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 1, March 2026
Impact Factor: 8.2

Image Forgery Detection System

Ms. Krutika Suryawanshi[1], Mr. Borade Sarthak Sandeep[2], Mr. Jadhav Harshal Shivaji[3]
Ms. Kakulte Khushi Vijay[4], Ms. Sabale Sakshi Chintaman[5]
Lecturer, Department of Artificial Intelligence & Machine Learning[1]
Student, Department of Artificial Intelligence & Machine Learning[2,3,4,5]
Mahavir Polytechnic, Nashik, Maharashtra, India

Abstract: *Image forgery has become a serious issue with the rapid growth of digital media and image editing tools. Manipulated images are often used in fake news, digital fraud, and misinformation, making image authenticity verification extremely important. This paper presents an Image Forgery Detection System based on Artificial Intelligence and Deep Learning techniques that automatically identifies whether a digital image is real or tampered.*

The proposed system uses Error Level Analysis (ELA) to detect compression inconsistencies in images caused by editing or manipulation. A Convolutional Neural Network (CNN) model analyzes these ELA images and classifies them into real or tampered categories. The system provides fast, accurate results along with a confidence score through a user- friendly web interface.

Experimental results show that the system achieves high accuracy in detecting forged images and reduces the need for manual inspection. Overall, the proposed solution is efficient, scalable, and useful for applications such as digital forensics, media verification, and fraud detection.

Keywords: Image Forgery Detection, Deep Learning, Error Level Analysis, Computer Vision, Digital Forensics, CNN

I. INTRODUCTION

With the widespread availability of image editing software, digital images can be easily modified without leaving visible traces. Such manipulated images are frequently used in social media, journalism, legal evidence, and online transactions, leading to serious trust and security issues. As a result, verifying the authenticity of digital images has become an important research area.

Traditional methods of image verification rely on manual inspection or basic image processing techniques, which are time-consuming and often unreliable. Human observation may fail to detect subtle manipulations, especially when tampering is performed skillfully.

To address these challenges, this project presents an Image Forgery Detection System using machine learning and deep learning techniques. The system automatically analyzes uploaded images using Error Level Analysis (ELA) and a deep learning model to determine whether the image is real or tampered. This automated approach improves accuracy, reduces human effort, and enables fast image verification.

II. LITERATURE SURVEY

Several researchers have proposed methods for detecting image forgery using image processing and machine learning techniques. Early approaches focused on detecting inconsistencies using pixel-based analysis, color filters, and edge detection methods. While these methods provided basic forgery detection, they were sensitive to noise and lighting variations.

Researchers have also explored Error Level Analysis (ELA) for detecting image manipulation by identifying different compression levels within an image. ELA-based methods are effective in detecting edited regions but require strong classification techniques for reliable results.

DOI: 10.48175/IJARSCT-31415

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 1, March 2026 Impact Factor: 8.2

Recent studies have shown that Deep Learning models, especially Convolutional Neural Networks (CNNs), provide better accuracy by automatically extracting features from images. Datasets such as CASIA 2.0 have been widely used to train and evaluate forgery detection models. However, many existing systems lack real-time usability or user-friendly interfaces.

The proposed system builds upon these research works by combining ELA with a powerful CNN architecture and a web- based interface for practical and efficient image forgery detection.

III. PROBLEM OF STATEMENT

In the current digital era, it is difficult to verify whether an image is authentic or manipulated due to advanced editing tools. Manual inspection is unreliable and requires expert knowledge. Existing automated solutions often lack accuracy, scalability, or real-time response.

There is a need for an intelligent system that can automatically analyze digital images, detect forgery with high accuracy, and provide fast and reliable results without human intervention. The system should also be easy to use and suitable for real-world applications such as media verification and fraud prevention.

IV. EXISTING PROBLEM

Existing image forgery detection systems mainly rely on traditional image processing techniques such as edge detection, noise analysis, and color inconsistencies. Some systems use machine learning algorithms like SVM or KNN, which require manual feature extraction and offer limited performance.

These systems often struggle with different image formats, compression levels, and complex manipulations. Many solutions also lack a proper user interface and do not provide confidence scores or detailed results. As a result, they are less effective for large-scale or real-time image verification.

V. PROPOSED SYSTEM

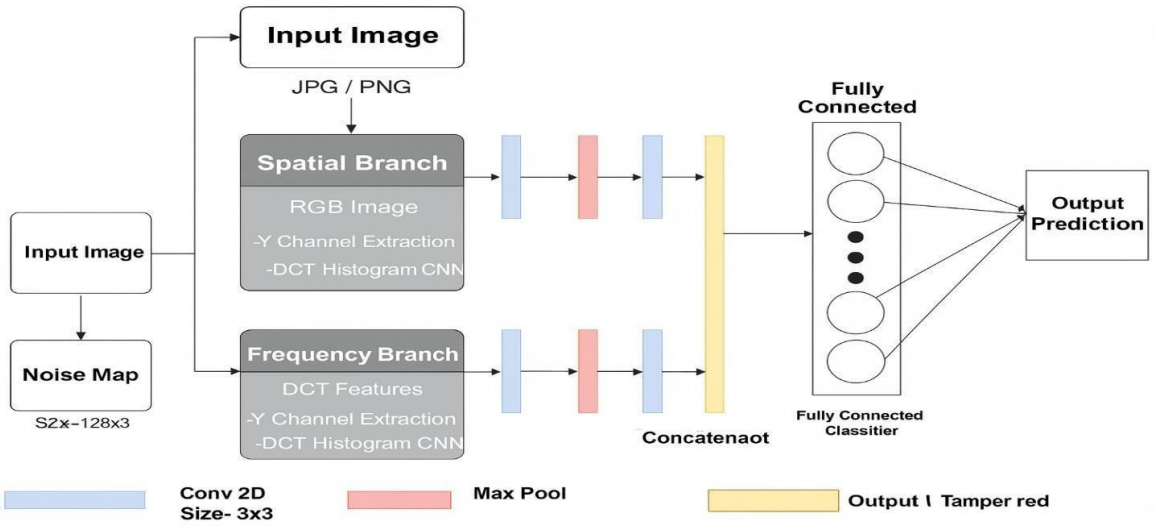


Image Forgery Detection Architecture Diagram

Step-by-step explanation :

1. Start

The process begins when the Image Forgery Detection System is launched by the user.

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 1, March 2026
Impact Factor: 8.2

2. Select Input

The user selects how to provide the image for verification :

• Upload Image: Upload a single image in JPG or PNG format.

• Camera Image (optional) : Capture an image using a camera for real – time analysis.

3. Load Input Image

The selected image is loaded into the system.

The system also generates a noise map from the input image to highlight hidden inconsistencies caused by editing or manipulation.

4. Image Preprocessing

Before analysis, the image undergoes preprocessing steps to make it suitable for the AI Model:

• Resizing: The image is resized to a fixed dimension required by the model.

• Normalization : Pixel values are normalized for better learning.

• Y-Channel Extraction: The luminance (Y) channel is extracted as it is more sensitive to tampering.

5. Spatial Branch Analysis

The preprocessed image is passed through the Spatial Branch, which analyzes pixel-level information:

• RGB image feature are extracted.

• DCT histogram feature are generated.

• Convolution (Conv2D) and Max Pooling layers extract important spatial patterns related to forgery.

6. Frequency Branch Analysis

At the same time, the image is processed in the Frequency Branch:

• DCT features are extracted from the image.

• DCT features are extracted from the image.

• CNN layers learn frequency-domain forgery traces.

7. Feature Concatenation

The feature extracted from:

• Spatial Branch

• Frequency Branch

Are combined (concatenated) into a single feature vector for final classification.

8. Classification

The combined features are passed to a Fully Connected Neural Network:

• The classifier analyzes both spatial and frequency features.

• The system performs binary classification.

9. Generate Results

The final output is generated:

• Real Image – Image is authentic

• Tampered Image – Image has been manipulated

• A confidence score is also displayed for better understanding.

IV. CONCLUSION

The proposed Image Forgery Detection System provides an effective and automated solution for identifying tampered images using Error Level Analysis and Deep Learning. By analyzing compression inconsistencies and using a CNN-based model, the system accurately classifies images as real or tampered.

The web-based interface allows users to upload images easily and view results instantly along with confidence scores. The system reduces manual effort, improves reliability, and can be deployed as a desktop application, web application, or cloud-based service.

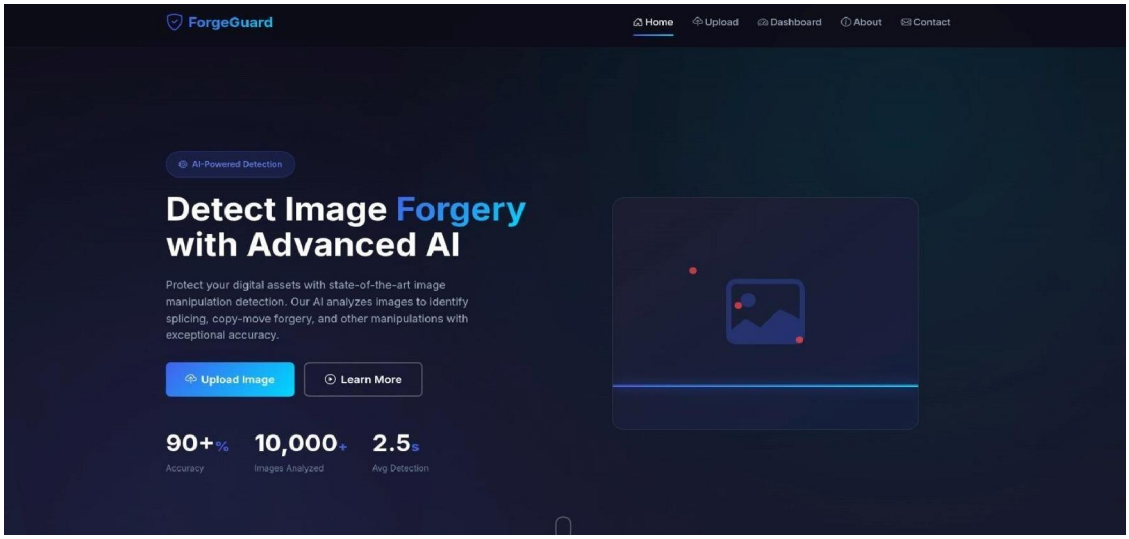
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, March 2026
Impact Factor: 8.2

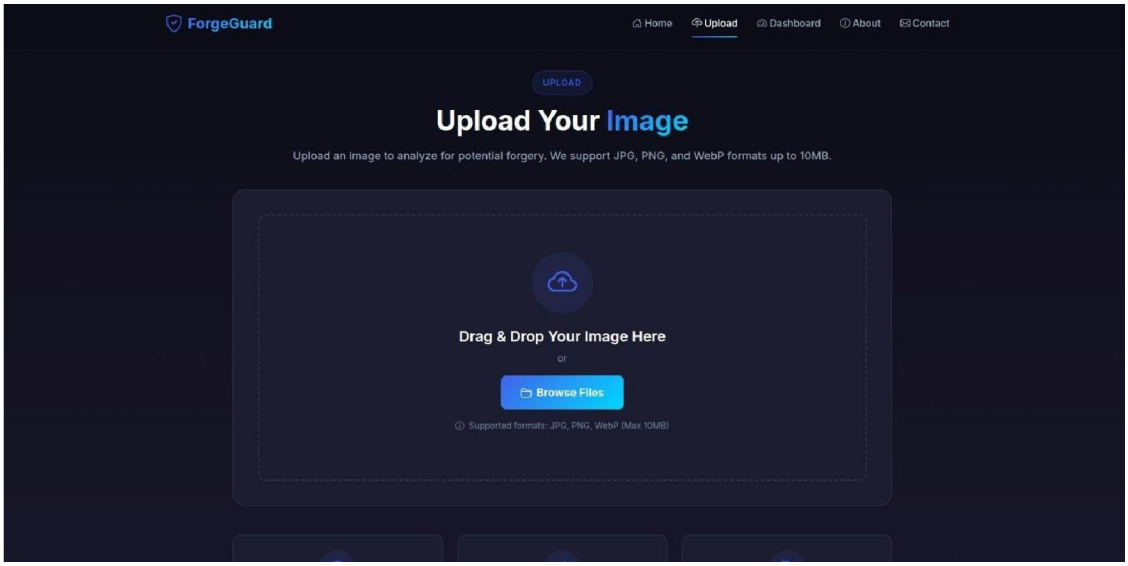
Overall, this project demonstrates the practical use of AI and computer vision in digital forensics and content verification, making it a valuable tool for fraud detection and media authenticity verification.

V. ACKNOWLEDGMENT

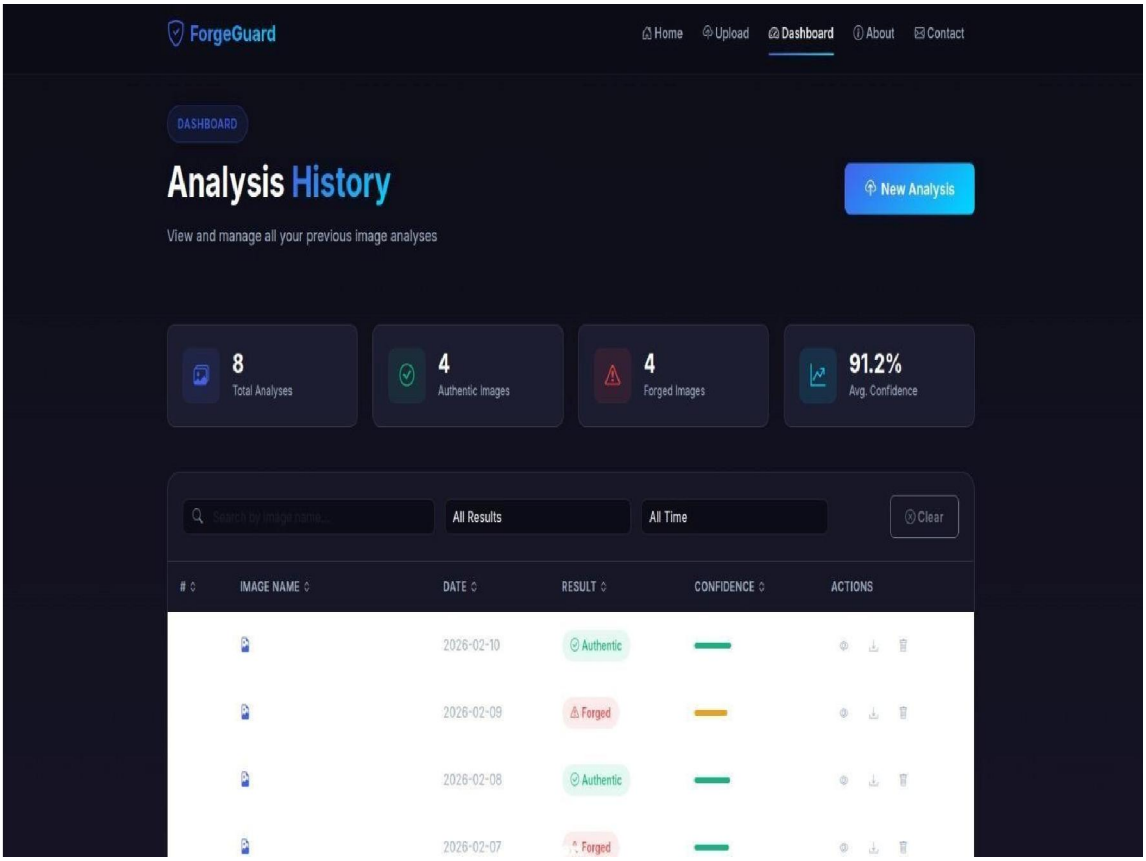
I would like to express my sincere gratitude to our project guide for their continuous guidance, support, and valuable suggestions throughout the development of the Image Forgery Detection System. Their technical insights helped improve the accuracy and performance of the system. I am also thankful to my institution for providing the necessary infrastructure and resources. Finally, I would like to thank my peers who contributed through testing and feedback, which played an important role in the successful completion of this project.

VI. OUTPUT





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 1, March 2026
Impact Factor: 8.2



REFERENCES

[1]. J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy–move forgery in digital images," Proceedings of Digital Forensic Research Workshop, Cleveland, OH, USA, 2003.
[2]. H. Farid, "Image forgery detection," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, 2009.
[3]. T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1003–1017, 2012.
[4]. J. Dong, W. Wang, and T. Tan, "CASIA Image Tampering Detection Evaluation Database," IEEE China Summit & International Conference on Signal and Information Processing, 2013.
[5]. Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," IEEE International Workshop on Information Forensics and Security (WIFS), 2016.
[6]. G. H. Chen, M. Wu, and Y. Q. Shi, "Detecting image splicing based on noise level inconsistencies," IEEE International Conference on Multimedia and Expo, 2007.
[7]. G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely Connected Convolutional Networks," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.
[8]. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, 2011.
[9]. M. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," ACM Workshop on Information Hiding and Multimedia Security, 2016.