



## **EDITED IMAGE DETECTION AND RESTORATION**

Dinesh R Bhagwat<sup>1</sup>, Sandeep<sup>2</sup>, Shobhith<sup>3</sup>, Shodhan<sup>4</sup>, Vikas S G<sup>5</sup>

Campus Technology Officer, Dept. of Computer Science & Engineering, Mangalore Institute of Technology & Engineering, Moodabidri, India<sup>1</sup>,

Student, Dept. of Computer Science & Engineering, Mangalore Institute of Technology & Engineering, Moodabidri, India<sup>2,3,4,5</sup>

*Abstract:* Edited image detection and restoration are crucial in various fields such as digital forensics, media integrity, and security. Edited image detection helps identify manipulated or tampered images, ensuring the authenticity of visual content, which is vital for preventing misinformation, fraud, and mistrust in media. Restoration aims to recover or reconstruct images that have been altered, either for forensic purposes. The provided code implements a deep learning pipeline for detecting manipulated images using Error Level Analysis (ELA). It preprocesses images by generating ELA maps to highlight manipulation traces. A custom dataset class loads ELA images and corresponding ground truth masks, applying necessary transformations. The model, based on a pre-trained ResNeXt-50, is fine-tuned to predict manipulation maps. The training function handles loss computation and parameter updates using batches of images and masks. Finally, the trained model is saved for future use in detecting image manipulations.

**Index Terms - Image Manipulation, Media Integrity, Tampered Image, Image Restoration etc.**

### **I. INTRODUCTION**

The rise in image manipulation has led to misinformation and authenticity issues across digital platforms. An automated solution for detecting and restoring edited images can significantly reduce the propagation of false information. With the growing use of image editing software, the detection of tampered images has become critical in various fields, including forensics, journalism, and digital content verification. Traditional methods often fail to keep up with the sophistication of modern editing techniques, making automated detection essential. This project aims to bridge the gap by developing an advanced system for detecting edited images using deep learning models and restoring them to their probable original form. This will enhance the reliability of digital images in sensitive applications.

## II. LITERATURE SURVEY

[1] The task of detecting whether an image has been tampered with involves analyzing inconsistencies in the image's properties. Early techniques focused on digital forensics, using pixel-level analysis to detect irregularities in lighting, noise, or compression artifacts. Farid (2009) explored noise pattern analysis as a method to identify edited regions in an image, as image modifications often disrupt the natural noise present in photographs.

[2] Convolutional Neural Networks (CNNs) have been widely applied for forgery detection, as they can automatically learn features related to image tampering without explicit programming. Zhou et al. (2018) proposed a two-stream CNN architecture, where one stream focuses on spatial information and the other on noise inconsistencies to identify manipulated regions.

[3] Restoration of edited images is a complementary problem, aiming to recover the original, unaltered image or reconstruct the missing or tampered parts. Traditional methods focused on inpainting techniques, where the damaged or altered parts of an image are filled using surrounding pixel information. Early approaches by Bertalmio et al. (2000) used partial differential equations (PDE) to propagate known image information into unknown regions, producing visually plausible results.

## III. SCOPE AND METHODOLOGY

### Scope

The goal of edited image detection is to identify manipulated areas within an image. This task is critical for applications like forensic analysis, fake news detection, and image authentication. Detecting tampered regions helps to verify the integrity of visual media, ensuring that they have not been altered without proper disclosure. Once an edited image is detected, restoration focuses on correcting the tampered areas to recover the original state or a plausible approximation of the unaltered image. This is crucial in cases where the goal is not only to detect but also to repair tampered or degraded images.

### Methodology

The methodology for edited image detection and restoration begins with image preprocessing to prepare the image for analysis. This involves loading and standardizing the image, followed by techniques like Error Level Analysis (ELA), where the image is compressed at a lower quality and the difference between the original and compressed images is computed. High discrepancies in the compression levels often indicate manipulations like object insertion, splicing, or cloning. Additionally, deep learning models like CNNs are used for feature extraction, whereas pre-trained models like ResNeXt can capture spatial and semantic features of the image, helping to identify manipulated regions.

Once the image is preprocessed, feature extraction is performed using deep learning models. Convolutional neural networks (CNNs), especially those pre-trained on large datasets (e.g., ImageNet), can be fine-tuned for the specific task of edited image detection. These models can learn to distinguish between authentic and manipulated areas by detecting anomalies in pixel relationships. For more localized detection, segmentation models like U-Net can be used to generate masks indicating which regions have been edited, while classification models can determine if the entire image is tampered.

After detecting the manipulated areas, restoration begins by identifying the regions requiring correction. This can be done using the output of the detection step, which provides masks or bounding boxes around the tampered regions. Once these areas are identified, image inpainting techniques are applied to fill in the missing or altered parts. Traditional methods like patch-based or exemplar-based inpainting rely on neighboring regions to restore missing pixels.

The final step involves post-processing and evaluation of the restoration results. This includes cleaning up any noise in the segmentation masks and refining the restored image to ensure smooth integration of the in-painted areas. The restored image is then evaluated for visual realism, consistency with surrounding context, and semantic accuracy. Both detection and restoration models may be iteratively refined and trained on large

datasets to improve their effectiveness, especially in handling complex manipulations like deepfakes or splicing, which require more sophisticated algorithms to detect and restore.

#### IV. SYSTEM ARCHITECTURE

The System Architecture for Edited Image Detection and Restoration consists of several interdependent modules designed to identify and restore manipulated images. The process begins with the image input, where an image, typically in formats such as JPEG or PNG, is fed into the system. The image is then passed through a preprocessing stage, which includes resizing, normalization, and the application of Error Level Analysis (ELA). ELA highlights differences between the original and compressed versions of the image, which can reveal discrepancies indicating potential manipulation. The output of this stage provides a modified image that can be used for further analysis.

Next, the Edited Image Detection module leverages deep learning models to identify altered areas. Convolutional Neural Networks (CNNs) or pre-trained models like ResNet or VGG are used to extract deep features from the image, which are crucial for identifying manipulated regions. Segmentation networks such as U-Net can be employed to generate pixel-level masks that identify tampered areas, or a classification model can determine if the entire image has been edited. The ELA map is also integrated into this process to enhance detection by focusing on regions with high error levels.

Once manipulations are detected, the system moves to the Restoration phase. In this step, the tampered regions identified by the detection model are restored using inpainting techniques. These can include traditional methods like patch-based or exemplar-based inpainting, which fills in missing pixels from surrounding areas, or more advanced deep learning models. The inpainting results in a more realistic restoration of the image, making it appear less altered.

Finally, the Post-Processing stage refines the restored image. This includes smoothing out any rough edges in the in-painted regions and ensuring that the restored parts blend seamlessly with the surrounding content. Further refinement may involve mask cleaning

using morphological operations or additional adjustments to improve the visual quality. The resulting restored image is then evaluated for visual fidelity, with metrics such as SSIM (Structural Similarity Index) or PSNR (Peak Signal-to-Noise Ratio) used to assess the quality of restoration. The system architecture ensures that each stage works in tandem to accurately detect manipulations and restore altered content effectively.

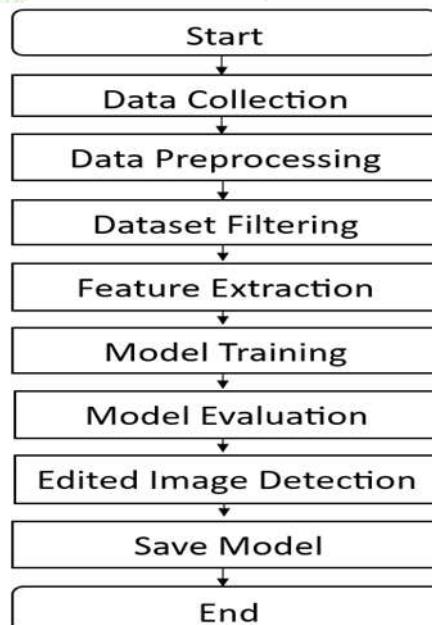


Figure 4.1: System Architecture

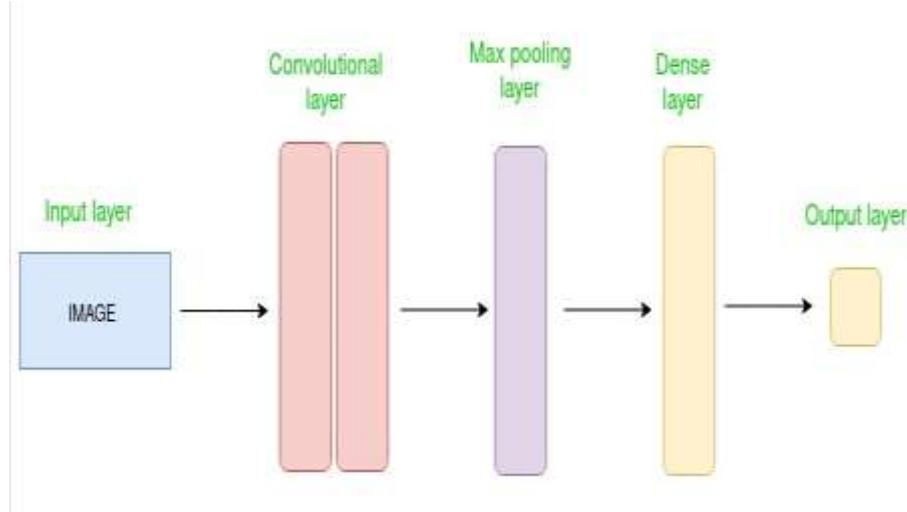


Figure 4.2: CNN Architecture

## V. CONCLUSION

In conclusion, edited image detection and restoration is a crucial area in digital forensics, media verification, and maintaining content authenticity. By combining advanced techniques such as Error Level Analysis (ELA), deep learning models like Convolutional Neural Networks (CNNs) this process allows for both the accurate identification of image manipulations and the restoration of tampered content. The detection phase focuses on highlighting suspicious regions through deep feature extraction and segmentation, while the restoration phase leverages inpainting methods to reconstruct manipulated areas realistically.

With the increasing sophistication of image editing tools, this methodology offers a robust approach to ensuring that digital content remains trustworthy. The system's ability to seamlessly integrate detection and restoration provides a comprehensive solution, addressing the challenges posed by digital image manipulation. As the technology continues to evolve, the integration of more advanced models and improved algorithms will further enhance the accuracy, efficiency, and effectiveness of these systems in preserving the integrity of digital images.

## REFERENCES

- [1] "Deep-Learning-Based on Digital Forensics Network for Image Forgery Detection" David Fischinger, Martin Boyer (2023), IMVIP-The 25th Irish Machine Vision and Image Processing conference.
- [2] "Casis image tampering detection evaluation database" by Dong J, Wang W and Tan T (2013). In IEEE China Summit Inter Conf. Signal Info Proc IEEE.
- [3] "Ransomware detection using machine learning" based on review, research limitations and future directions JAMIL ISPAHANY (Graduate Student Member, IEEE), MD RAFIQUL ISLAM (Senior Member, IEEE), MD ZAHIDUL ISLAM (Senior Member, IEEE) and M. ARIF KHAN (Senior Member, IEEE).