



Enhancing Digital Image Forgery Detection using Transfer Learning

¹C. Tejaswani, ²M. Yamini, ³Y. Deepthi, ⁴G M Anand Reddy

¹Student, ²Student, ³Student, ⁴Professor,
Department of Computer Science and Engineering,
R. L. Jalappa Institute of Technology, Doddaballapura, Bengaluru, India

ABSTRACT

In recent times, digital images have become widely used across various sectors, making them a prime target for manipulation by malicious actors. The act of altering digital images for fraudulent purposes is referred to as image forgery. To address this challenge, this project proposes an efficient framework for detecting image forgeries using transfer learning models. The findings from this study demonstrate that the proposed method achieves exceptional accuracy in detecting forgeries within a dataset of 220 images, comprising both genuine and manipulated samples. The models utilized in the framework, such as ResNet50, VGG16, Xception, DenseNet201, Mobile Net, and Dense Net Mobile, showcase their effectiveness in accurately identifying tampered images.

I. INTRODUCTION

Digital images are integral to modern communication, particularly through social media. However, the rise of advanced image-editing tools has made it easier to manipulate images for malicious purposes. Image forgeries, which are often indistinguishable to the naked eye, can spread misinformation, damage reputations, and even compromise legal evidence. The detection of these forged images is therefore critical, particularly for fields such as forensic analysis, journalism, and cyber security. Digital image forgery can be classified into several types, including copy-move, image splicing, and image retouching. These types of forgery involve duplicating parts of an image, combining elements from multiple images, or modifying visual features to misrepresent information. Current approaches to forgery detection rely on both active methods, which embed verification data, and passive methods, which analyze image inconsistencies.

II. EXISTING SYSTEM

Transfer learning offers a powerful strategy in machine learning, where a model developed for one task is adapted for use in a related domain. In image forgery detection, this technique involves utilizing a pre-trained convolutional neural network (CNN) model—originally trained on extensive datasets like ImageNet—to identify tampered or manipulated images. Rather than training a model from scratch, which is resource-intensive and requires a large labelled dataset, transfer learning enables faster convergence and improved performance with less data. To begin, a suitable CNN architecture is selected, with widely adopted choices including ResNet, VGG, Inception, and Efficient Net. These models are capable of extracting rich and abstract features from images, making them well-suited for distinguishing between authentic and forged content.

III. PROPOSED SYSTEM

Develop a lightweight, efficient deep learning-based model using pre-trained architectures. Enhance detection accuracy for copy-move and splicing forgeries simultaneously. Minimize computational costs and training time by leveraging transfer learning. Utilize the CASIA 2.0 benchmark dataset for testing and validation.

Our proposed deep learning-based approach is an extension of the CNN architecture. The proposed architecture has the following modules:

- i) Pre-processing module
- ii) Convolutional module
- iii) Classification module

IV. LITERATURE SURVEY

Digital image forgery detection has been an area of intense research interest due to the growing prevalence of image manipulation.

1. K. D. Kadam et al. (2021)

Title: Multiple Image Splicing Dataset (MISD): A Dataset for Multiple Splicing

Description: This study presents the Multiple Image Splicing Dataset (MISD), developed to support research in detecting multiple image splicing forgeries. The dataset emphasizes the complexity and variability of spliced images under different environmental and contextual conditions, aiming to provide a comprehensive benchmark for evaluating and improving forgery detection algorithms.

2. F. Li et al. (2022)

Title: Image Forgery Detection Using Tamper-Guided Dual Self-Attention Network

Description: This work proposes a novel forgery detection framework that combines convolutional neural networks with a tamper-guided dual self-attention mechanism. The approach improves the model's ability to localize and identify manipulated regions in spliced images by focusing on contextual and semantic inconsistencies.

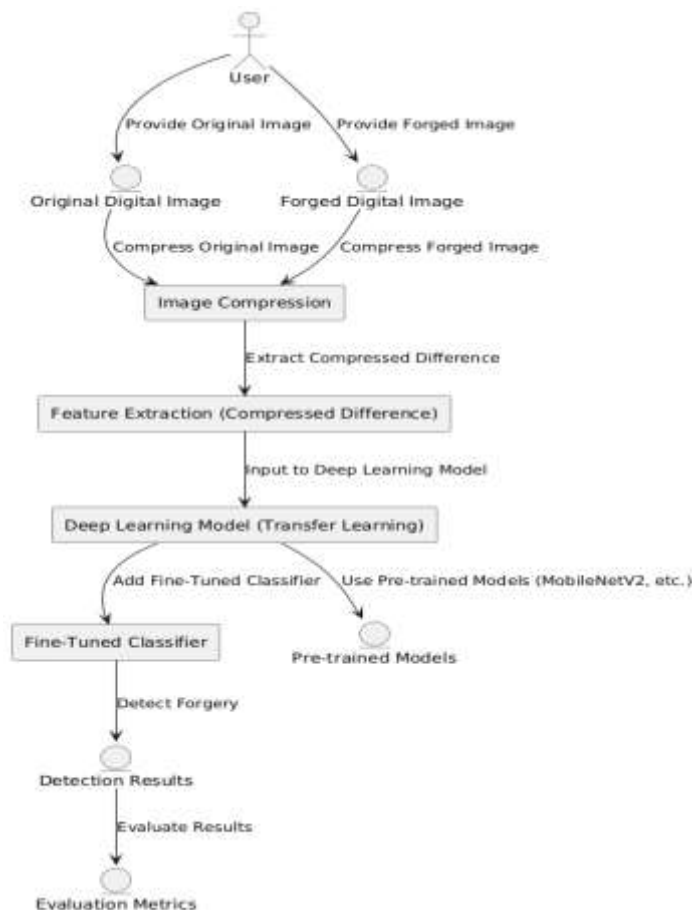
3. K. M. Hosny et al. (2023)

Title: A New Method to Detect Splicing Image Forgery Using Convolutional Neural Network

Rephrased Description: This paper introduces an efficient and lightweight CNN-based model designed for real-time detection of image splicing forgeries. The approach prioritizes computational efficiency, making it suitable for deployment in resource-constrained environments while maintaining high detection accuracy.

V. SYSTEM ARCHITECTURE

Storage and Retrieval handle the storage and retrieval of user data and input texts, while the AI model controller manages the loading and operation of AI models, including GPT-2 and BERT. These AI models, acting as the system's intelligence, generate narrative content and multiple-choice questions based on the provided input.



VI. RESULTS

To assess the performance and robustness of the proposed forgery detection approach, we conducted extensive experiments on widely-used benchmark datasets, including CASIA v2.0, CoMoFoD, and the Columbia Image Splicing Dataset. These datasets contain diverse and realistic image manipulations, providing a comprehensive basis for evaluation. Our methodology employs transfer learning by fine-tuning pre-trained deep convolutional neural networks (CNNs), specifically ResNet50 and EfficientNet-B0, on forgery detection tasks. This approach enables the models to leverage learned visual features from large-scale image datasets, significantly reducing training time and improving generalization.

VII. CONCLUSION

This survey paper has provided a detailed exploration of digital image forgery detection techniques, with a particular focus on the transition from traditional, handcrafted-feature-based methods to advanced deep learning approaches. Traditional techniques, while instrumental in the early development of forgery detection systems, often struggle with generalization and are limited in their effectiveness against complex or novel manipulations. The advent of deep learning has introduced a paradigm shift, enabling models to autonomously learn hierarchical representations and features from data. This capability significantly improves the robustness and accuracy of forgery detection systems across a diverse range of manipulations, including copy-move, splicing, and content-aware editing. Among these, transfer learning has emerged as a particularly promising direction, allowing models to leverage pre-trained networks for efficient and scalable implementation.

VIII. REFERENCES

- [1] K. D. Kadam, S. Ahirrao, and K. Kotecha, "Multiple image splicing dataset (MISD): A dataset for multiple splicing," *Data*, vol. 6, no. 10, p. 102, Sep. 2021.
- [2] R. Agarwal, O. P. Verma, A. Saini, A. Shaw, and A. R. Patel, "The advent of deep learning-based," in *Innovative Data Communication Technologies and Application*. Singapore: Springer, 2021.
- [3] M. A. Elaskily, M. H. Alkinani, A. Sedik, and M. M. Dessouky, "Deep learning based algorithm (ConvLSTM) for copy move forgery detection," *J. Intell. Fuzzy Syst.*, vol. 40, no. 3, pp. 4385–4405, Mar. 2021.
- [4] U. Haq, Q. Emad, Z. Tanveer, and A. Abdulrazaq, "Deep Learning-Based Digital Image Forgery Detection System," *Applied Science*, MDPI, 2022.