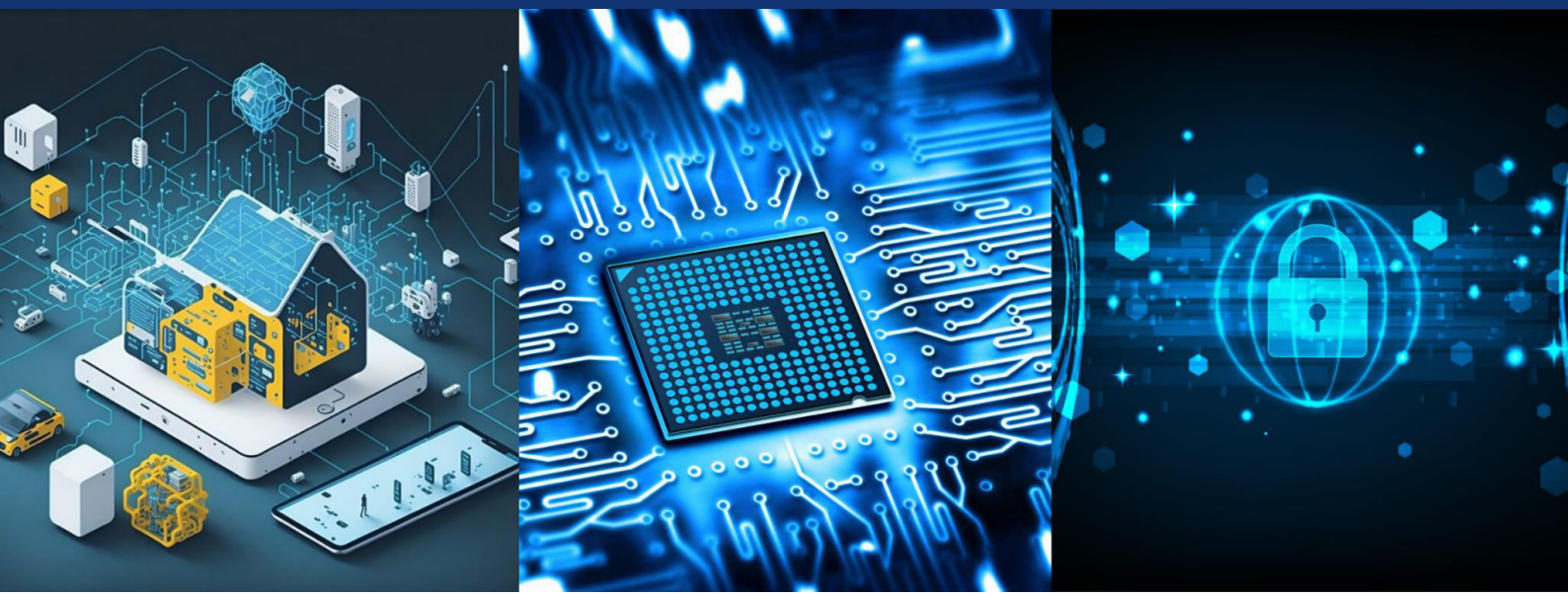
IJIRCCE

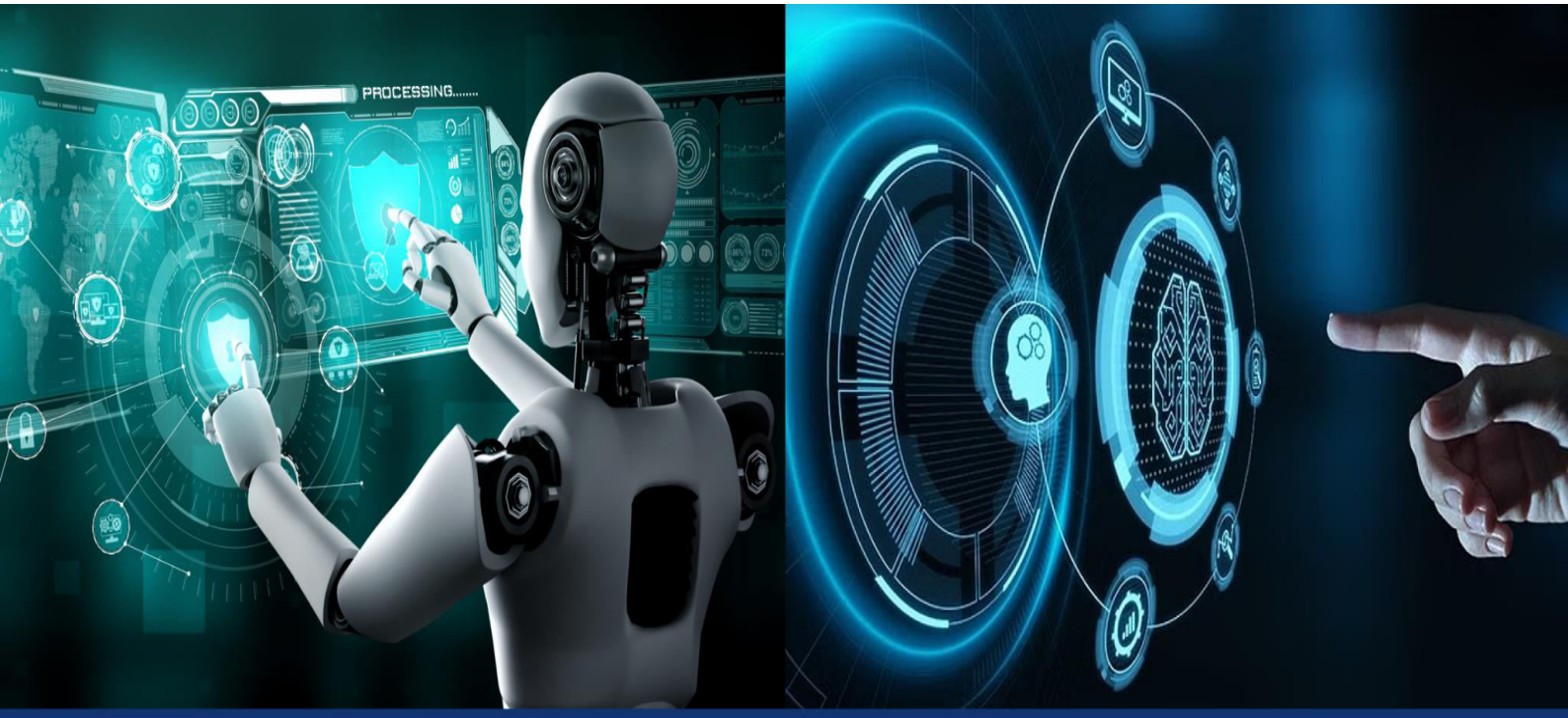
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407068

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Hybrid Forensic Framework for Robust Image Forgery Detection Using ELA, Histogram and Hash Analysis

Pasika Archana, Dr. M. Chandra Mohan

PG Student, Department of Computer Science and Engineering, University College of Engineering, Science and Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India

Professor, Department of Computer Science and Engineering, University College of Engineering, Science and Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India

ABSTRACT: A multi-level image forgery detection system is essential for identifying manipulation and tampering in digital images using advanced forensic techniques. This paper proposes a hybrid forensic framework that integrates three complementary approaches: Error Level Analysis (ELA), histogram feature inspection, and cryptographic hash comparison. ELA exposes subtle compression artifacts left by modifications, distinguishing altered regions from authentic image areas. Histogram analysis provides insight into intensity distribution changes, enabling detection of anomalous pixel patterns caused by editing, while hash analysis detects alterations by comparing the SHA-256 fingerprint of a suspected image with a trusted baseline. The system operates through a modular workflow in which each detection layer supplies corroborative evidence to a rule-based fusion engine, strengthening the overall reliability and precision of forgery identification. The framework is implemented as a Flask-based web application using Python, OpenCV, PIL, NumPy and Matplotlib, and is evaluated on sample images to demonstrate its ability to classify images as authentic or suspicious with interpretable, legally explainable evidence, without relying on computationally expensive machine learning models.

KEYWORDS: Image Forgery Detection; Error Level Analysis (ELA); Histogram Analysis; SHA-256 Hash Verification; Digital Image Forensics; Fusion Decision Engine

I. INTRODUCTION

The escalating misuse of manipulated digital media in judicial and public domains has made image authenticity verification a critical requirement in modern cyber forensics. As tampering techniques evolve, dependence on resource-heavy, black-box machine learning models is no longer viable for rapid, transparent investigations. There is a strong operational need for a lightweight, deterministic framework that can provide mathematically backed evidence suitable for forensic and investigative applications.

Existing image forgery detection systems mainly rely on single-level analysis methods or computationally expensive machine learning models. Techniques such as Error Level Analysis alone cannot accurately verify all types of image manipulation, while statistical methods may fail to identify localized tampering regions. In addition, AI-based systems require large datasets, high computational resources, and often produce non-interpretable results that are difficult to justify in forensic investigations. There is, therefore, a need for an integrated and lightweight forensic framework capable of detecting image forgery using visual analysis, statistical analysis, and cryptographic verification together.

The main objective of this work is to develop a hybrid forensic framework for robust image forgery detection using Error Level Analysis, Histogram Analysis and Hash Verification techniques. The system aims to identify manipulated regions, analyze abnormal pixel distribution patterns, and verify image integrity at the binary level. By combining visual, statistical, and cryptographic analysis methods, the framework improves detection accuracy, reduces false results, and provides reliable forensic evidence suitable for cybercrime investigations and digital authenticity verification.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The key contributions of this paper are summarized as follows:

• A lightweight, deterministic hybrid framework that fuses visual, statistical, and cryptographic evidence without relying on machine learning models.

• A rule-based fusion decision engine that combines the outputs of ELA, histogram, and hash analysis to reduce false positives and improve interpretability.

• A Flask-based web interface that enables non-expert users to upload images, view intermediate forensic outputs, and generate complete forensic reports.

• An experimental evaluation demonstrating the framework's ability to classify images as authentic or suspicious with explainable forensic evidence.

II. RELATED WORK

Digital image forgery detection has evolved significantly in response to the proliferation of advanced tampering tools. Contemporary literature extensively explores manipulation vectors such as image splicing, pixel retouching, and copy-move forgery. While early forensic methodologies isolated single variables, such as compression degradation or localized pixel anomalies, modern tampering techniques easily bypass these solitary analytical defenses.

Recent research has shifted heavily toward convolutional neural networks (CNNs) and automated feature extraction for artifact detection. Despite their theoretically high accuracy, these data-driven models introduce practical limitations, including extreme computational latency and strict hardware dependency. More critically, their lack of mathematical interpretability restricts their utility in formal forensic investigations, where legal evidence must be transparent and deterministic.

Consequently, classical deterministic techniques remain highly relevant when applied correctly. Error Level Analysis continues to effectively map differential compression artifacts left by localized modifications. Statistical histogram tracking successfully identifies unnatural intensity shifts introduced during pixel cloning, and cryptographic algorithms such as SHA-256 remain the global standard for establishing strict chain-of-custody protocols at the binary level. This work addresses the vulnerabilities of single-method detection by engineering a unified hybrid architecture that fuses visual artifact extraction, statistical pixel distribution analysis, and cryptographic hashing into a resilient, explainable, and resource-efficient alternative to contemporary AI-dependent models.

A closer examination of existing systems reveals several recurring limitations that motivate the proposed design. First, over-reliance on single-level analysis reduces overall detection reliability, since a system depending exclusively on either visual or statistical parameters remains vulnerable to manipulations that evade detection in that one domain. Second, machine learning and deep learning based methods demand large labeled datasets and substantial computational resources, which makes them unsuitable for lightweight, real-time forensic deployment. Third, visual-only detection techniques often fail against pixel-perfect retouching or subtle cloning, which bypass anomaly detection tools and require parallel statistical verification. Fourth, AI-driven models tend to produce non-interpretable, black-box outputs, which are difficult to justify in formal forensic and legal proceedings that require deterministic, mathematically grounded evidence. Finally, the absence of integrated cryptographic verification in many existing systems prevents investigators from establishing a secure chain of custody or detecting non-visual structural modifications. The hybrid framework proposed in this paper is designed specifically to overcome these five limitations by combining complementary, explainable analysis techniques within a single unified pipeline.

III. PROPOSED METHODOLOGY

The proposed system introduces a hybrid forensic framework for robust image forgery detection using Error Level Analysis, Histogram Analysis, and Hash Verification. Fig. 1 illustrates the overall system architecture. The user uploads a digital image through a Flask-based web interface, after which the image is passed to a preprocessing module for validation, resizing, format conversion, and metadata extraction. The preprocessed image is then simultaneously forwarded to the three forensic analysis modules, and their outputs are combined by a fusion decision engine to generate the final authenticity report.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407068

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

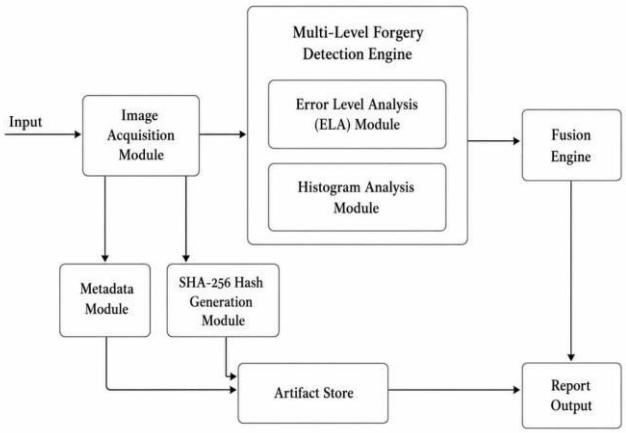


Fig. 1. System Architecture of the Proposed Hybrid Forensic Framework

Step 1 – Image Upload and Preprocessing: The suspected image is uploaded into the system and preprocessed for forensic analysis. Basic image information and metadata are extracted for further examination.

Step 2 – Error Level Analysis (ELA): The system recompresses the image at a predefined quality level and compares it with the original to identify compression inconsistencies and suspicious regions. Edited portions usually exhibit different compression characteristics than authentic regions. ELA is computed as

$$ELA = |I_{original} - I_{recompressed}| \quad (1)$$

where Ioriginal is the original image and Irecompressed is the recompressed version of the same image.

Step 3 – Histogram Analysis: Histogram analysis is performed on RGB and grayscale channels to identify abnormal pixel intensity distributions and statistical inconsistencies caused by image manipulation. The histogram is computed as

$$H(i) = \Sigma_x \Sigma_y \delta(I(x,y) - i) \quad (2)$$

where H(i) is the frequency of intensity level i, I(x,y) is the pixel intensity at position (x,y), and the summation is taken over all image dimensions.

Step 4 – Hash Verification: Cryptographic hash algorithms such as SHA-256 are used to verify image integrity at the binary level. Even a small modification in the image generates a completely different hash value:

$$Hash = SHA256(Image\ Data) \quad (3)$$

Step 5 – Fusion Decision Analysis: The outputs from the ELA, histogram, and hash verification modules are combined using rule-based decision logic to generate the final authenticity result and a detailed forensic analysis report.

IV. SYSTEM DESIGN

The internal design of the framework is further illustrated through its data flow, which traces how information moves between the user interface, processing modules, analysis engines, and report generation unit during execution. As shown in Fig. 2, the process begins with image upload, followed by preprocessing and the three parallel forensic analysis operations. The intermediate outputs are then merged by the fusion engine, which produces the final authenticity verification report delivered back to the user.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407068

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

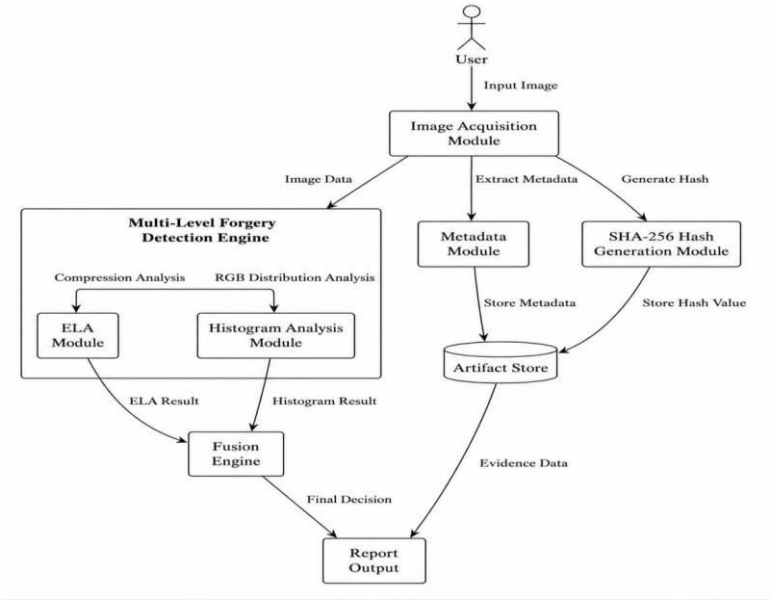


Fig. 2. Data Flow Diagram of the Proposed Framework

At the module level, the framework is organized into seven cooperating components: a user interface module that manages image upload requests; an image processing module that performs validation, resizing, and format conversion; an Error Level Analysis module; a Histogram Analysis module; a Hash Verification module; a metadata extraction module that scrapes EXIF information such as hardware signatures and software manipulation tags; and a report generation module that consolidates all outputs into a single forensic document. This modular decomposition keeps each analysis technique independent and individually testable, while the fusion engine provides the single point where their results are reconciled into one authenticity decision.

V. IMPLEMENTATION

The framework is implemented entirely in Python and deployed using the Flask web framework. OpenCV is used for low-level matrix manipulation, including pixel-stream reading and the dual-image subtraction required to generate ELA heatmaps. PIL performs controlled JPEG recompression to isolate compression artifacts. NumPy serves as the mathematical engine for processing high-dimensional image arrays and computing pixel intensity distributions, while Matplotlib renders the RGB and grayscale histogram graphs included in the final report. The hashlib module generates SHA-256 checksums for binary integrity validation, and ExifRead extracts embedded metadata such as hardware signatures and software manipulation tags. The system does not require a dedicated database; uploaded images, processed outputs, and generated reports are managed through lightweight file-based storage, which improves portability and execution efficiency.

Table 1 summarizes the hardware and software configuration used to develop and evaluate the framework. The minimal requirements confirm that the proposed system can be deployed on standard commodity hardware without specialized GPUs or cloud infrastructure, which is an important practical advantage over deep-learning-based forensic pipelines.

TABLE 1. System Requirements

Category	Specification
Processor	Intel Core i3 / i5 or higher
RAM	4 GB minimum (8 GB recommended)
Storage	20 GB or more
Operating System	Windows 10 / Linux Ubuntu
Programming Language	Python

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407068

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Web Framework	Flask
Core Libraries	OpenCV, PIL, NumPy, Matplotlib, hashlib, ExifRead
Development Tool	Visual Studio Code

VI. SYSTEM TESTING

System testing was carried out to validate whether the complete, integrated framework performs according to its specified requirements. Testing verified that the forensic modules correctly analyze suspected images, detect manipulations, and generate accurate forensic reports, and that the Flask-based web interface remains stable throughout the workflow.

Unit testing was performed independently on each module: the image upload module for successful upload and format validation; the preprocessing module for resizing, conversion, and metadata extraction; the ELA module for correct heatmap generation; the histogram module for RGB and grayscale graph generation; the hash verification module for correct SHA-256 computation; and the report generation module for complete report assembly.

Integration testing confirmed smooth interaction between all forensic modules, verifying that an uploaded image is processed through preprocessing, ELA, histogram analysis, hash verification, fusion analysis, and report generation without failure.

System and validation testing evaluated the complete framework end-to-end using multiple authentic and manipulated images of different formats and sizes. Manipulated images consistently produced visible ELA artifacts and abnormal histogram distributions, whereas authentic images produced consistent histogram distributions and minimal ELA inconsistencies, confirming that the forensic outputs align with the expected ground truth.

TABLE 2. Representative Test Cases

Test Case	Input	Expected Output	Result
Upload Image	Suspected image file	Image uploaded successfully	Pass
Preprocessing	Uploaded image	Metadata extracted successfully	Pass
ELA Analysis	Image file	ELA output generated	Pass
Histogram Analysis	Image file	RGB and grayscale histograms generated	Pass
Hash Verification	Image file	SHA-256 hash generated	Pass
Fusion Analysis	All forensic outputs	Correct authenticity classification	Pass
Report Generation	Forensic results	Detailed forensic report generated	Pass
Multiple Format Testing	JPG, PNG, BMP, TIFF images	Successful analysis for all formats	Pass

The testing process confirmed that the proposed framework meets its design objectives: Error Level Analysis effectively highlighted suspicious edited regions, histogram analysis identified abnormal pixel intensity distributions in forged images, SHA-256 hashing correctly verified image integrity, and the fusion decision engine accurately classified image authenticity while the web interface remained stable and responsive throughout analysis.

VII. RESULTS AND DISCUSSION

The proposed framework was evaluated by uploading suspected images through the web interface and examining the outputs generated by each forensic module. Fig. 3 shows a representative ELA output, in which brighter regions or abnormal patterns highlight areas with different compression characteristics that may indicate editing. Fig. 4 shows the corresponding RGB and grayscale histogram analysis, which is used to detect abnormal peaks, gaps, or inconsistent intensity distributions caused by tampering.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407068

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

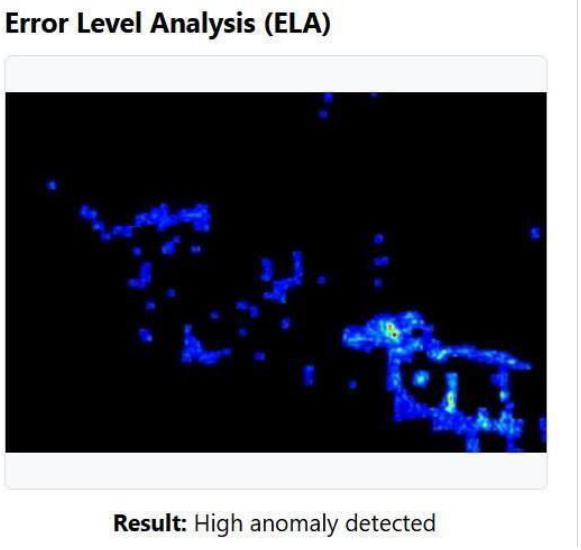


Fig. 3. Error Level Analysis (ELA) Output Highlighting Compression Inconsistencies

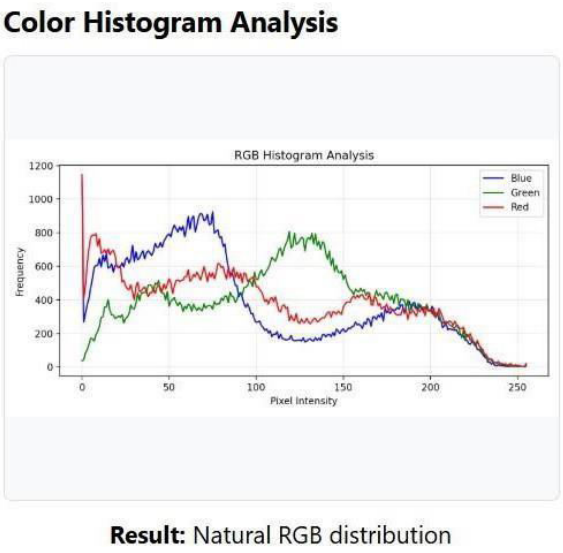


Fig. 4. RGB and Grayscale Histogram Analysis of the Uploaded Image

Table 3 summarizes the outcome of the fusion decision engine for two representative test images. In the first case, moderate ELA anomalies combined with a natural histogram distribution led the fusion engine to classify the image as suspicious, requiring further review, while retaining a unique SHA-256 fingerprint for future integrity checks. In the second case, uniform compression levels and a natural RGB distribution, together with the absence of significant anomalies, led the system to classify the image as authentic. These results demonstrate that combining visual, statistical, and cryptographic evidence through a rule-based fusion engine produces more reliable and interpretable conclusions than any single forensic technique used in isolation.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407068

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

TABLE 3. Fusion Decision Outcomes for Representative Test Images

Test Image	ELA Observation	Histogram Observation	Hash Verification	Final Classification
Sample 1	Moderate compression anomalies in localized regions	Natural RGB distribution retained	Unique SHA-256 fingerprint generated	Suspicious – further review required
Sample 2	Uniform compression, no abnormal regions	Natural RGB distribution, no irregular peaks	Unique SHA-256 fingerprint generated	Authentic – no forgery detected

Fig. 5 shows a sample final forensic report generated by the system. The generated report consolidates metadata information, ELA outputs, histogram graphs, hash values, and the final authenticity conclusion into a single document, making the framework directly usable for forensic investigations and digital evidence documentation. Because the system relies on deterministic, mathematically grounded techniques rather than opaque machine learning models, every classification produced by the framework can be traced back to an explainable analytical basis, which is essential for legal and investigative acceptance.

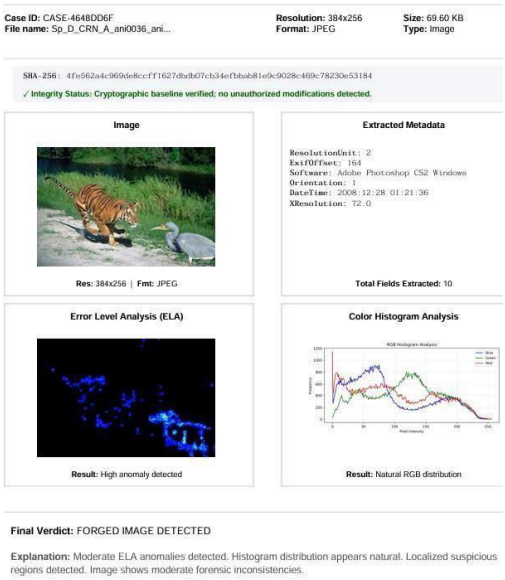


Fig. 5. Sample Final Forensic Investigation Report

Overall, the experimental evaluation and system testing results confirm that the hybrid framework is efficient, reliable, and suitable for practical forensic investigation applications, while remaining lightweight enough to run on standard commodity hardware without specialized GPUs or cloud infrastructure.

VIII. CONCLUSION AND FUTURE WORK

This paper presented a hybrid forensic framework for robust image forgery detection that integrates Error Level Analysis, Histogram Analysis, and SHA-256 Hash Verification through a rule-based fusion engine. Unlike single-method or machine-learning-based approaches, the proposed framework combines visual, statistical, and cryptographic evidence to deliver accurate, lightweight, and explainable forgery detection suitable for cybercrime investigations and digital authenticity verification. The Flask-based web interface allows users to upload images, view intermediate forensic outputs, and download complete investigation reports without requiring specialized technical expertise. System testing confirmed that all forensic modules operate correctly both independently and as an integrated pipeline, and the experimental evaluation showed that the fusion engine produces reliable, explainable authenticity classifications.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

While the framework performs effectively in its current form, several directions can further extend its capabilities:

• **Integration with Artificial Intelligence and Deep Learning:** Convolutional Neural Networks and deep learning-based forensic models can be incorporated for automatic feature extraction and detection of sophisticated manipulations such as deepfakes and AI-generated synthetic images.

• **Real-Time Forgery Detection:** The framework can be extended to analyze images instantly during upload, social media sharing, or live surveillance operations rather than only offline.

• **Extension to Video Forgery Detection:** The methodology can be applied to individual video frames to detect temporal inconsistencies, enabling detection of manipulated videos and deepfake multimedia content.

• **Cloud-Based Forensic Platform:** Deploying the system as a cloud-based service would allow remote users to submit images for automated forensic analysis and report generation, improving scalability and accessibility.

• **Blockchain-Based Evidence Integrity:** Blockchain technology can be integrated to securely store forensic reports, image hashes, and metadata, ensuring tamper-proof evidence preservation and chain-of-custody records for legal investigations.

• **Mobile Application Development:** A mobile forensic application would allow field investigators and journalists to analyze suspicious images directly from smartphones and tablets.

• **Advanced Metadata and Geolocation Analysis:** EXIF inconsistency detection, GPS verification, camera fingerprint analysis, and timestamp validation can strengthen forensic authenticity verification.

• **Automated Forensic Decision Support:** The fusion engine can be enhanced with intelligent scoring and probabilistic models to provide confidence levels alongside automated forensic recommendations for investigators.

REFERENCES

[1] Dubey Krishna Pradeep, Gupta Sejal Kailash, Patil Viraj Kunjan and Meet Chudasama, “Image Forgery Detection with ELA,” International Journal of Research Publication and Reviews, Vol. 5, No. 3, pp. 1400–1406, March 2024.

[2] H. Farid, “Image Forgery Detection: A Survey,” IEEE Signal Processing Magazine, Vol. 26, No. 2, 2009. DOI: 10.1109/MSP.2008.931079.

[3] Adarsh N and H. P. Mohan Kumar, “Error Level Analysis in Image Forgery Detection,” IRJET, Vol. 10, Issue 7, July 2023.

[4] R. Idlbek, M. Pešić and K. Šolić, “Enhancing Digital Image Forensics with Error Level Analysis (ELA),” 47th MIPRO ICT and Electronics Convention (MIPRO), IEEE, 2024.

[5] G. Batista, J. Welligton, M. Alves, W. Junior and H. Kuribayashi, “Recent Advances in Digital Image Forgery Detection: A Systematic Mapping Study,” IEEE Access, 2026.

[6] S. Chandana, C. R. Nagarathna, A. Amrutha and A. Jayasri, “Detection of Image Forgery using Error Level Analysis,” 2nd International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (ICIITCEE), IEEE, 2024.

[7] A. H. Khalil, A. Z. Ghalwash, H. A. Elsayed, G. I. Salama and H. A. Ghalwash, “Enhancing Digital Image Forgery Detection Using Transfer Learning,” IEEE Access, Vol. 11, pp. 91583–91594, 2023.

[8] S. S. Ali, I. I. Ganapathi, N. S. Vu, S. D. Ali and N. Saxena, “Image Forgery Detection Using Deep Learning by Recompressing Images,” IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 448–463, 2022.

[9] E. U. H. Qazi, T. Zia and A. Almorjan, “Deep Learning-Based Digital Image Forgery Detection System,” Applied Sciences, Vol. 12, No. 6, p. 2851, 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details