International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Image Forgery Detection Using Hybrid Deep Learning

Dhinakaran R[1] , Hari K[2], Hemanth V[3], Vijayalakshmi R[4]

[1,2,3]Bachelor of Engineering in Computer Science and Engineering Adhiyamaan College of Engineering (An Autonomous Institution) Anna University, Chennai
[4]Assistant Professor, Department of CSE, Adhiyamaan College of Engineering (An Autonomous Institution) Anna University, Chennai

ABSTRACT
Digital image forgery has become increasingly sophisticated with the advancement of image editing tools and AI-based generative models. Detecting such manipulations is critical for applications in digital forensics, journalism, and legal investigations. This paper presents **DeepScan**, a hybrid image forgery detection system that integrates classical forensic techniques with deep learning to improve accuracy, robustness, and explainability. The system employs Error Level Analysis (ELA) and Photo Response Non-Uniformity (PRNU) noise profiling to capture compression and sensor inconsistencies, while a Convolutional Neural Network (CNN) performs multi-class classification of images into Authentic, Forged, and AI-Generated categories. A fusion decision engine combines outputs from both analysis paths to generate a final verdict with confidence. Additionally, Grad-CAM is used to provide visual explanations through heatmaps, and SHA-256 hashing ensures forensic integrity. Experimental results demonstrate that the hybrid approach outperforms standalone methods, achieving improved accuracy and reliability. DeepScan provides a transparent, explainable, and practical solution for modern image forgery detection.

KEYWORDS: Image Forgery Detection, CNN, Grad-CAM, ELA, PRNU, Explainable AI, Digital Forensics, Deep Learning

1. INTRODUCTION (Shortened for journal)

With the rapid growth of digital media, images are widely used in communication, journalism, and legal systems. However, advancements in image editing tools and AI-based generative models have made it increasingly easy to create realistic forged images. These manipulated images can spread misinformation, mislead investigations, and compromise trust in digital content.

Traditional image forgery detection methods rely on handcrafted features such as noise patterns, compression artifacts, and edge inconsistencies. While effective to some extent, these methods fail when dealing with advanced manipulations and AI-generated content. On the other hand, deep learning models offer improved accuracy but often lack interpretability, making them unsuitable for forensic applications.

To address these limitations, this paper proposes **DeepScan**, a hybrid system combining forensic techniques and deep learning with Explainable AI. The system not only detects forgery but also explains the reasoning behind its decisions, ensuring transparency and reliability.

2. RELATED WORK

Recent research in image forgery detection has focused on deep learning and hybrid approaches. CNN-based methods have achieved high accuracy by learning complex patterns in manipulated images. However, studies have shown that deep learning models are vulnerable to adversarial attacks and lack interpretability.

Classical forensic methods such as Error Level Analysis and PRNU remain useful for detecting compression inconsistencies and sensor noise patterns. Additionally, Explainable AI techniques such as Grad-CAM have been introduced to improve model transparency.

Hybrid approaches combining forensic and deep learning techniques have demonstrated improved performance and robustness. This work builds upon these approaches by integrating multiple detection methods into a unified system.

3. PROPOSED METHODOLOGY

3.1 System Overview

DeepScan follows a hybrid architecture combining forensic analysis and deep learning. The system processes an input image through multiple stages, including preprocessing, forensic analysis, CNN classification, and decision fusion.

3.2 Forensic Analysis

- **Error Level Analysis (ELA):** Detects compression inconsistencies
- **PRNU Noise Analysis:** Identifies sensor noise variations

3.3 CNN-Based Classification

A CNN model (EfficientNet-based) is used to classify images into:

- Authentic
- Forged
- AI-Generated

3.4 Explainable AI (Grad-CAM)

Grad-CAM generates heatmaps highlighting regions influencing the model's decision.

3.5 Fusion Decision Engine

Combines forensic and CNN outputs to improve accuracy and reduce false positives.

3.6 Evidence Integrity

SHA-256 hashing is used to ensure image authenticity and chain-of-custody.

4. IMPLEMENTATION

The system is implemented using:

- **Backend:** Python, Flask / FastAPI
- **Frontend:** React, HTML, CSS
- **Libraries:** TensorFlow, OpenCV, NumPy

The application supports real-time image upload and analysis with visual and textual outputs.

5. RESULTS AND DISCUSSION

The system was tested on multiple image categories including authentic images, spliced images, copy-move forgeries, and AI-generated images.

- Achieved **~93% accuracy**

- Hybrid model outperformed CNN-only model
- Grad-CAM improved interpretability
- PRNU + ELA improved detection reliability

Real-world validation showed effectiveness in:

- Journalism verification
- Legal evidence analysis
- AI-generated image detection

6. CONCLUSION

This paper presented DeepScan, a hybrid image forgery detection system combining forensic techniques and deep learning with Explainable AI. The system improves accuracy, reliability, and transparency compared to traditional methods. The integration of Grad-CAM and SHA-256 hashing makes it suitable for forensic applications.

7. FUTURE WORK

- Video deepfake detection
- Mobile application
- Diffusion model detection improvement
- Browser extension for real-time detection