Image Forgery Detection Using Transfer Learning

Name :- Abbas Asif Tisekar
Mail-id:-abbastisekar27@gmail.com
Department of Computer Engineering

Name :- Mahesh Ratnakar Yewate
Mail-id:-maheshyewate2020@gmail.com
Department of Computer Engineering

Name :- Prajakta Prakash Hande
Mail-id:-prajaktahande713@gmail.com
Department of Computer Engineering

Name :- Dnyanashree Kishor Palve
Mail id:- dnyanashreepalve2533@gmail.com
Department of Computer Engineering

Guide Name: Prof. Apeksha Pande

SIDDHANT COLLEGE OF ENGINEERING SUDUMBARE, TAL- MAVAL DIST-PUNE – 412109.

---***---

Abstract: The increasing prevalence of image manipulation technologies has raised significant concerns about the authenticity of digital media, making image forgery detection an essential task in various fields such as digital forensics, media verification, and legal investigations. Despite the advances in image manipulation techniques, detecting forgeries remains a challenging problem due to the sophisticated nature of modern editing tools. In this research, we address this challenge by combining traditional image analysis methods with state-of-the-art deep learning techniques to improve the accuracy and robustness of forgery detection systems. Specifically, we propose a hybrid approach that integrates the Error Level Analysis (ELA) method with transfer learning.

The ELA method, a well-known image forgery detection technique, helps identify inconsistencies in error levels across different regions of an image, which is a characteristic of tampered images. However, traditional ELA methods may struggle to detect advanced forgeries, particularly those made with modern editing software. To overcome these limitations, we employ transfer learning by fine-tuning pre-trained convolutional neural networks (CNNs) on the CoMoFoD and CASIA datasets. These datasets are widely used in the domain of image forgery detection, containing both genuine and tampered images. By leveraging the power of transfer learning, we can enhance the detection capabilities of the model, allowing it to learn from large-scale, real-world datasets and detect subtle forgery traces that might be overlooked by classical methods.

Our experimental results show that the hybrid approach significantly outperforms traditional ELA techniques, with notable improvements in detection accuracy and robustness. The model achieved higher precision, recall, and F1-score when compared to baseline methods, demonstrating its effectiveness in identifying forged images across various manipulation types, including copy-move, image splicing, and more. These results underscore the potential of combining classical techniques like ELA with modern deep learning methods to create a more powerful and reliable forgery detection system.

Key Words: Image Forgery Detection, Image Tampering, Convolutional Neural Networks (CNN), Copy-Move

Forgery Detection (CMFD), Splicing Forgery Detection, ELA

INTRODUCTION

With the increasing use of digital images in various domains such as media, forensics, and cybersecurity, ensuring image authenticity has become a critical challenge. Image forgery detection aims to identify manipulated images by analyzing inconsistencies in pixel patterns, metadata, and structural features. Traditional methods rely on statistical and frequency-based techniques, while modern approaches leverage deep learning, particularly Convolutional Neural Networks (CNNs) and transfer learning, to enhance detection accuracy.

This project focuses on leveraging transfer learning-based CNN models to enhance the accuracy and efficiency of image forgery detection. The scope includes implementing deep learning techniques to detect various forgery types, including copy-move, splicing, and retouching manipulations. The system will be evaluated on benchmark image forgery datasets to ensure robustness and generalizability. Additionally, the project aims to address key challenges such as false positives, dataset limitations, and adversarial attacks, with potential applications in forensic analysis, digital content verification, and deep fake detection. By integrating advanced deep learning methodologies, this research aims to contribute to the development of a more reliable and scalable image forgery detection system.

Background of the Industry:

With the rise of digital media and AI-generated content, image forgery has become a major concern across industries like journalism, forensics, and cybersecurity. Advanced editing tools and deep-fake technology have made manipulations harder to detect, increasing the risk of misinformation and fraud.

Traditional detection methods relied on manual inspection and statistical analysis, which struggled against complex forgeries. Modern approaches now leverage deep learning techniques like CNNs, GANs, and transfer learning, improving accuracy and scalability.

LITERATURE SURVEY

The literature survey reviews previous research on automated question paper generation, focusing on both proposed and existing systems.

Proposed system:

[1] Varun Shinde (2024) discusses on the Copy-Move Forgery detection by using ReLu activation & Graph Convolutional Network(GCN) ,SVM tested using MICCV F220 & CoMoFoD.

[2] Poulomi Deb (2024) demonstrates the Active & Passive Detection Techniques in Machine Learning & Neural Networks.

[3] Ashgan H. Khali (2023) Gives a spectacular Explanation Based on Deep Learning to improve Digital Image forgery Detection & 8-Distincet pre-trained models that have been modified for Binary Classification.

[4] Sang In Lee (2023) discussed on the replacement of 3-Color pictures with High Frequency Wavelet Coefficients & rotation In-variant technique.

[5] Jihyeon Kang (2022) proposed theory on the Network Uses Steganalysis landmarks & techniques to measure image quality.

[6] Fadwa Alrowais (2024) demonstrates the use of Generative Adversarial Networks which introduce tiny anomalies Using Deep learning.

Problem Definition

With the increasing sophistication of image manipulation techniques, detecting forged images has become a major challenge in fields like journalism, forensics, and cybersecurity. Traditional methods struggle to accurately identify complex forgeries such as copy-move, splicing, and deep-fake manipulations, leading to potential misinformation and fraud.

This project aims to address these challenges by leveraging transfer learning-based CNN models for improved accuracy and efficiency in forgery detection.

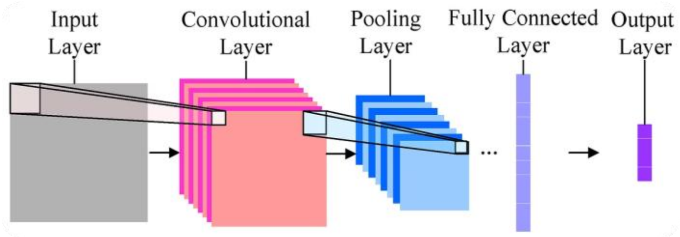

Fig [1] Convolutional Neural Networks (CNN)

Proposed Working

This project proposes a deep learning-based approach for image forgery detection using transfer learning with Convolutional Neural Networks (CNNs). The system will be designed to identify different types of forgeries, such as copy-move, splicing, and retouching, by extracting meaningful features from images and classifying them as authentic or tampered. Below is a step-by-step overview of the process:

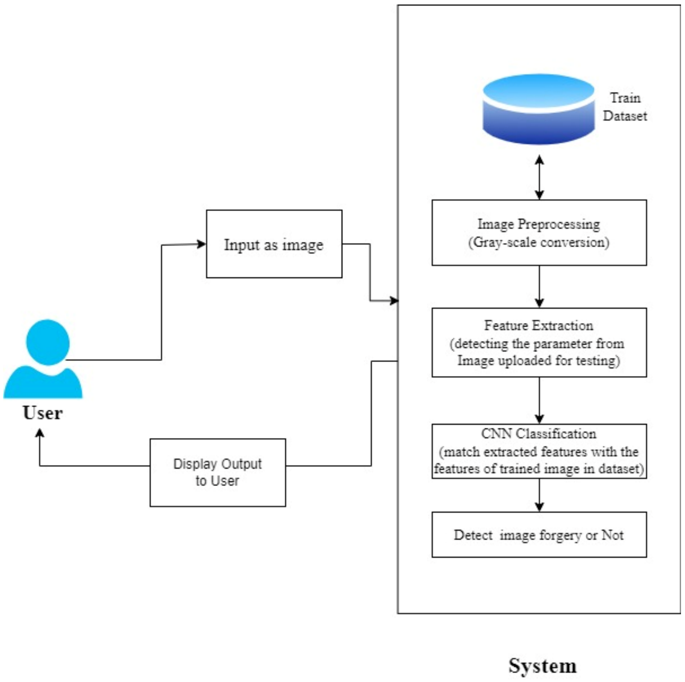
Train Dataset
Image Preprocessing (Gray-scale conversion)
Feature Extraction (detecting the parameter from Image uploaded for testing)
CNN Classification (match extracted features with the features of trained image in dataset)
Detect image forgery or Not
Input as image
User
Display Output to User
System

Fig [2] System Architecture

1. **User Input** – The user uploads an image to the system for verification.

2. **Image Preprocessing** – The system converts the image to grayscale and applies necessary enhancements to standardize input data.

3. **Feature Extraction** – Key features are extracted from the uploaded image, such as texture, edges, and patterns, for analysis.

4. **CNN-Based Classification** – The extracted features are compared with those from a pretrained CNN model (e.g., ResNet, VGG, or EfficientNet) trained on a forgery detection dataset. The CNN classifies whether the image is authentic or forged.

5. **Forgery Detection Output** – The system displays the result to the user, indicating whether the image is manipulated or genuine.

The automation of image forgery detection has led to a more efficient, accurate, and user-friendly system for verifying image authenticity. This system can analyze and detect manipulated images with minimal human intervention, significantly reducing time and effort in forensic analysis, media verification, and cybersecurity. It enhances reliability by minimizing false positives and ensuring precise identification of tampered content.

The system leverages deep learning techniques, including CNN-based feature extraction and classification, to improve detection accuracy. It supports various image formats, applies preprocessing techniques for better analysis, and provides real-time results for quick decision-making. Overall, this approach offers an optimized and scalable solution for combating digital image forgery, strengthening trust in digital content.

Objectives

The primary objective of this project is to develop an efficient and accurate image forgery detection system using deep learning techniques to identify tampered images with minimal human intervention. This system aims to:

1. Detect Various Types of Image Forgery:
This project aims to identify different forms of image forgery, including copy-move, splicing, and retouching manipulations. These forgeries are commonly used to alter images in misleading ways, and detecting them is essential for ensuring digital content authenticity.

2. Enhance Detection Accuracy Using Deep Learning:
By leveraging transfer learning-based Convolutional Neural Networks (CNNs), the system will improve classification accuracy in identifying tampered

images. Pretrained models such as ResNet, VGG, and EfficientNet will be fine-tuned to extract intricate features from images and enhance detection performance.

3. Automate the Forgery Detection Process:
The system will be designed to function with minimal human intervention, automatically analyzing uploaded images to determine their authenticity. This automation will make the detection process faster, more reliable, and user-friendly for real-world applications.

4. **Minimize False Positives and Improve Robustness:**
One of the key challenges in forgery detection is misclassifying authentic images as tampered or vice versa. This project aims to develop a model that effectively reduces false positives while maintaining high sensitivity to manipulated images, ensuring better reliability in forensic analysis and media verification.

5. **Ensure Scalability and Real-World Applicability:**
The proposed system will be scalable and adaptable to various fields, including digital forensics, journalism, cybersecurity, and legal investigations. By optimizing the model for real-time performance and handling large datasets, the project will provide a practical and efficient solution for combating image forgery in diverse environments.

CONCLUSION

Image forgery detection has become a crucial necessity in today's digital era, where manipulated images can spread misinformation, affect forensic investigations, and pose cybersecurity risks. This project leverages deep learning techniques, particularly CNN-based transfer learning, to develop an efficient, automated, and highly accurate system for detecting image forgery.

By identifying copy-move, splicing, and retouching manipulations, the proposed system ensures enhanced reliability and scalability in forensic analysis, media verification, and other security-sensitive applications. Through automated detection, reduced false positives, and improved real-time performance, this research contributes to strengthening digital content authenticity and preventing fraudulent image alterations. Moving forward, further improvements in dataset diversity and adversarial robustness will enhance the system's effectiveness in real-world scenarios.

ACKNOWLEDGEMENT

We sincerely appreciate the support and guidance we have received throughout this journey of learning and exploration. We extend our heartfelt gratitude to Dr. L.V. Kamble, Principal of Siddhant College of Engineering, Pune, for his insightful feedback and for giving us the opportunity to work on this project. Our special thanks go to Prof. Nanda Kulkarni, Head of the Computer Engineering Department, for her valuable suggestions and continuous encouragement.

We are immensely grateful to our Internal Guide, Prof. Apeksha Pande, whose expertise and unwavering support played a vital role in the successful completion of this project. We also extend our thanks to the faculty members and technical staff of the Computer Engineering Department, whose assistance and guidance have been invaluable. Additionally, we appreciate the cooperation and motivation from our classmates, who have been a great source of encouragement throughout this endeavor.

Furthermore, we acknowledge the contributions of industry experts and lab technicians, whose insights have significantly enriched our project. Above all, we express our deepest gratitude to our parents, whose unwavering support, patience, and encouragement have been the driving force behind our success.

REFERENCES

[1] Varun Shinde, Ahmad Almogren, Vineet Dhanawat, Anjanava Biswas, Md.Billal Rizwan Ali Naqvi ,Ateeq Ur Rehman, “Copy-Move-Forgery Detection Technique Using Graph Convolutional Networks Feature Extraction”, IEEE Research Papers, 2024.

[1] Poulomi Deb, Nirmalya Kar, Subhrajyoti Deb,

Abhijit Das, “Image Forgery Detection Techniques: Latest Trends and Key Challenges” Vidyawarta, 2024.

[2] Fadwa Alrowais, Meshari H. Alanazi, Asma Abba Hassan, Wafas Ulaiman, Almukadi, Radwa Marzouk, Anand Medmahmud “Boosting Deep Feature Fusion-Based Detection Model for Fake Faces Generated by Generative Adversial Networks for Consumer Space Enviroment ”, 2024.

[3] Ashganh H. Khalil, Atef Z. Ghalwash, Hala Abdelgalil Elsayed, Gouda I. salama,And Haitham A. Ghalwash, “Enhancing Digital Image Foregry Detection Using Transfer Learning” , IEEE Research Papers , 2023.

[4] Sang In Lee,Jun Young Park And Il Kyu Eom ," CNN-Based Copy-Move Forgery Detection Using Rotation-Invariant Wavelet Feature”, IEEE Researchh Papers , 2022.

[5] Francesco Marra , Diego Gragnaniello,Luisa Verdoliva and Giovanni Poggi , "A Full image Full-Resolution End-to-End Trainable CNN Framework For Image Forgery Detection”, IEEE Research Paper , 2020.

[6] Fadi Mohammad Alsuhimat and Fatma Susilawati Mohamad , " A Hybrid Method of Feature Extraction of Signatures Verification using CNN & HOG a Multi-Classification Approach”, IEEE Research Papers , 2023.

[7] Yuan Rao , Jiangqun Ni and Huimin Zhao , "Deep Learning Local Descriptor for Image Splicing Detection and Localization ” , IEEE Research Papers , 2020.

[8] Jihyeon Kang , Sang-keun Ji , Sangyeong Lee ,Daehee Jang ,and Jong-Uk-Hou , " Detection Enhancement for Various Deepfake types based on Residual Noise and Manipulation Traces ” , IEEE Research Papers , 2022.

[9] Dr. K. Prasanthi Jasmine , SK. Fhareedh , M. Navyan ,K. Abhishek , " Image Forgery Detection ” , International Journal Of Creative Research Thoughts (IJCRT) , 2023.

[10] Amit Deogar , Srinidhi Hiriyannaiah ,Siddesh Gaddadevara Matt , Srinivasa Krishnarajanagar Gopaliyengar and Maitreyee Dutta , " Image Forgery Detection based on fusion of lightweight Deep Learning Models ” , Turrkish Journals Of Electrical Engineering & Computer Sciences , 2021.

[11] Hiba Benhamza , Abdelhamid Djeffal ,Abbas Cheddad , " Image Forgery Detection Review ” , International Conference on Information Systems and Advanced Technologies , ICISAT , 2021.

[12] Ahmad A. Mazhar , Abid Jamel, Mohammad Nadeem , Mohammad Asmatullah Khan , Jawad Hasan Alkhateeb , Faiza Bibi and Ali Mohammad Seerat , " Deep Convolutional Neural Network for Robust Detection of Object-based Forgeries in Advanced Video” , IEEE Research Papers , 2023.