.mdpi.com/2079-9292/11/3/403
3. Digital Image Forgery Detection with focus on a copy-move forgery detection survey S Gazzah, LR Haddada, I Shallal… - … on Cyberworlds (CW), 2023 - ieeexplore.ieee.org https://ieeexplore.ieee.org/abstract/document/10337571
4. Deepfake Detection Enhanced Model for Image Forgery Detection Combat Academic Misconduct survey J Ding, J Liu, J Shi, X Hu, X Qiao - 2024 11th International …, 2024 - ieeexplore.ieee.org https://ieeexplore.ieee.org/abstract/document/10780724
5. Image Forgery Detection: comprehensive review of Digital Forensics Approaches S Singh, R Kumaar – Journal of Computational Social Science, 2024 – Springer https://link.springer.com/article/10.1007/s42001-024-00265-8
6. Multi-approach survey and in-depth analysis of image forgery detection techniques: A. Bhowal et al. A Bhowal, R Naskar, S Neogy - The Visual Computer, 2025 – Springer https://link.springer.com/article/10.1007/s00371-025-0401