“Image Forgery Detection Using Transfer Learning”

Team members-

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: In today’s digital world, images are often shared and used as evidence in news, legal cases, and social media. However, it has become easier to manipulate images using editing tools, which can lead to false information and serious consequences. Detecting these changes, known as image forgery, is important to make sure images are trustworthy.

Traditional methods for detecting image tampering often struggle with accuracy, especially when the edits are small or done carefully. These methods also require a lot of manual work and may not keep up with the fast-growing technology of image editing.

This project presents a smart system that uses transfer learning to detect forged images. Transfer learning is a machine learning method that uses pre-trained deep learning models, like CNNs (Convolutional Neural Networks), to understand and analyze images more effectively. These models can find tiny changes in images that are hard to notice with the human eye.

The system works by checking for common types of forgery, such as copy-move, splicing, and removal. It is trained on real and tampered images, helping it learn the patterns of forgery. Once trained, it can quickly check new images and say whether they are original or fake.By automating the detection process, this project saves time, improves accuracy, and helps fight the spread of false visuals. It provides a reliable tool for media, law enforcement, and digital forensics to make sure images are real and trustworthy.**Key Words:** Image forgery detection, transfer learning, deep learning, digital image forensics, convolutional neural networks (CNN), copy-move forgery, splicing, tampered images, machine learning, automated detection systems

INTRODUCTION

Image forgery is a growing concern in today’s digital age, where edited images can easily spread misinformation or be used for malicious purposes. Identifying such tampered images manually is difficult and often unreliable, especially when forgeries are subtle or professionally done.This project provides a smart and automated solution for detecting image forgeries using deep learning techniques, specifically transfer learning. By leveraging powerful pre-trained models like CNNs,

the system can effectively identify different types of manipulations such as copy-move, splicing, and object removal. This ensures a more accurate and consistent detection process.
To make the system user-friendly, it includes features for visualizing the results and exporting reports, helping investigators, educators, and digital forensics experts analyze and verify image authenticity with ease.

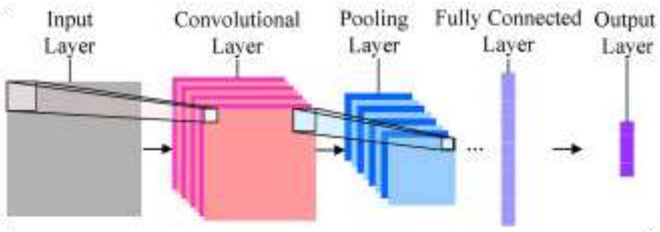


Fig [1] Convolutional Neural Networks (CNN)

Background of the Industry:

With the rapid growth of digital content, images have become a powerful medium for communication and evidence in sectors like media, law, and social platforms. However, advancements in editing tools have made it easier to manipulate images without leaving visible traces, leading to widespread concerns over fake visuals and misinformation.
Traditional image forgery detection methods are often manual, time-consuming, and struggle to identify subtle or complex manipulations. This makes it difficult for industries to rely on visual content without the risk of deception.

This project tackles these challenges by offering an automated and intelligent image forgery detection system using transfer learning. It enables faster, more accurate identification of tampered images, supporting industries such as digital forensics, journalism, and law enforcement in maintaining the integrity and authenticity of visual data.

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:

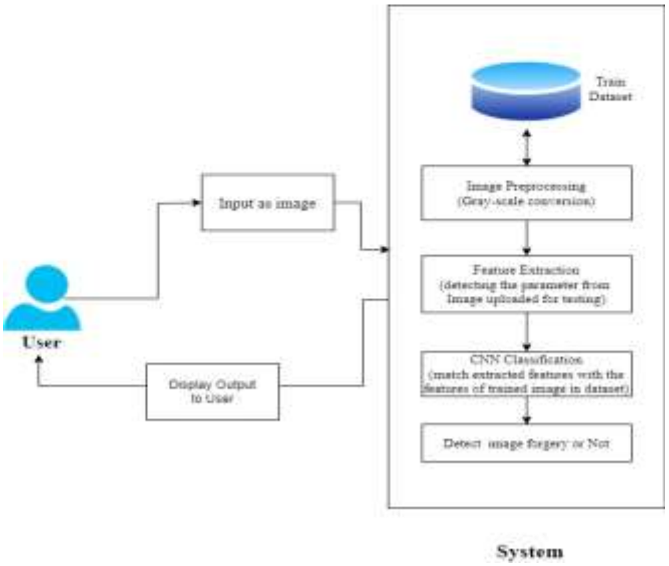

Train Dataset
Input as image
Image Preprocessing (Gray-scale conversion)
Feature Extraction (detecting the parameter from Image uploaded for testing)
CNN Classification (match extracted features with the features of trained image in dataset)
Detect image forgery or Not
User
Display Output to User
System

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 made the process faster, more accurate, and easier to use, offering a reliable way to verify the authenticity of digital images. By reducing the need for manual checks, the system significantly cuts down the time and effort required in fields like forensic investigations, media validation, and cybersecurity. It improves accuracy by lowering the chances of false detections and accurately identifying manipulated areas within images.

The automation of image forgery detection has resulted in a highly efficient, accurate, and accessible system for verifying digital image authenticity. With minimal human involvement, the system can detect various types of image manipulation, significantly reducing the time and manual effort required in areas such as digital forensics, journalism, and cybersecurity.

It minimizes the chances of false results and ensures consistent and precise detection of tampered content. The system supports different image formats, allows for real-time analysis, and includes preprocessing steps to enhance accuracy. Overall, it delivers a reliable and scalable solution that strengthens the integrity of digital content and improves the efficiency of visual content verification.

Methodolgy

The Image Forgery Detection System Using Deep Learning and Transfer Learning follows a systematic approach to accurately identify manipulated images and ensure content authenticity. The methodology involves the following key stages:

1. **Data Collection and Preprocessing:** A large dataset of authentic and forged images is collected from standard datasets such as CASIA, CoMoFoD, and Columbia. These images include various types of forgery like copy-move, splicing, and object removal. Preprocessing steps such as resizing, normalization, and image augmentation are applied to enhance the dataset's quality and consistency.

2. **Feature Extraction using Transfer Learning:** A pre-trained Convolutional Neural Network (CNN) model such as VGG16 or ResNet50 is used to extract deep features from the images. Transfer learning allows the system to benefit from models trained on large image datasets, improving detection accuracy with fewer computational resources.

3. **Classification:** The extracted features are passed through custom classification layers to distinguish between original and forged images. The model is trained and validated using labeled data, ensuring that it learns the distinguishing characteristics of tampered images.

4. **Forgery Localization (Optional):** In advanced versions, techniques like heatmaps or Grad-CAM are applied to visualize and localize tampered regions in the image, providing clear insights into where manipulation has occurred.

5. **Evaluation and Reporting:** The system's performance is evaluated using metrics such as accuracy, precision, recall, and F1-score. Forgery detection results are displayed in real time, and reports can be exported in PDF format for review and documentation.

This methodology ensures a reliable, efficient, and scalable solution for detecting image forgeries, contributing to improved trust in digital content and supporting industries that rely on image verification.

Tools and Technologies Used

The Image Forgery Detection System utilizes a range of tools and technologies to enable accurate detection and provide a user-friendly experience:

1) Programming Language:
    - Python
2) GUI Framework:
    - Tkinter
3) Deep Learning Libraries:
    - TensorFlow ,Keras ,OpenCV ,NumPy
4) Data Handling and Analysis:
    - Pandas, Matplotlib , Seaborn
5) Development Tools:
    - Jupyter Notebook / Visual Studio Code
    - GitHub

Results

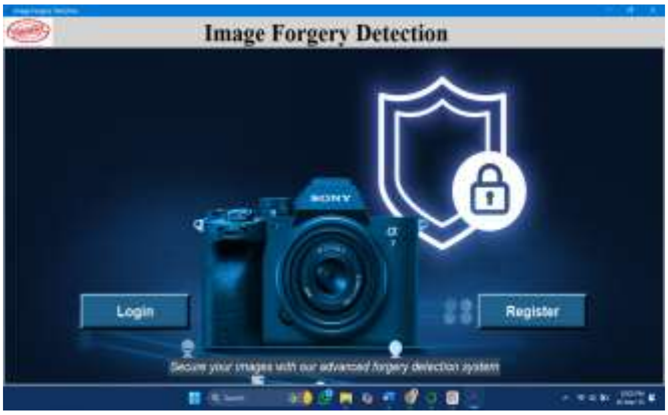


Image Forgery Detection
Login
Register
Secure your images with our advanced forgery detection system

Fig [2] Dashboard

The Image Forgery Detection System is a professional solution designed for forensic analysts, cybersecurity experts, and media verifiers to detect tampered images with high accuracy. Featuring a clean and intuitive GUI built with Tkinter, it offers a user-friendly interface for uploading images, running forgery detection in real time, and viewing detailed results—making the process streamlined and accessible even for non-technical users.

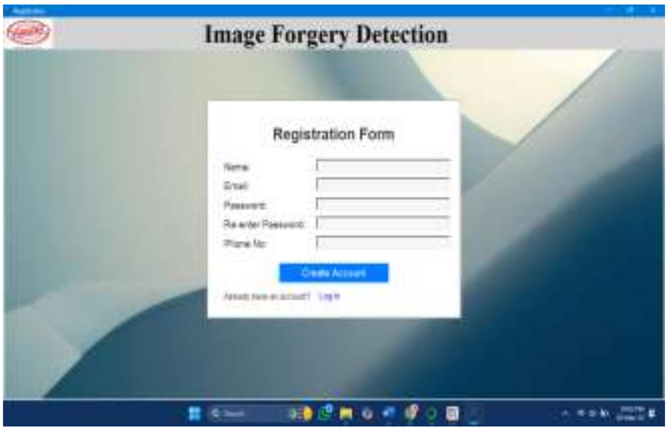


Fig [3] Registration page

The registration page enables users to create accounts with essential details like name, email, and password. It features a clean design, validation checks for security, and a seamless user experience. Upon successful registration, users receive a confirmation and are redirected to the login page.

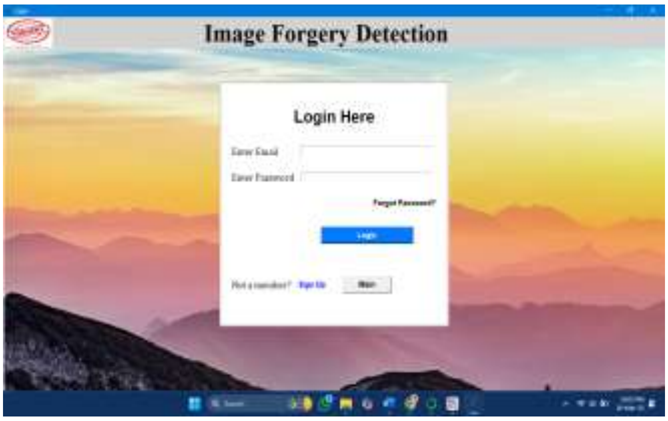
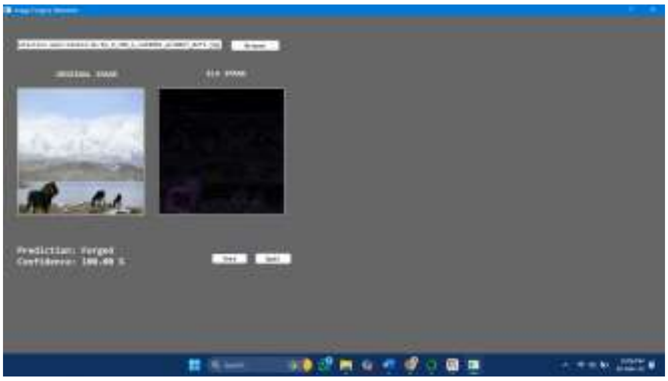


Fig [4] Login page

The login page provides a secure, user-friendly entry for registered users. It features email and password fields, ensuring easy access while maintaining security. A "Register Now" option guides new users to sign up. The streamlined design enhances accessibility and trust in the platform.



Prediction: Forged
Confidence: 100.00 %

Fig [5] Image Forgery Detection

The image forgery detection interface provides a structured and user-friendly experience for users to verify image authenticity with ease. The GUI includes intuitive options for uploading images, viewing detection results, and navigating between features. Users can select image files using a file browser, and real-time feedback displays whether the image has been manipulated. The system also offers options to visualize tampered regions and export results for reporting. This streamlined design enhances usability, making the tool accessible for professionals in forensic analysis, media, and cybersecurity.

Objectives

The goal of this project is to develop an automated system for detecting image forgery using deep learning and transfer learning techniques. The system is designed to enhance the efficiency, accuracy, and reliability of digital image verification by achieving the following objectives:

1. **Automation of Image Forgery Detection:** The system automates the detection of forged or manipulated images, reducing the need for manual inspection and improving verification speed in forensic and media applications.

2. **Use of Deep Learning and Transfer Learning Models:** By leveraging pre-trained CNN architectures like VGG16 or ResNet50, the system improves detection performance and generalization across diverse image formats and forgery types.

3. **Minimization of False Positives and Negatives:** The deep learning-based approach enhances the precision of tampering detection, ensuring accurate identification of altered regions and reducing misclassifications.

4. **User-Friendly Interface:** A GUI developed using Tkinter enables non-technical users to upload images, receive real-time analysis, and visualize tampered areas, making the system accessible and practical for a wide audience.

5. **Scalability and Real-Time Processing:** The solution is designed to handle large volumes of image data and provide fast results, making it suitable for real-world applications in cybersecurity, journalism, and digital forensics.

CONCLUSION

The Image Forgery Detection System using Deep Learning and Transfer Learning marks a significant advancement in the field of digital forensics and content verification. By automating the complex task of detecting manipulated images, it greatly improves efficiency while maintaining high levels of accuracy and reliability.

The integration of CNN architectures and transfer learning enables the system to detect forgeries with precision, supporting a wide range of image types and manipulation techniques. Its intuitive, Python-based GUI built with Tkinter enhances accessibility, making it practical for both professionals and general users.

This system is adaptable for use in multiple domains, including forensic analysis, media verification, and cybersecurity. Overall, it represents a transformative step forward in the fight against digital misinformation, offering a scalable and intelligent solution for ensuring the authenticity of visual content.

ACKNOWLEDGEMENT

We are truly grateful to everyone who has supported and guided us during this journey of learning and discovery. We would like to thank Dr. L.V. Kamble, Principal of Siddhant College of Engineering, Pune, for his valuable feedback and for allowing us to undertake this project. A special thanks to Prof. N.S. Kulkarni, Head of the Computer Engineering Department, for her helpful suggestions and continuous guidance throughout the project.

We also want to express our heartfelt thanks to our internal guide, Prof. Apeksha Pande, and the faculty and technical staff of the Computer Engineering Department for their constant support and guidance, which was crucial to completing this project.

We would also like to acknowledge the support from industry experts, lab technicians, and our classmates, whose contributions and encouragement added great value to our project and kept us motivated throughout.

Lastly, our deepest gratitude goes to our parents for their unconditional support and motivation during this entire journey.

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.

[2] Poulomi Deb, Nirmalya Kar, Subhrajyoti Deb, Abhijit Das, “Image Forgery Detection Techniques: Latest Trends and Key Challenges”, Vidyawarta, 2024.

[3] 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 Adversarial Networks for Consumer Space Environment”, 2024.

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

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

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

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

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

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

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

[11] Amit Deogar, Srinidhi Hiriyannaiah, Siddesh Gaddadevara Matt, Srinivasa Krishnarajanagar Gopaliyengar, Maitreyee Dutta, "Image Forgery Detection Based on Fusion of Lightweight Deep Learning Models”, Turkish Journal of Electrical Engineering & Computer Sciences, 2021.

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

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