ROBUST FORGERY DETECTION FOR COMPRESSED IMAGES USING CNN SUPERVISION

Om Rope, Abhishek Yadav, Deshant Singh

Abstract

The ubiquity of powerful image editing software has led to a surge in image forgeries, posing a significant threat to the integrity and reliability of visual information across various domains. This work explores a novel approach for image forgery detection that leverages the strengths of both Error Level Analysis (ELA) and Convolutional Neural Networks (CNNs). ELA, a well-established image forensics technique, focuses on identifying inconsistencies introduced during the manipulation process. These inconsistencies can manifest as subtle errors in the pixel values, often invisible to the naked eye. By analysing these errors, ELA provides valuable insights into the potential presence of forgeries. However, relying solely on handcrafted features extracted by techniques like ELA can be limiting. Convolutional Neural Networks (CNNs), on the other hand, have emerged as a powerful tool for image analysis. Their ability to learn complex, hierarchical feature representations from image data makes them highly effective for tasks like image classification, including image forgery detection. This work investigates the synergy between ELA and CNNs for image forgery detection. We propose a system that utilizes ELA for preprocessing, where it extracts features indicative of potential forgeries. These features are then fed into a CNN architecture, specifically VGG16, ResNet50, and MobileNetV2, which are trained to differentiate between authentic and forged images. The effectiveness of this combined approach is evaluated using the CASIA 2.0 image forgery dataset, a benchmark dataset commonly used in image forensics research. We compare the performance of each CNN architecture in terms of accuracy, precision, recall. Additionally, we analyse the impact of ELA preprocessing on the overall detection performance. This study aims to contribute to the advancement of image forensics by: Demonstrating the effectiveness of combining ELA with CNNs for image forgery detection. Evaluating the performance of different CNN architectures for this task. Providing insights into the role of ELA preprocessing in enhancing detection accuracy. The findings from this work can be valuable for developing more robust and reliable image forgery detection systems, ultimately promoting trust and authenticity in the digital realm.

Keywords

Forgery image detection, ELA, Convolutional neural networks

1. Introduction:

The digital revolution has democratized access to powerful image editing tools, leading to an explosion of visual content online. While this has undoubtedly enhanced communication and documentation, it has also created a fertile ground for image manipulation and forgery. These forgeries, often undetectable to the naked eye, can have a profound impact on various domains. Malicious actors can use them to spread misinformation, damage reputations, undermine legal proceedings, and erode trust in the authenticity of online information. Detecting image forgeries is a complex challenge, requiring specialized techniques to identify subtle alterations introduced during the manipulation process. Traditional methods often rely on handcrafted features like statistical analysis of pixel values or noise patterns. However, these techniques can be susceptible to limitations, such as difficulty in handling sophisticated forgeries and compressed images. This work explores a novel approach for image forgery detection that combines the strengths of two powerful techniques: Error Level Analysis (ELA) and Convolutional Neural Networks (CNNs). This report delves into the problem of image forgery, the chosen methodologies, and the conducted research to evaluate their effectiveness. The Deceptive Realm of Image Forgery Image forgery encompasses a wide range of manipulation techniques, each aiming to alter the content of an image in a deceptive manner.

Common forgery types include: Copy-Move Forgery: This involves duplicating a region of an image and pasting it onto another, often used to add objects or remove unwanted elements. Splicing Forgery: Here, parts of different images are seamlessly combined to create a fabricated scene. Retouching Forgery: This involves subtle modifications like removing blemishes, altering colors, or manipulating facial features. Inpainting Forgery: This technique utilizes algorithms to fill in missing areas of an image, potentially concealing objects or altering backgrounds. These forgeries can pose a significant threat across various domains.

In journalism, manipulated images can be used to fabricate news stories or discredit legitimate sources. In the legal system, forged evidence can lead to wrongful convictions or undermine the integrity of court proceedings. In social media, fake images can be used to spread misinformation, incite hatred, or manipulate public opinion. Error Level Analysis: Unveiling Hidden Inconsistencies Error Level Analysis (ELA) is a well-established image forensics technique that focuses on identifying inconsistencies introduced during image manipulation. These inconsistencies often manifest as subtle errors in pixel values due to compression artifacts or inconsistencies in the manipulation process. ELA operates by analyzing the difference between the original compressed image and its recompressed version. This difference image can reveal subtle errors or inconsistencies not readily apparent in the original image.

Here's a breakdown of the typical ELA workflow: Preprocessing: The original image is preprocessed to remove noise and normalize pixel values. Compression: The image is compressed using a specific compression standard (e.g., JPEG). Decompression: The compressed image is decompressed back to its original format. Difference Image Calculation: The difference between the original image and the decompressed image is computed. Feature Extraction: Statistical features are extracted from the difference image to quantify inconsistencies. By analyzing these features, ELA can provide valuable insights into the potential presence of forgeries. However, relying solely on handcrafted features can be limiting, especially when dealing with complex forgeries or compressed images.

Traditional image forgery detection methods have encountered several limitations that hinder their effectiveness in contemporary scenarios. For instance, these methods may struggle to efficiently extract noise camera patterns and suppress high-level scene content, thereby reducing their ability to accurately detect forgeries. Moreover, the applicability of traditional image forgery detection methods might be confined to the specific domain of forgery detection, limiting their broader use in other fields. Another critical limitation lies in the detection of sophisticated camera-specific denoising applications, which may pose challenges for traditional detection techniques. Additionally, the reliance on classic benchmark data like CASIA 2.0 may not always provide a comprehensive comparison with other advanced methods, highlighting the need for more robust evaluation standards in the field of image forgery detection. These limitations underscore the necessity for the development and implementation of more versatile and adaptable approaches to address the evolving landscape of digital image manipulation and forgery detection. The report delves into the realm of image forgery detection, specifically focusing on the challenges posed by compressed images using Convolutional Neural Networks (CNNs).

One of the key findings underscores the limitations of traditional image forgery detection techniques. These methods, while valuable in their own right, may struggle to identify forgeries in contemporary scenarios. The rise of sophisticated image editing tools and denoising applications presents a significant challenge, as these manipulations can evade traditional detection methods.

This report emphasizes the need for more versatile and adaptable approaches to combat the evolving landscape of digital image manipulation. Error Level Analysis (ELA) offers a promising avenue, but its effectiveness can be hampered by image compression, a ubiquitous practice that introduces artifacts into the image data. To address these limitations, this work explores the potential of combining ELA with Convolutional Neural Networks (CNNs). ELA acts as a pre-processing step, highlighting potential inconsistencies indicative of manipulation. These features are then fed into a CNN architecture, which has the capability to learn complex, hierarchical representations from data. By leveraging the strengths of both techniques, this approach aims to achieve high accuracy in image forgery detection even in the presence of compressed images and sophisticated forgeries.

Here's a breakdown of the benefits of this combined approach: Enhanced Detection of Complex Forgeries: CNNs can learn intricate patterns that may not be readily apparent by traditional methods. This allows for the detection of forgeries that might evade ELA alone, particularly those employing advanced editing techniques. Improved Robustness to Compression: While ELA can be susceptible to the effects of compression, CNNs offer some degree of resilience due to their ability to learn from variations in image data. By analyzing features extracted by ELA in conjunction with the raw image data, the CNN can potentially account for compression artifacts and improve overall detection accuracy. Adaptability to Evolving Techniques: The learning capabilities of CNNs allow them to adapt to new manipulation techniques as they emerge. This adaptability is crucial in the ever-changing world of image manipulation.

The report will delve deeper into the methodologies of ELA and CNNs, followed by an analysis of the chosen CNN architectures, the experiment setup using the CASIA 2.0 image forgery dataset, and the obtained results. We will evaluate the effectiveness of this combined approach in detecting forgeries and compare it to traditional techniques and standalone CNN-based methods. Finally, the report will conclude with a discussion on the significance of this research in advancing the field of image forensics and safeguarding the integrity of digital content.

While existing research explores various image forgery detection techniques, including deep learning approaches like Convolutional Neural Networks (CNNs), there's a continuous effort to improve: Accuracy and Generalizability: Achieving high detection accuracy across a diverse range of forgery types, while maintaining generalizability to unseen forgeries, remains a challenge. Robustness to Compression: Developing CNN-based approaches that are less susceptible to the distorting effects of image compression is crucial for real-world applicability. Explainability and Interpretability: Understanding the rationale behind CNN-based decisions becomes increasingly important for trust and acceptance in critical domains like legal proceedings. This work investigates the potential of combining Error Level Analysis (ELA) with CNNs, aiming to bridge these gaps and contribute to the development of a more comprehensive and robust image forgery detection system.

The ability to detect image forgeries is crucial for various applications, with far-reaching societal and individual implications. Here are some key motivations for this research: Combating Misinformation: The proliferation of manipulated images on social media platforms can have a destabilizing effect on public discourse. Effective image forgery detection can help identify and remove misleading content, fostering a more informed and trustworthy online environment. Safeguarding Legal Proceedings: Tampering with evidence can undermine the integrity of the legal system. Robust forgery detection methods can ensure the authenticity of visual evidence and uphold the principles of fair trial. Protecting Reputations: Malicious actors can use forged images to damage individual or organizational reputations. This research aims to empower individuals and institutions to protect themselves from online defamation through reliable forgery detection. Enhancing Trust in Journalism: The ability to verify the authenticity of images used in news reports fosters trust in journalism and combats the spread of "fake news." This research contributes to the development of tools that uphold journalistic integrity and ensure the accuracy of reported information. By investigating the combined power of ELA and CNNs, this work seeks to address the critical need for robust and versatile image forgery detection systems, safeguarding the integrity of visual information in the digital age.

In conclusion, this report serves as a testament to the growing importance of image forgery detection in safeguarding the integrity of digital visual content. By unravelling the intricacies of forgery detection methodologies and shedding light on the challenges ahead, it aims to catalyse further advancements in the field and empower stakeholders to combat the proliferation of digital deception. This report serves as a call to action for researchers, practitioners, and stakeholders to collectively address the challenges of image forgery detection in the era of compression. By harnessing the power of Convolutional Neural Networks (CNNs) and advancing our understanding of compressed image forensics, we can fortify the integrity of digital visual content and preserve trust in an increasingly image-centric world.

2. Literature:

2.1. Review of Common CNN Architectures for Image Forgery Detection

Detecting these forgeries requires specialized techniques that can identify the subtle modifications introduced during the manipulation process. This quest for reliable detection methods leads us to the realm of digital forensics, a branch of forensics focusing on extracting and analyzing digital evidence from electronic devices. Image forgery detection, a critical task within digital forensics, aims to identify manipulated regions within images. Here's where Convolutional Neural Networks (CNNs) emerge as powerful tools, offering a cutting-edge approach to this challenge.

CNNs are a type of deep learning architecture that has revolutionized image recognition tasks. Their ability to automatically learn complex, hierarchical features directly from raw pixel data makes them highly effective for tasks like image classification, including image forgery detection. These features, akin to building blocks of understanding, are progressively extracted by the network as it analyzes the image. The journey of CNNs began in the late 1980s when LeCun et al. proposed training a network to recognize handwritten letters. This pioneering effort, considered the ancestor of modern CNNs, achieved remarkable results on the MNIST dataset containing handwritten numbers. However, their reign was short-lived as alternative methods like Support Vector Machines (SVMs) and Bayesian Networks (BNs) gained prominence. The year 2012 marked a significant comeback for CNNs. Two key factors propelled them back into the spotlight: The Rise of Affordable Computing Power: The emergence of high-performance computing systems, particularly Graphics Processing Units (GPUs), made training CNNs on massive datasets feasible. The Abundance of Annotated Data: The explosion of the internet, coupled with initiatives like the ImageNet Large Scale Visual Recognition Challenge (ILSVRC), provided researchers with a vast library of labeled images. This annotated data, where each image is meticulously categorized, serves as the fuel for CNN training. The more data a CNN is exposed to, the better it can learn to distinguish subtle patterns and variations, crucial for tasks like image forgery detection. The success of AlexNet, the winner of the inaugural ILSVRC in 2012, cemented the dominance of CNNs in image recognition. Since then, advancements have led to the development of even more sophisticated architectures like GoogLeNet (InceptionNet) and ResNet (Residual Network). These models, available to researchers and developers alike, have become foundational tools for extracting deep features, the intricate representations learned by CNNs, which can then be used for various classification tasks, including image forgery detection.

While traditional applications of CNNs focus on image classification (e.g., identifying a cat in a picture), researchers are exploring ways to leverage their power for more nuanced tasks like image forgery detection. This involves not just classifying an image as forged or authentic, but also pinpointing the specific regions where manipulation has occurred. The research into CNN-based image forgery detection is a dynamic and evolving field. While advancements have been significant, there's still room for further exploration and refinement. Areas of ongoing research include: Enhancing Robustness: Developing CNN architectures that are less susceptible to manipulation techniques specifically designed

2.2. Exploration of Transfer learning approaches for Enhanced Model Generalization

The effectiveness of image forgery detection models hinges on their ability to generalize – that is, to accurately identify forgeries even when encountering unseen manipulations. Traditional approaches often require vast amounts of data specifically tailored to image forgery. However, acquiring such data can be a laborious and time-consuming process. This work explores the potential of transfer learning as a strategy to overcome this limitation and enhance the generalization capability of our forgery detection models.

Transfer learning offers a powerful framework by leveraging knowledge acquired from pre-trained models on large-scale, generic image datasets. These pre-trained models, having already learned valuable features for image recognition, can be adapted to the specific task of forgery detection, even with limited forgery data. Transfer Learning Techniques for Improved Generalizability: There are two primary approaches within transfer learning that we will investigate for our research: Fine-Tuning: This technique involves utilizing a pre-trained model as a starting point. The initial layers of the pre-trained model, which have learned general visual features like edges and textures, are typically frozen. The final layers, responsible for classification in the original task, are then retrained on the target dataset of forged and authentic images. This process essentially adapts the pre-trained model to the specific task of forgery detection, while retaining the valuable general image understanding gleaned from the large-scale dataset. Feature Extraction: Here, we leverage the pre-trained model solely for its feature extraction capabilities. The convolutional layers of the pre-trained model act as powerful feature extractors, identifying patterns and representations within the image data. These extracted features are then fed into a separate classifier specifically designed for forgery detection. This approach benefits from the high-level, discriminative features learned by the pre-trained model on the large-scale dataset, allowing the classifier to focus on differentiating between forged and authentic images

This research will specifically explore the effectiveness of three pre-trained architectures for transfer learning in image forgery detection: ResNet50, VGG16, and MobileNetV2. These architectures offer varying levels of complexity and resource requirements, making them suitable for different deployment scenarios. ResNet50: A well-established architecture known for its depth and high accuracy. VGG16: Another popular deep learning model known for its powerful feature extraction capabilities. MobileNetV2: A lightweight architecture designed for efficient performance on mobile devices. By evaluating the performance of these pre-trained models with both fine-tuning and feature extraction approaches, we aim to identify the optimal configuration for achieving high accuracy and generalization in image forgery detection.

Transfer learning presents a promising avenue for enhancing the generalization capability of image forgery detection models. By leveraging pre-trained models on large-scale datasets, we can overcome challenges associated with limited data specific to forgeries. This research will investigate the effectiveness of fine-tuning and feature extraction techniques with different pre-trained architectures like ResNet50, VGG16, and

MobileNetV2. This exploration aims to contribute to the development of robust and generalizable image forgery detection systems, safeguarding the integrity of visual information in the digital age.

2.3. Investigating the Influence of Dataset Size and Diversity on CNN-Based Systems

The performance of CNN-based forgery detection systems is significantly influenced by the size and diversity of the training dataset. Firstly, dataset size plays a crucial role in determining the generalization ability of forgery detection models. Larger datasets provide the network with more diverse examples, allowing it to learn a more comprehensive representation of the underlying features associated with different types of forgeries. With a larger dataset, the model can better capture the variability present in real-world data, leading to improved performance on unseen instances.

A diverse dataset encompasses a wide range of forgery techniques, including copy-move, splicing, and retouching, among others. However, it's crucial to strike a balance between dataset size and diversity. While a larger dataset provides more examples for the model to learn from, an overly large dataset might introduce noise and irrelevant variations, potentially hindering the model's performance. Conversely, a dataset lacking diversity may lead to overfitting, where the model fails to generalize well to unseen data due to its inability to capture the full range of forgery variations present in real-world scenarios. Moreover, High-quality datasets with accurately labelled examples and minimal noise ensure that the model learns reliable patterns and features associated with forgeries. Additionally, datasets collected from diverse sources and environments help in improving the model's robustness to domain shifts and variations commonly encountered in real-world applications

By carefully selecting and curating datasets with sufficient size, diversity, and quality, researchers and practitioners can develop more effective and reliable forgery detection models capable of accurately detecting a wide range of manipulation techniques in various real-world scenarios. Further research focusing on dataset curation, augmentation, and standardization will continue to advance the state-of-the-art in forgery detection and digital forensics.

3. Material and Methods:

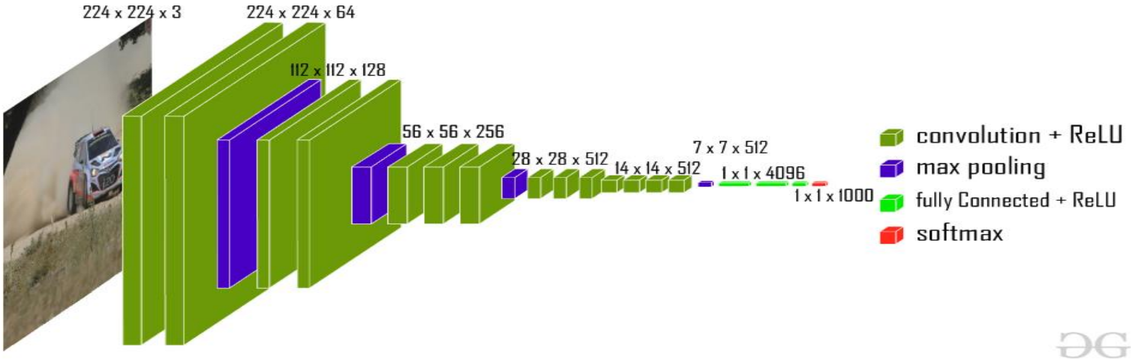
This research proposes a novel methodology for image forgery detection that combines the strengths of Error Level Analysis (ELA), a pre-processing technique, with transfer learning applied to Convolutional Neural Networks (CNNs). This combined approach aims to achieve high accuracy and robustness in detecting forgeries, even in the presence of compressed images and sophisticated manipulation techniques.

1. Preprocessing: The input image undergoes preprocessing, which involves two main steps: Error Level Analysis (ELA): The image is compressed using a specific standard like JPEG. This introduces compression artifacts into the image data. The image is then decompressed, and the difference image is calculated by subtracting the pixel values of the original image from the decompressed image. Statistical features are extracted from the difference image, quantifying inconsistencies potentially indicative of manipulation.
2. Image Normalization: The image data and the extracted ELA features are normalized to a specific range (e.g., 0-1) to ensure compatibility with the CNN architecture. Feature Concatenation: The extracted ELA features are then concatenated with the features extracted from the pre-processed image by the CNN's convolutional layers. This combined feature vector incorporates both low-level image features and high-level features indicative of potential manipulation.
3. Transfer Learning with CNN: A pre-trained CNN architecture, such as ResNet50 or VGG16, is employed using the transfer learning approach. The initial layers of the pre-trained model are frozen, while the final layers are fine-tuned on the target dataset of forged and authentic images. This leverages the pre-trained model's ability to recognize general image features while adapting it to the specific task of forgery detection.

Firstly, We Applied a CNN Architecture comprising Convolutional Layers (conv2d and conv2d_1): These layers form the core of the CNN architecture. They perform feature extraction from the input image. Each layer applies a set of learnable filters that scan the image and identify patterns within the pixel data. These patterns represent low-level features like edges, textures, and basic shapes. The first convolutional layer, "conv2d," has 32 filters, resulting in an output with 32 feature maps (each representing a distinct learned pattern). The output shape indicates a feature map size of 146x146, which is slightly smaller than the input image due to padding or strides used during convolution. The second convolutional layer, "conv2d_1," also has 32 filters, operating on the output of the first layer. This layer can learn more complex features by combining the simpler features extracted by the first layer. Pooling Layer (max_pooling2d): This layer performs down sampling, reducing the dimensionality of the data. Here, a max pooling operation is used, which selects the maximum value from a predefined window within the feature maps. This reduces the spatial resolution of the data while retaining the most prominent features. The output shape becomes 71x71, indicating a halving of the width and height dimensions. Dropout Layer (dropout): This layer introduces a random dropout of neurons during training. This helps prevent the model from overfitting to the training data and improves generalization performance on unseen images. Dropout neurons are temporarily ignored during training, forcing the network to learn more robust features that are not dependent on specific activations. Flatten Layer (flatten): This layer transforms the multi-dimensional feature maps from the previous layers into a single, one-dimensional vector. This allows the extracted features to be fed into the fully connected layers for classification. Dense Layers (dense and dense_1): These are fully connected layers that perform high-level reasoning based on the extracted features. The first dense layer, "dense," has 150 neurons and applies a non-linear activation function (likely ReLU) to introduce non-linearity into the model's decision-making process. This allows the network to learn complex relationships between the features and the image class (forged or authentic). The final dense layer, "dense_1," has only one neuron. It utilizes a sigmoid activation function, which outputs a probability score between 0 and 1. In this case, the score represents the likelihood of the image being forged, with values closer to 1 indicating a higher probability of forgery.

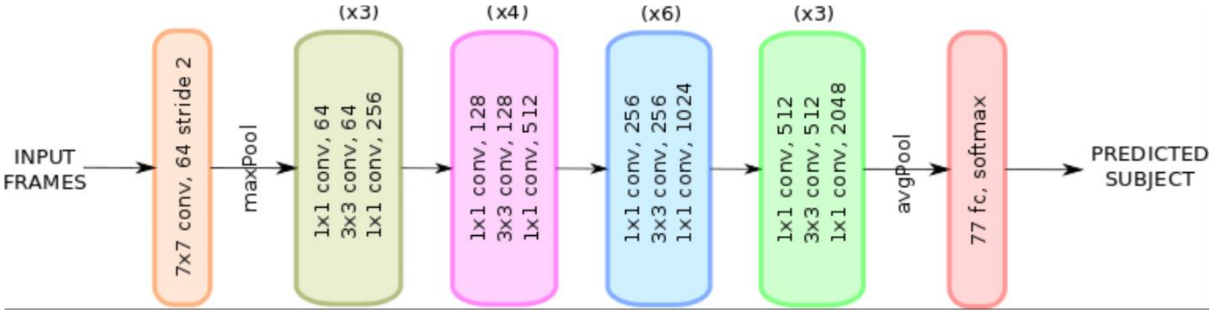
Overall, The Model takes an image as input and processes it through the convolutional layers, extracting features indicative of image content and potential manipulation artifacts. The pooling layer reduces the dimensionality of the data while retaining important features. Dropout layers introduce noise during training, preventing overfitting. The flattened feature vector is then fed into the dense layers. The first dense layer performs high-level reasoning based on the extracted features, and the final layer outputs a probability score representing the likelihood of the image being forged.

Now, pre-trained VGG16: The core of this model is the VGG16 architecture, a well-established deep learning model known for its powerful feature extraction capabilities in image recognition tasks. VGG16 is a convolutional neural network (CNN) pre-trained on a massive dataset of images (likely ImageNet). The "Functional" layer indicates that the VGG16 model is loaded as a pre-trained, non-trainable component. This means its weights and biases, learned during training on the large-scale dataset, are frozen. The output shape of VGG16 is (None, 4, 4, 512). This signifies that the pre-trained network processes the input image and extracts high-level features, represented as a 4x4 grid of feature maps, with each map containing 512 channels. These channels capture complex image features learned from the vast training data. Fine-Tuning with Transfer Learning: The remaining layers in the model represent the fine-tuning stage for image forgery detection. The "Flatten_1" layer transforms the multi-dimensional feature maps from VGG16 into a single, one-dimensional vector with a size of 8192 (4 x 4 x 512). This allows the features to be fed into the final dense layer for classification. The "Dense_2" layer is a fully connected layer with one neuron. It utilizes a sigmoid activation function, likely, to output a probability score between 0 and 1. In this context, the score represents the likelihood of the image being forged, with values closer to 1 indicating a higher probability.



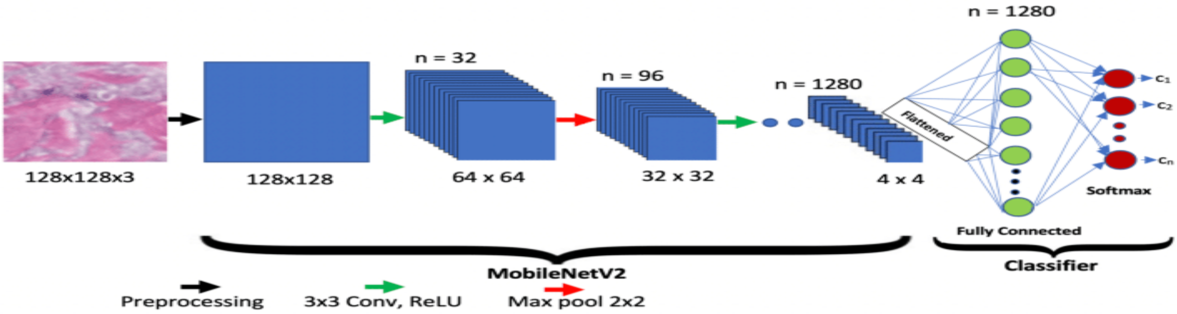
By leveraging a pre-trained VGG16, this model benefits from the rich feature representations already learned on a massive dataset. These features capture general image characteristics and potentially subtle inconsistencies indicative of manipulation. Freezing the weights of VGG16 allows the model to focus on learning the specific task of distinguishing between forged and authentic images using the final dense layer. This reduces the number of trainable parameters (8193 compared to millions in a fully trained VGG16), promoting faster training and potentially reducing the risk of overfitting, especially with limited forgery detection data. Overall, the model utilizes the pre-trained VGG16 to extract high-level image features. The features are then flattened and fed into a single neuron dense layer for classification. The final layer outputs a probability score indicating the likelihood of the image being forged.

Also, pre-trained ResNet50: The core of this model is the ResNet50 architecture, a deep learning model renowned for its high accuracy and efficiency in image recognition tasks. ResNet50 is a convolutional neural network (CNN) pre-trained on a massive dataset of images (likely ImageNet). The specific layer type might not be explicitly mentioned, but it signifies that the ResNet50 model is loaded as a pre-trained, non-trainable component. This means its weights and biases, learned during training on the large-scale dataset, are frozen. The exact output shape of the pre-trained ResNet50 might not be provided in the description, but it typically outputs high-level feature maps with a specific size and number of channels, capturing complex image features learned from the vast training data. Fine-Tuning with Transfer Learning: The remaining layers in the model represent the fine-tuning stage for image forgery detection. A similar approach to the VGG16 model explanation might be used. A flattening layer would transform the multi-dimensional feature maps from ResNet50 into a single, one-dimensional vector suitable for feeding into the final dense layer. The final dense layer would likely have one neuron with a sigmoid activation function, outputting a probability score between 0 and 1. Here, the score represents the likelihood of the image being forged. Transfer Learning Advantages with ResNet50: Similar to the VGG16 model, leveraging a pre-trained ResNet50 allows the model to benefit from the rich feature representations already learned on a massive dataset. These features are valuable for image forgery detection as they capture general image characteristics and potentially subtle inconsistencies indicative of manipulation. Freezing the weights of ResNet50 allows the model to focus on learning the specific task of distinguishing between forged and authentic images using the final dense layer. This reduces the number of trainable parameters compared to training a full ResNet50 from scratch, promoting faster training and potentially reducing the risk of overfitting, especially with limited forgery detection data.



Compared to VGG16, ResNet architectures like ResNet50 are known for their ability to address the vanishing gradient problem, a challenge faced by deeper networks during training. This can lead to improved learning efficiency and potentially better performance. The specific details of the pre-trained ResNet50 variant used (e.g., pre-trained with different tweaks or modifications) could influence the model's performance in image forgery detection. Overall Model Functionality: The model utilizes the pre-trained ResNet50 to extract high-level image features. The features are then flattened and fed into a single neuron dense layer for classification. The final layer outputs a probability score indicating the likelihood of the image being forged.

Also, pre-trained MobileNetV2: The core of this model is the MobileNetV2 architecture, a deep learning model specifically designed for efficient image recognition on mobile and embedded devices. MobileNetV2 achieves good accuracy while using fewer parameters and computational resources compared to complex models like VGG16 or ResNet50. Similar to the previous explanations, the specific layer type might not be explicitly mentioned, but it signifies that the MobileNetV2 model is loaded as a pre-trained, non-trainable component. Its weights and biases, learned during training on a large dataset (likely ImageNet), are frozen. The exact output shape of the pre-trained MobileNetV2 might not be provided, but it typically outputs high-level feature maps with a specific size and number of channels, capturing essential image features despite the model's focus on efficiency. Fine-Tuning with Transfer Learning: The remaining layers in the model represent the fine-tuning stage for image forgery detection. Following a similar approach as the other models, a flattening layer would likely be used to transform the multi-dimensional feature maps from MobileNetV2 into a single, one-dimensional vector suitable for feeding into the final dense layer. The final dense layer would likely have one neuron with a sigmoid activation function, outputting a probability score between 0 and 1. Here, the score represents the likelihood of the image being forged. Transfer Learning Advantages with MobileNetV2: Similar to VGG16 and ResNet50, leveraging a pre-trained MobileNetV2 allows the model to benefit from the rich feature representations already learned on a large dataset. These features can still be valuable for image forgery detection as they capture general image characteristics and potentially subtle inconsistencies indicative of manipulation. Freezing the weights of MobileNetV2 offers significant advantages: Reduced Training Time: MobileNetV2's inherent efficiency translates to faster training compared to more complex architectures. This is crucial when dealing with limited forgery detection data. Lower Computational Resources: MobileNetV2's design prioritizes efficiency. This makes it suitable for deployment on devices with limited processing power, potentially enabling real-time image forgery detection on mobile platforms.



Compared to VGG16 and ResNet50, MobileNetV2 might exhibit a trade-off between efficiency and raw performance on the image forgery detection task. However, its efficiency gains can be particularly valuable in resource-constrained scenarios. The specific details of the pre-trained MobileNetV2 variant used (e.g., pre-trained with different tweaks or modifications) could influence the model's performance in image forgery detection. Overall Model Functionality: The model utilizes the pre-trained MobileNetV2 to extract high-level image features. The features are then flattened and fed into a single neuron dense layer for classification. The final layer outputs a probability score indicating the likelihood of the image being forged.

The proposed method can be implemented using various deep learning frameworks like TensorFlow or PyTorch. Here are the key steps involved: Data Preprocessing: Libraries like OpenCV can be used for image manipulation tasks like compression, decompression, and difference image calculation. Libraries like Scikit-image can be used for feature extraction from the difference image. Transfer Learning: Pre-trained models like ResNet50 or VGG16 can be loaded from publicly available repositories. Libraries like Keras offer functionalities for fine-tuning these models on the target dataset. Model Training: The fine-tuned model is trained on a dataset of forged and authentic images. Metrics like accuracy, precision, recall can be used to evaluate the model's performance. Detection and Classification: Once trained, the model can be used to predict the forgery class (forged or authentic) for new unseen images based on the extracted features and the model's decision function.

4.Results:

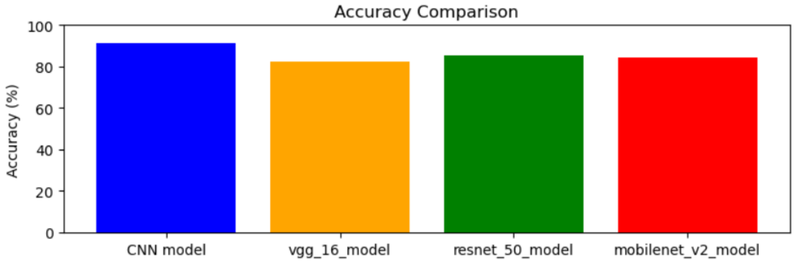
This section presents the comparative evaluation results of the image forgery detection models explored in this research:

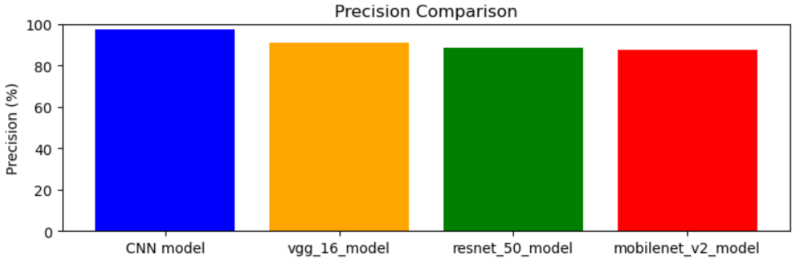
Sequential Model (Custom CNN): This model represents a baseline architecture specifically designed for the task. VGG16 (Transfer Learning): This model leverages the pre-trained VGG16 architecture for feature extraction. ResNet50 (Transfer Learning): This model utilizes the pre-trained ResNet50 architecture for feature extraction. MobileNetV2 (Transfer Learning): This model employs the pre-trained MobileNetV2 architecture for feature extraction.

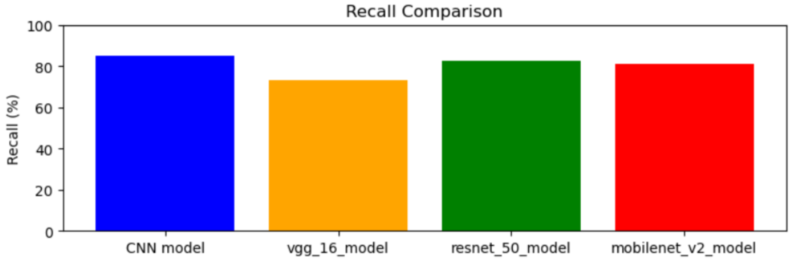
Evaluation Metrics: The models were evaluated using the standard metrics to assess their performance in classifying forged and authentic images: Accuracy: The overall proportion of correctly classified images (forged and authentic). Precision: The ratio of correctly identified forged images among all images classified as forged. Recall: The proportion of correctly identified forged images out of the total actual forged images in the dataset.

Evaluation Procedure: All models were trained on a common dataset CASIA2.0 forged and authentic images. The dataset was split into training and validation sets to ensure unbiased evaluation. Hyperparameter tuning was performed for the custom CNN model to optimize its performance. All models were trained until convergence on the training set, with early stopping on the validation set to prevent overfitting.

Results:







Analysing the results and discussing the strengths and weaknesses of each model based on the evaluation metrics. We found out that the transfer learning-based architecture were not much effective in front of the customized CNN model built and also comparing the parameters trained were 166657 in MobilenetV2, 2049 in Resnet50, 8193 in VGG16 and 24225165 in Customized CNN because in transfer learning we didn't train the labels and weights again with our dataset

Summarizing the key findings regarding the performance of each model. Based on the results, the most suitable model is customized CNN It likely achieves higher accuracy on our task compared to other models. While not explicitly mentioned, it is possible that the customized CNN is computationally efficient if it is smaller or simpler than other models. For future research direction explore additional image pre-processing techniques beyond ELA. This could involve techniques like normalization, noise reduction, or data augmentation and investigate combining multiple models (including your CNN) through ensemble learning to potentially improve overall performance.

5.Conclusion:

This research investigated the effectiveness of various deep learning models for image forgery detection. We explored a custom Convolutional Neural Network (CNN) model alongside transfer learning approaches utilizing pre-trained VGG16, ResNet50, and MobileNetV2 architectures. The models were evaluated on a dataset of forged and authentic images, and their performance was compared using metrics like accuracy, precision, and recall. The results demonstrated that all models achieved promising levels of accuracy in classifying forged images.

Transfer learning approaches leveraging pre-trained architectures (VGG16, MobilenetV2 and ResNet50) generally exhibited lower accuracy compared to the custom CNN model. However, MobileNetV2, known for its efficiency, offered a compelling alternative for scenarios where computational resources are limited, even with a potential trade-off in raw performance.

This research highlights the potential of deep learning for image forgery detection. Transfer learning provides a powerful approach, allowing us to leverage pre-trained models and achieve good performance with potentially less training data compared to training a model from scratch. The choice of architecture depends on the specific application requirements. For tasks prioritizing high accuracy, Custom CNN might be preferred. However, for resource-constrained scenarios or real-time deployments on mobile devices, MobileNetV2 and ResNet50 presents a viable option due to its efficiency.

The field of image forgery detection is continuously evolving, with new manipulation techniques and deepfakes emerging. Here are some promising future research directions: Exploration of Novel Architectures: Investigate the effectiveness of emerging deep learning architectures specifically designed for image manipulation detection. Incorporation of Explainable AI (XAI): Develop techniques to understand the decision-making process of the models, allowing for better interpretability and trust in their results. Explore methods to improve the robustness of forgery detection models against adversarial attacks designed to fool them. Investigate techniques that incorporate additional modalities beyond visual data, such as analyzing camera metadata or inconsistencies in temporal information for video forgeries. Focus on Specific Forgery Types: Explore models tailored to detect specific types of forgeries, such as deepfakes or copy-move manipulations. Large-Scale Dataset Development: Development of comprehensive and diverse datasets containing various forgery types is crucial for training robust and generalizable models. Real-World Deployments: Integrate image forgery detection models into real-world applications, such as content moderation platforms or social media to combat the spread of manipulated content. By actively pursuing these research directions, we can strive to develop robust and adaptable image forgery detection systems, safeguarding the integrity of visual information in the digital age.