IMAGE FORGERY DETECTION USING DEEP LEARNING

Kunal Bhagat*1, Niketan Gadade*2, Sohail Korbu*3, Anurag Gosavi*4, Prof S.B. Bhonkar*5

*1,2,3,4,5Information Technology, Sinhgad College Of Engineering, Pune, India.

ABSTRACT

In the contemporary era, digital images constitute a primary means of disseminating information on social media platforms. However, this prevalence has given rise to a pressing issue—malicious software adept at fabricating images to propagate false information. Addressing this concern, existing literature has explored various digital image forgery detection techniques. Yet, many of these methods are confined to detecting singular types of forgery, such as image splicing or copy-move, which may not accurately reflect real-world scenarios. This paper introduces a novel approach to bolster digital image forgery detection by leveraging deep learning techniques through transfer learning. The goal is to simultaneously uncover two distinct types of image forgery. The proposed method hinges on identifying variations in the compressed quality of forged areas, typically deviating from the compressed quality of the rest of the image. A deep learning-based model is presented for forgery detection in digital images. This involves calculating the disparity between the original image and its compressed version to generate a featured image, serving as input to a pre-trained model. The pre-trained model undergoes training with its classifier removed, and a new fine-tuned classifier is introduced. A comparative analysis is conducted among eight different pre-trained models tailored for binary classification. Experimental results demonstrate that implementing the proposed technique with the adapted pre-trained models surpasses existing state-of-the-art methods. This conclusion is drawn from a comprehensive evaluation involving metrics, charts, and graphs. Notably, the results reveal that employing the technique with the MobileNetV2 pre-trained model achieves the highest detection accuracy rate, approximately 95%, while requiring fewer training parameters, leading to expedited training times.

Keywords: Deep Learning, Convolution Neural Network (CNN), Image Tampering, Transfer Learning, Sharpening Filter, Fine-Tuning, Logistic Regression, Accuracy, Precision, Recall.

I. INTRODUCTION

Since the inception of photography, there has been a persistent pursuit by individuals and organizations to manipulate images, aiming to deceive viewers. Initially, this task demanded considerable expertise and hours of work from professional technicians. However, with the advent of digital photography, the ease of image modification has become accessible to virtually anyone, yielding results that mimic professionalism effortlessly. Consequently, this widespread accessibility has given rise to social issues, ranging from the reliability of images presented by the media to the alteration of photographs of models to enhance their appearance or body image.

The extensive array of methods available for image manipulation has led to a growing interest in image forgery detection, both in academic research and the professional domain. While numerous detection methods exist, determining the most efficient and practical ones to implement and execute proves challenging. An algorithm with a high detection rate may concurrently exhibit a substantial rate of false positives. Additionally, while runtime significantly influences an algorithm’s efficiency and usability, it is often discussed academically rather than in practical, real-world terms.

To streamline this complex task, algorithms will be categorized into five distinct types: JPEG Compression Quantization, Edge Detection, Clone Detection, Resampling Detection, and Light & Color Anomaly Detection. Specific research will then be conducted on each group, assessing the general efficiency of the described algorithm types. If a method is deemed reliable, an algorithm from that group will be implemented. These categories are chosen based on the entirely different detection methods they employ, promising diverse outcomes depending on the type of image forgery.

The subsequent phase involves extensive testing of the implemented algorithms using a diverse image library to ascertain their success rates. General properties, such as false positive rates and runtime, will be meticulously documented. Moreover, specific tests on variants of the same algorithm will be conducted. For instance, algorithms may have parameters that significantly impact their performance and detection rate on particular...
image classes. By systematically testing these values, the project aims to comprehensively evaluate an algorithm's performance across various image types, ensuring that advanced algorithms are not unfairly dismissed due to the need for parameter adjustments.

II. LITERATURE REVIEW

The evolution of deep learning (DL) over the last decades has positioned it as a dominant force across various domains. In the realm of digital image forensics, an expanding body of literature explores DL-based techniques for detecting and classifying tampered regions in images. This comprehensive literature survey aims to categorize and analyze state-of-the-art DL-based methods for image forgery detection, considering document type, forgery type, detection method, validation dataset, evaluation metrics, and results.

1. **Image Forgery Detection (General Overview):** The literature survey reveals that the majority of forgery detection works center on images, with seminal studies contributing to the development of various detection methods. These include traditional approaches, modern techniques like deep learning, and feature-based methods.

2. **Document Forgery Detection:** While image forgery detection remains a focal point, pioneering studies extend the focus to the analysis of administrative documents, contributing to improved forgery detection accuracy.

3. **Copy-Move Forgery Detection (CMFD):** Recent advancements in CMFD techniques are presented in a state-of-the-art technical review. A new CMFD process pipeline is introduced, offering insights and updated information on CMFD to researchers in the field.

4. **Deep Learning for Image Forgery Detection:** The impact of deep learning on image forgery detection is substantial. The article under consideration provides a comprehensive survey of DL-based methods, specifically focusing on copy-move and spliced images, two prevalent types of forgeries. Recent advances in DL have significantly outperformed traditional non-DL-based methods. Techniques surveyed involve the development or fusion of various efficient DL methods, such as CNN, RCNN, or LSTM, to adapt to detecting tampered traces.

5. **Classification Framework:** The literature survey's classification framework encompasses document type, forgery type, detection method, validation dataset, evaluation metrics, and obtained results. This comprehensive approach offers a nuanced understanding of the varied aspects covered in forgery detection research.

6. **Research Trends and Gaps:** The literature review underscores the integration of deep learning in forgery detection, highlighting the substantial improvements achieved by DL-based methods. It emphasizes the importance of addressing challenges in administrative document forgery. This literature review provides a holistic overview of image forgery detection, integrating insights from multiple research papers.

**OBJECTIVES**

1. To develop a robust and accurate deep learning-based solution for image forgery detection to enhance the integrity and trustworthiness of digital images in various domains, such as forensics, journalism, and social media.

2. To conduct a detailed literature review on image forgery detection method and related Technologies.

3. To ensure that the detection model is robust and can effectively identify forgeries in images with varying levels of complexity, quality, and resolution.

4. To Develop a user interface that allows users to easily upload images and view forgery detection results.

**EXISTING SYSTEM**

In the realm of digital image forgery detection, the utilization of deep learning techniques has become increasingly prevalent. An existing system, which employed the MobileNetV2 architecture, stands as a testament to the efficacy of this approach in addressing the critical challenge of detecting image forgeries. MobileNetV2 is a state-of-the-art neural network architecture that has been specifically designed for mobile and embedded vision applications. Its lightweight design and computational efficiency make it an attractive choice for tasks where resource constraints are a concern. In the context of digital image forgery detection, MobileNetV2 provides a streamlined and effective solution. The existing system, utilizing MobileNetV2, demonstrated impressive results in distinguishing between authentic and tampered images.
III. RESEARCH METHODOLOGY

A) Image Enhancement:
Error Level Analysis (ELA) is applied as a pre-processing step to identify tampering in JPEG images. ELA leverages the differences in compression levels to highlight areas that may have undergone manipulation. Additionally, a sharpening filter is implemented using advanced techniques from the Pillow-python image processing library. This filter enhances pixel contrast, focusing on areas prone to distortion during image manipulation, such as edges and lines.

B) CNN Architecture:
The Convolutional Neural Network (CNN) architecture is meticulously designed. It comprises an input layer for image ingestion, followed by convolutional layers responsible for feature extraction. Subsequently, pooling layers reduce spatial dimensions, and fully-connected layers enable classification using a SoftMax activation function. The architecture is optimized for learning hierarchical features and patterns. The CNN is trained on the training dataset using an appropriate optimizer and loss function. Extensive hyperparameter tuning is performed to strike a balance between model complexity and overfitting. The training process involves multiple epochs to ensure the convergence of the model. The model's performance is assessed on the testing set to gauge its ability to distinguish between authentic and manipulated images. The model's performance is assessed on the testing set to gauge its ability to distinguish between authentic and manipulated images.

C) Transfer Learning:
Transfer learning is employed using pre-trained models, specifically VGG16 and ResNet50, acknowledged for their prowess in image recognition tasks. These models serve as a starting point, leveraging previously learned features to enhance performance on the forgery detection task. To facilitate efficient model training and thorough evaluation, the dataset is further split into 40% for training, 30% for validation, and 30% for testing. The selected models are trained on the training dataset, and their performance is evaluated on the validation set. This process involves fine-tuning hyperparameters to optimize the models for the specific forgery detection task. To tailor ResNet50 to the forgery detection task, the last layer is customized to match the classes in the dataset (real or fake). Further training is conducted to adapt the model to the nuances of image manipulation, striking a balance between leveraging pre-trained features and learning task-specific information.

IV. PROPOSED SYSTEM

The proposed system for image forgery detection is a comprehensive approach that combines Convolutional Neural Network (CNN) architecture with Error Level Analysis (ELA) to achieve accurate and robust detection of manipulated images. This system addresses the critical need for reliable forgery detection in the era of digital image manipulation. The proposed system employs a CNN model as its core. The CNN is designed to perform feature extraction and classification of images efficiently. The model is trained on a diverse dataset comprising both authentic and tampered images. During training, it learns to identify distinctive patterns, features, and inconsistencies that indicate image manipulation. Various hyperparameters, such as the number of layers, filter sizes, and learning rates, are fine-tuned to optimize the model's performance. Appropriate activation function such as ReLU (Rectified Linear Unit), is used to introduce non-linearity in the model.

ADVANTAGES OF PROPOSED SYSTEM

Advantages:

a. High Accuracy: The proposed system combines the strengths of CNNs and ELA to achieve high accuracy in detecting digital image forgeries. The CNN's ability to learn intricate patterns and features is complemented by ELA's capability to highlight inconsistencies, resulting in precise detection.

b. Robustness: By integrating ELA as a preprocessing step, the system gains robustness against various forgery techniques and manipulation types. It can effectively detect both simple and complex forgeries, making it versatile and reliable.

c. Adaptability: The system's CNN architecture is highly adaptable and can be fine-tuned to specific forgery detection tasks. This adaptability allows it to perform well across a wide range of image content and manipulation methods.
d. **Real-Time Detection:** The proposed system is designed with real-time implementation in mind, making it suitable for applications where immediate forgery detection is crucial, such as social media content filtering and forensic analysis.

V. **ARCHITECTURE**

Building a deep learning model involves a series of systematic steps to ensure effective development and deployment. The process typically starts with defining the problem and gathering relevant data. After data collection, the dataset is preprocessed, involving tasks like handling missing values, scaling features, and encoding categorical variables. The next step is to split the data into training and testing sets, facilitating the evaluation of the model's performance. Following this, a suitable algorithm is selected based on the nature of the problem and the characteristics of the data. The chosen model is then trained using the training dataset, optimizing its parameters to enhance performance. Post-training, the model is evaluated on the testing dataset, and its performance metrics, such as accuracy or F1-score, are assessed. If the model meets the desired criteria, it is deployed for making predictions on new, unseen data. Regular monitoring and updates may be necessary to maintain model accuracy and relevance over time.

A) **Preprocessing:**

Preprocessing in the context of deep learning refers to the essential steps taken to clean, transform, and organize raw data before it is fed into a model for training. Typical preprocessing tasks encompass addressing missing values, scaling numerical features, encoding categorical variables, and eliminating irrelevant or redundant information. By carefully preparing the data through preprocessing techniques, such as normalization or standardization, the deep learning model becomes more robust, improving its ability to discern meaningful patterns and relationships within the dataset.

B) **Feature Extraction:**

Feature extraction involves transforming raw data into a subset of essential features, effectively capturing the most relevant information for analysis and model training. This technique aims to reduce the dimensionality of the dataset while retaining the critical characteristics that contribute to the underlying patterns. By extracting pertinent features, the computational complexity of models is reduced, and the risk of overfitting is mitigated. At this juncture, feature descriptors are crafted from each block or key point, stemming from preceding processes. These descriptors, essentially vectors derived from image data, possess a high degree of discriminative power. Consequently, in the context of Copy-Move Forgery (CMF), it is imperative that the original and duplicated images yield sets of feature descriptors exhibiting similarity or close correlation. Employing a robust extraction technique ensures that each descriptor generated carries a formidable level of discriminative power, ultimately contributing to the overall accuracy of the detection system. This stage not only holds significance in determining the comprehensive detection accuracy but also serves as a pivotal factor influencing the processing speed of the system. In practical terms, the presence of a considerable number of key points or blocks within a single image, particularly in high-resolution images, underscores the critical role of this feature extraction stage.

C) **Classification:**

Classification in deep learning is a fundamental task where the goal is to assign predefined labels or categories to input data based on discerned patterns learned during the training phase. This process involves constructing a predictive model capable of distinguishing between different classes within a dataset. The model learns from labeled examples, extracting features and mapping them to corresponding output categories. Popular classification algorithms include CNN, Support Vector Machines.
Fig 1: System Architecture for Image Forgery Detection using Deep Learning.

**Precision**: - It is calculated as the ratio of true positive predictions to the sum of true positives and false positives.

\[
    \text{Precision} = \frac{\text{True Positive}(TP)}{\text{True Positive}(TP) + \text{False Positive}(FP)}
\]

**Recall**: - It is calculated as the ratio of true positive predictions to the sum of true positives and false negatives

\[
    \text{Recall} = \frac{\text{True Positive}(TP)}{\text{True Positive}(TP) + \text{False Negative}(FN)}
\]

**F1-Score**: - It is a harmonic mean of precision and recall.

\[
    F_1 = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}
\]

**Accuracy**: - It is a performance metric used in machine learning to evaluate the overall correctness of predictions made by a model.

\[
    \text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}}
\]

VI. ACTIVITY DIAGRAM

An activity diagram is a visual representation within the Unified Modeling Language (UML) that illustrates the flow of activities or actions within a system or business process. The login process is initiated after successful registration. After successful login model goes through pre-processing, Feature Extraction and Classification process are done. The Output will be provided and accordingly forgery results will be shown.
VII. CONCLUSION

The integration of deep learning analysis for image forgery detection prediction represents the best approach with the potential to improve the way we understand, prevent, and combat this public trust issue. As discussed in this research paper, this innovative combination of technologies offers real-time forgery detection, predictive modeling, and a deeper understanding of the image forgery detection. The utilization of deep learning in image forgery detection prediction is an exciting and promising avenue for research and practical application. As technology advances and data collection methods become more sophisticated, the potential for early detection in the fight against image forgery will only grow. By controlling the power of these cutting-edge technologies, we can take significant steps towards a manipulated image and more sustainable future for individuals and society.
VIII. REFERENCES


