ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research

Vol. 16, Issue, 08, pp.29589-29593, August, 2024
DOI: https://doi.org/10.24941/ijcr.47657.08.2024

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEW ARTICLE

ADVANCED DEEP LEARNING STRATEGIES FOR IMAGE FORGERY DETECTION: USING CNN ARCHITECTURES

[1]*Prof. V Vijayalakshmi, [2]Prof. Noor Ayesha, [3]Prithvi Prabhu Pani V., [4]Tejushree R., [5]Sadiya Fathima N. and [6]Sameen Mehnaz Fathima

[1]Assistant Professor, CSE Department, Atria Institute of Technology, Bangalore, India
[2]Assistant Professor, ECE Department, HKBK College of Engineering, Bangalore, India
[3,4,5,6] Student, CSE Department Atria Institute of Technology, Bangalore, India

ARTICLE INFO

Article History:
Received 18th May, 2024
Received in revised form
19th June, 2024
Accepted 25th July, 2024
Published online 30th August, 2024

Key words:
CNN, Image Forgeries, Deep Learning Strategies, Forgery Detection, Image Security.

***Corresponding author:**
Prof. V Vijayalakshmi

ABSTRACT

This research explores advanced strategies utilizing deep learning for detecting image forgeries, focusing specifically on leveraging Convolutional Neural Network (CNN) architectures. CNNs are employed due to their ability to analyze and learn hierarchical features, which are crucial for identifying subtle manipulations in images. By exploiting CNNs, this study aims to enhance the reliability and accuracy of forgery detection methods, contributing to improved security and authenticity verification in digital media.

Citation: Prof. V Vijayalakshmi, Prof. Noor Ayesha, Prithvi Prabhu Pani V., Tejushree R., Sadiya Fathima N. and Sameen Mehnaz Fathima. 2024. "Advanced Deep Learning Strategies for Image Forgery Detection: Using CNN Architectures.". *International Journal of Current Research*, 16, (08), 29589-29593.

INTRODUCTION

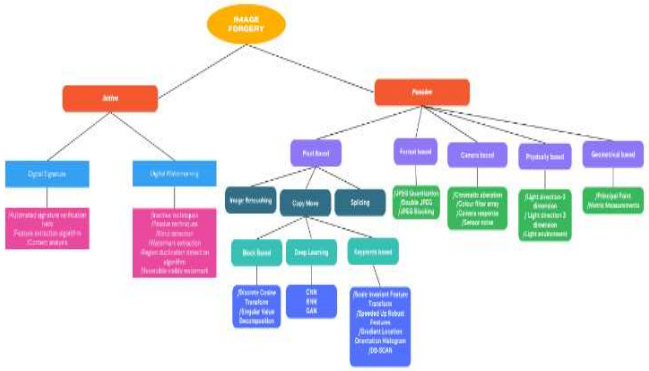
"All is not always what they seem" – never have these words been truer in the digital landscape than they are today. Images have become a pervasive aspect of our life with the ubiquity of devices such as smart phones and cameras. The ease of Internet usage has also contributed to the pervasiveness. As a result, the number of image manipulation software also has increased. These tools have become more accessible, such that anyone may easily modify and share images online. In parallel, image tampering has also increased. It has become a genuine societal harm. In this context, image processing has emerged as a crucial tool for identifying and preventing forgeries by analysing digital images for inconsistencies and alterations. This research paper delves into the role of image processing in forgery detection techniques, the effectiveness of various techniques, and the potential of advanced algorithms such as Convoluted Neural Network to improve the overall accuracy and reliability of detecting forgeries.

Overall, image processing serves as a cornerstone in the area of forgery detection, enabling the extraction of essential features from images to identify and distinguish between manipulated and authentic content, ultimately upholding the reliability and credibility of digital imagery.

IMAGE FORGERY

Forgery remains a prevalent issue in various fields, including art, currency, and document verification, necessitating robust forgery detection techniques. Additionally, operations like blurring, JPEG-compression, and smoothing are applied to forged areas, necessitating frequent improvements in existing forgery detection processes. Image processing techniques, including examining embedded noise, waveforms, and lossy-format error levels, are instrumental in detecting image forgery and alterations, contributing to the overall integrity of the process [Zanardelli, 2022].

The utilization of advanced algorithms such as Convolutional Neural Networks (CNN) are showing promising results. CNN algorithms play a pivotal role in image processing by analysing visual data through multiple layers of learning, mimicking the human brain's visual processing.



Source: Adapted from [1]

Figure 1. Flowchart depicting image forgery techniques and detection methods

METHODOLOGY

Feature extraction in image forgery detection utilizing Convolutional Neural Networks (CNNs) involves using deep learning techniques to automatically identify patterns and anomalies that indicate manipulation. The hierarchical feature extraction process of CNNs allows them to analyze images at multiple levels of detail [Boubacar Diallo, 2020].

Data Collection and Pre-processing

- Collection of a diverse set of images including both authentic and forged examples is the inital step. The dataset should include various types of forgeries such as splicing, cloning, and tampering. Image Net can be utilized for obtaining dataset.
- Pre-processing of images is an important step in image processing pipeline. It involves application of series of operations on raw input images for further analysis or feature extraction. Pre-processing techniques are formulated with the aim to improve the data quality. Noise reduction, contrast enhancement, standardization of formatting are some pre-processing techniques that are implemented in the forgery detection methodology.
- Histogram equalization is a pre-processing technique used to enhance the query image so as to make its details stand out more. It is a necessary step as minute forgeries can sometimes remain undetected through the process. This is a contrast enhancement technique where intensities are adjusted using histogram of the image. By adjusting pixel intensity distribution, contrast is improved and details are revealed in both dark and bright regions.
- Removal of noise is another critical step in pre-processing of images for forgery detection. De-noising can be done using median filtering with MATLAB. Each pixel value is replaced with median value to reduce salt-and-pepper noise.

Feature Extraction

Using Convolutional Neural Networks (CNNs) in automated image analysisyields numerous advantages over conventional neural architectures like:

- Their weight-sharing feature minimizes the number of common parameters across different parts of the feed. This enhances the network's ability to generalize data in an effective way and minimize the risk of over fitting leading to more interpretable prototypes.
- When the layers responsible for feature extraction and classification are studied simultaneously, the prototype's output becomes highly smooth structured, even textured and strongly subordinated on the gleaned patterns.
- In comparison to the other divisions of neural systems, implementing large-scale networks is significantly easier with CNNs as it maintains accuracy over time.

There are 3 major classifications of layers, they are: convolutional layer, pooling layer and fully connected layer.

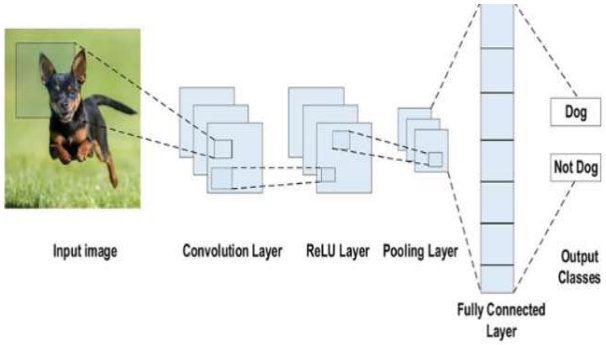
Convolutional Layer: In a CNN model, the initial layer is the input node layer, where the height, width and depth of the source image are specified. Immediately after the input interface, convolutional layers are defined with the sum of filters (also called as kernels), filter window size (3x3 or 5x5), padding (to sustain dimensional parameters) and stride (step interval of filter) and activation as the attributes.

Convolution layers are employed to extractpurposeful feature maps for the input location by transitioning pixel-by-pixel consequently resulting in the creation of a weighted sum. This contributes to the composition of feature maps, which are subsequently processed through an activation function and bias is added to fabricate the final output. Typically, rectilinear unit (ReLU) activation is adopted in this process.

Pooling Layer: Pooling layers are employed to downsize the previous outcomes of the combined convolutional layers. These layers mainly assist in obtaining unique features. As the number of kernels in the convolutional layer grows, the prototype's size expands which leads to an exponential increase in output configuration.

Pooling layers are incorporated to alleviatethe dimensions to simplify computation and sometimes to suppress noise. These layers exist in multiple forms. They are: max pooling layer, mean pooling layer, global pooling layer (spatial pooling layer). For retrieving the detailed low-level features of an image, we use max pooling layer.

Fully Connected Layer: This is a dense layer comprised of neurons, weights and biases, positioned immediately before the output layer in a CNN architecture. Within this layer, every neuron is linked to all the other neurons in the preceding layer, employing the Fully Connected (FC) strategy. This layer often functions as the CNN-based classifier, constituting the network's final layers. The output generated from the final pooling or conv filter layer is passed to the fully connected network layer, where it undergoes flattening before being processed.



Source: Adapted from [2]

Figure 2. CNN framework for image processing

Hybrid Model: Combining architectures, such as a feature fusion approach with ResNet and DenseNet, leverages the strengths of both models. Meaning merging different architectural designs, such as using a combination of ResNet and DenseNet approaches, in order to take advantage of the unique benefits and strengths that each model offers. ResNet is known for its ability to learn deep representations effectively, while DenseNet excels in feature reuse and propagation. Combining these models through feature fusion may lead to a more powerful and robust model thatbenefits from the strengths of each architecture.

STEP A: INPUT DATA

Load Pre-trained Models: Load ResNet and DenseNet models pre-trained on a large dataset like ImageNet.

Remove Final Classification Layers: Remove the final fully connected layers of both models, which are specific to the ImageNet classification task, to use the networks as feature extractors. This means taking out the last layers of neural network models that were designed for classifying images in the ImageNet dataset. By doing this, the models can be used to extract features from input data instead of providing classification outputs.

Define New Classification Head: Define new fully connected layers to combine and process the features extracted from ResNet and DenseNet for the specific task of image forgery detection. This means establishing new fully connected layers that will merge and process the features acquired from ResNet and DenseNet specifically for the purpose of identifying forged images

STEP B: FORWARDING THE DATA

The forward method defines how the input data passes through the network during training and inference. In the forward method:

- Input is passed through both ResNet and DenseNet models to extract features. In DenseNet apply global average pooling to match the feature dimension of ResNet.
- The features from each model are then flattened and concatenated into a single feature vector.
- This combined feature vector is passed through the defined classification head to get the final output, which represents the model's prediction. This means to take all the combined features that have been gathered or generated and pass them through the newly created classification (or categorization) system in order to generate the final result or output.

Define new fully connected layers to combine and process the features extracted from ResNet and DenseNet for the specific task of image forgery detection. This means establishing new fully connected layers that will merge and process the features acquired from ResNet and DenseNet specifically for the purpose of identifying forged images

Localization of Forgery*:* Localization is crucial in forgery detection as it identifies the specific regions in which tampering has occurred. Two powerful techniques for localization within the framework of CNNs are Region Proposal Networks (RPNs) and Attention Mechanisms [Ren, 2017].

Region Proposal Networks: Region Proposal Networks are neural networks designed to propose regions in an image that are likely to contain regions that might be forged. They are a crucial component in many object detection models such as Faster R-CNN.

Anchor boxes: RPNs start by defining a set of anchor boxes of various scales and aspect ratios across the image. These anchor boxes serve as initial guesses for possible regions of interest.

Region Proposals: The RPN scans the image with these anchor boxes and evaluates each one using a small sliding window. For each anchor box, the RPN predicts:

A score indicating the likelihood ofthat box containing a forgery. Refinement values to adjust the position and size of the anchor box to better fit the suspicious region. To reduce redundancy, Non-Maximum Suppression (NMS) is applied to keep only the highest-scoring regions and eliminate overlapping ones.

Integration with CNN

- **Shared Layers:** RPNs share convolutional layers with the main CNN used for feature extraction. The feature maps generated by the CNN are used by the RPN to propose regions, making the system efficient.
- **End-to-End Training:** The RPN and the detection network can be trained jointly, optimizing both region proposal and forgery classification simultaneously.

Benefits of RPNs in Forgery Detection

- **Focused Localization:** RPNs enable the model to concentrate on specific areas of the image, significantly improving the precision of forgery localization.
- **Scalability:** They work with various image sizes and aspect ratios, providing flexible and scalable solutions for detecting forgeries of different scales.

Attention Mechanisms: Attention mechanisms focus the model's capacity on the most suspicious regions. They allow neural networks to focus on the most relevant parts of the input when making predictions.

Implementation in CNNs:

- **Attention Layers:** These layers can be added on top of convolutional layers. They modify the feature maps by focusing on the most informative parts.
- **Attention Maps:** Generate attention maps that visually indicate the areas of the image the model is focusing on. These maps can help in understanding and interpreting the model's predictions.

Benefits of Attention Mechanisms in Forgery Detection

- **Enhanced Sensitivity:** They improve the model's ability to detect subtle and small-scale forgeries that might be missed without focused attention.
- **Improved Interpretability:** Attention maps provide visual insights into why and where the model detects forgery, making the process more transparent and interpretable.

E.Post-processing

In image processing and forgery detection, the outputs produced by Convolutional Neural Networks (CNNs) are further refined using post-processing techniques. These outputs are typically classified to:

- Class Scores or Probabilities: For overall image classification tasks into forged or genuine.
- Segmentation Maps: For pixel-level classification and localization of forged regions.
- Bounding Boxes: For object detection tasks to localize and classify objects within an image.
- Feature Maps: Intermediate representations capturing various image features.
- Heatmaps and Saliency Maps: Visualizations highlighting the important regions contributing to the CNN's decisions.

Post-processing in forgery detection with Convolutional Neural Networks (CNNs) focuses on enhancing the accuracy and reliability of the results. This involves applying various techniques and operations to the raw outputs produced by the CNNs to:

- Enhance the detection accuracy
- Reduce noise and false positives
- Highlight and clearly define forged regions
- Make the results more interpretable and actionable

Here are some of the most commonly used post-processing techniques:

Thresholding

Purpose: Converts the probability map or confidence scores from the CNN into a binary mask to differentiate between forged and genuine regions.

Morphological Operations

Purpose: Refines the binary mask to remove noise, fill gaps, and smooth the edges of detected regions.

Connected Component Analysis

Purpose: Identifies and labels distinct connected regions in the binary mask.

Process

- Labels each connected region (blob) and allows for filtering based on size, shape, or other properties.

Contour Detection and Analysis

Purpose: Detects and analyzes the boundaries of detected regions to understand their shapes and sizes.

Techniques

- Contour Detection: Identifies the contours or edges of the detected regions.
- Shape Analysis: Analyzes the detected contours to verify the shape and size of the regions.

Conditional Random Fields (CRF)

Purpose: Refines the segmentation results by modeling the spatial dependencies between pixels, enhancing the coherence of detected regions.

F.Evaluation of Metrics

- **Performance Metrics:** Use metrics such as accuracy, precision, recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) to evaluate the model's performance.
- Robustness Testing: Test the model against a variety of image manipulations and degradations to ensure robustness in real-world scenarios.

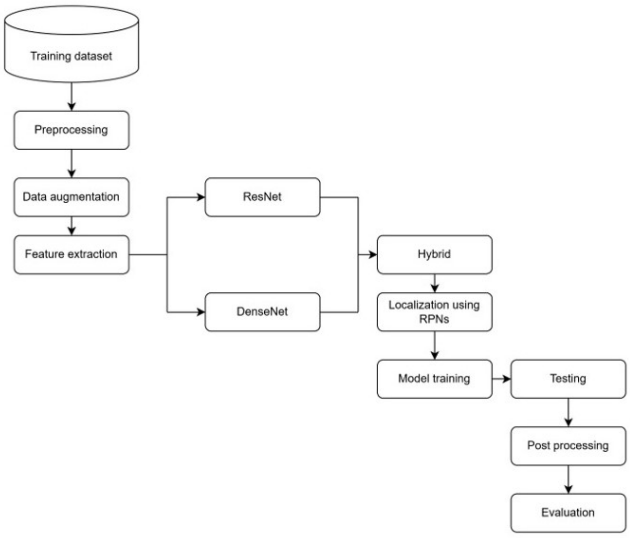


Figure 3. Our proposed methodology for forgery detection

CONCLUSION

Forgery detection in digital images is crucial across multiple domains, from digital forensics and journalism to e-commerce and healthcare. Advanced image processing techniques and machine learning algorithms, particularly Convolutional Neural Networks (CNNs), play a crucial role in enhancing the detection of image manipulations. By examining features at multiple levels, CNNs can effectively identify forgeries.

Pre-processing techniques like noise reduction and histogram equalization improve detection accuracy. As digital content grows, robust forgery detection methods are essential to maintain the integrity and trustworthiness of digital media.

ACKNOWLEDGMENT

We extend our gratitude towards Dr Karunakar Kothapalli at King University, Tennessee for his valuable input. We also thank Professor Sivasankari SS of Dayananda Sagar University for her time.

REFERENCES

Md. Ashif Raja, Active and Passive Detection of Image Forgery: A Review Analysis , retrieved from ion-of-image-forgery-a-review-analysis-IJERTCONV9IS05089

Alzubaidi, L., Zhang, J., Humaidi, A.J. *et al.* Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *J Big Data* **8**, 53 (2021). https://doi.org/10.1186/s40537-021-00444-8

Zanardelli, M. F. Guerrini, R. Leonardi, and N. Adami, "Image forgery detection: a survey of recent deep-learning approaches," *Multimedia Tools and Applications*, Oct. 2022, doi: https://doi.org/10.1007/s11042-022-13797-w.

Boubacar Diallo, Thierry Urruty, Pascal Bourdon, Christine Fernandez-Maloigne, Robust forgery detection for compressed images using CNN supervision, Forensic Science International: Reports Volume 2, December 2020, 100112

Ren, S.K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017, doi: https://doi.org/10.1109/tpami.2016.2577031.

****