Advancements in Image Forgery Detection, 2023

IMAGEGUARD

Enhancing Image Forgery Detection A Comprehensive Approach using ELA, CNN, and VGG16

Harshita Badhan[1], Ishpreet Kaur[1], and Sandhya Yadav[1]

[1]Department of Computer Engineering, National Institute of Technology, Kurukshetra

November 23, 2023

Abstract

Images serve as essential sources of authentic data. In an age of rapid progress in science and technology, Image forgery has become increasingly prevalent posing a serious menace. This threatens to undermine the validity of the shared information. The rise of image forgery poses a significant threat to the authenticity of image content. This paper addresses overcoming this through a deep learning approach, combining Error Level Analysis (ELA) with a customized Convolutional Neural Network (CNN). Additionally, we explore another method integrating VGG16, aiming to reinforce the detection of image tampering in the digital terrain.

Keywords : Deep Learning, Image Forgery, ELA, CNN, VGG16

1 Introduction

The global presence of images as a primary source of communication in the today's era accentuates the integral part they play in converying information. From social media to information reports, images are amongst some of the most potent tools for storytelling and information dissemination. However, the rapid addition of advanced digital image processing mechanisms has given rise to a concerning trend—image forgery.

Image forging, the intentional alterating of an image's content for deceitful purposes, has developed into a complex challenge. This practice endangers the authenticity of the digital content shared, posing a severe threat to the integrity of online information. The motivations behind image forgery may range from political manipulation and propaganda to biased misrepresentation and cybercrime. The substances of forged images expand beyond mere manipulation; the potential to swap perceptions, influence decision-making processes, and, in extreme cases, lead to misinformation and societal unrest are some of the critical challenges posed by escalation in advancements of image forgery techniques.

In response to this issue, our research addresses the critical need for robust image forgery detection methods. By integrating Error Level Analysis (ELA) with a custom Convolutional Neural Network (CNN) and exploring an alternative approach with the VGG16 architecture, IMAGEGUARD aim to reinforce the identification of forged images and distinguish between geunine and altered images. This research contributes to the ongoing efforts to defend the validity of digital visual content, ensuring reliability in an era marked by the all-growing threat of image manipulation.

2 Related Works

Previous studies in image forgery detection have established a foundation using varied methods to tackle the problems posed by manipulated image content. Previous research has delved into two main approaches: passive and active. Passive methods examine statistical features, pixels, and frequency domains without needing knowledge of the original image. On the other hand, active methods involve using techniques like adding data, such as watermarking, digital signatures, and robust hashing, to aid in later authentication. The following figure describes the extensive amount of research done previously on image forgery detection.

Table 1: Summary of Related Work in Image Forgery Detection

Title	**Authors**	**Dataset**	**Validation Accuracy**	**Approach**
A Study on Image Forgery Detection Techniques	Shijo Easow, Dr. L. C. Manikandan	Dataset 1	None	Discussion of different kinds of image forgery techniques like Active and Passive along with the summary of various techniques that help detect forgeries.
Image forgery detection using Deep Neural Network, 2022	Anushka Singh, Jyotsna Singh	CASIA V2.0	75.68% (CNN), 90.02% (CNN_ELA), 94.52% (CNN_sharpen_ela)	Method 1, employing a basic CNN with ELA and sharpening, and Method 2, utilizing transfer learning with VGG-16 and ResNet50, emphasizing fine-tuning for improved image forgery detection accuracy.
Image Forgery Detection Using Deep Neural Network, 2023	Dr. N P Nethravathi, Bylla Danny Austin, Dadireddy Sai Praneeth Reddy, Grandhi Venkata Naga Satya Pavan Kumar, Guduru Karthik Raju	CASIA V1.0 3	75.58% (ELA+CNN), 75.87% (VGG16)	ELA-CNN combines passive Error Level Analysis with a customized CNN, and VGG-16 undergoes transfer learning for image forgery detection.
Image Forgery Detection	Dipanshu Narayan, Himanshu, Rishabh Kamal	CASIA2	97.7%	The study uses block processing and a Convolutional Neural Network (CNN) for efficient detection of copy-move forgeries in both transformed and untransformed images.
Image Forgery Detection with ELA and DenseNet121	LABID93 (Kaggle)	v3 dataset	96%	Image forgery detection using Error Level Analysis (ELA) coupled with the DenseNet121 architecture.

3 Methodology

Error Level Analysis with Convolutional Neural Network (ELA-CNN)

Overview of ELA

ELA is used to identify tampering in images by assessing the consistency in different compression levels contained in the image. The tampered areas in an image contain compression levels that differ more frequently from the surrounding unedited areas. ELA helps identify such inconsistencies which makes it simpler to detect forgeries.

CNN architecture

In our project, we have used a customized CNN model which contains an input layer, a convolution layer for performing the convolution operation and feature detection, and fully connected layers. During training, we used the ReLU activation function and categorical cross_entropy loss function. To prevent overfitting, the model used a dropout layer. The hidden layers consisted of various types of layers including Convolutional Layers, Max Pooling, Dropout Layers, and Dense Layers. The architecture is described in Table 2 for better understanding.

lX

Layer	Description
Input	(128, 128, 3)
Conv2D_1	(124, 124, 32) filters: 32, kernel_size: (5, 5), activation: relu
Conv2D_2	(60, 60, 32) filters: 32, kernel_size: (5, 5), strides: (2, 2), activation: relu
MaxPool2D	(30, 30, 32) pool_size: 2, strides: None, padding: valid
Dropout	(30, 30, 32) rate: 0.25
Flatten	28800
Dense_1	256 activation: relu
Dropout	256 rate: 0.50
Dense_2 (Output Layer)	Number of Classes activation: softmax

Table 2: CNN Architecture

Dataset details

We have used the CASIA 2.0 dataset, developed by the Chinese Academy of Sciences Institute of Automation (CASIA), which is widely used in image forensics research and the detection of image forgery. CASIA 2.0_Groundtruth, a specific version of the dataset, includes a wide variety of images with various kinds of manipulations like copy-move forgery and splicing. It contains 12,614 images (7491 authentic and 5123 tampered) of color images 384x265 pixels. We separated the dataset into training and testing data using the 80%-20% format. Besides, the ELA technique provides the necessary preprocessing aimed at enhancing the necessary features of the dataset.

Pre-trained VGG16 model with ELA

Overview of VGG16

A popular deep learning, pre-trained model for image classification is the VGG16 model which contains 16 weight layers, including 13 convolutional layers and 13 fully-connected layers. The max pooling layers have a pool size of 2x2, whereas the convolutional layers have 3x3 filters with a stride of 1. This model can successfully extract features because it has already been trained on the ImageNet dataset. We have decided to use this model for comparison with the ELA and CNN model because of its noteworthy performance in computer vision applications.

Architecture of VGG16

The VGG16 model used in the project consists of convolutional and fully-connected layers as described above. We have used max pooling layers to downsample the data. The activation function used throughout is ReLU which introduces non-linearity to the model. The droupout rate is set to 0.25 after the Flatten Layer and set to 0.5 after the first Dense Layer. The last few layers of the VGG16 model are used for the specific classification task, including a flatten layer, a dense layer with 1024 units and ReLU activation, a dropout layer, and a final dense layer with softmax activation. The optimiser used is RMSprop optimizer with a specified learning rate of 0.001.

Dataset and Finetuning the model

VGG16 is a pre-trained model that uses the ImageNet dataset for image forgery detection. The finetuning of the model is done by modifying the final layers for forgery detection and the weights that are learned from the previous layers are used to capture relevant features.

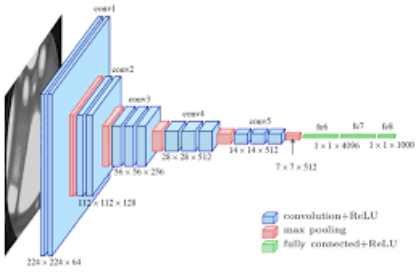

Figure 1: Basic Architecture of VGG16 Model

4 Experimental Results

Table 3: Summary of Experimental Results

(r2cm)1-2 **Method**	**Accuracy (%)**
A Study on Image Forgery Detection Techniques	None
Image forgery detection using Deep Neural Network, 2022	94.52
Image Forgery Detection Using Deep Neural Network, 2023	75.87
Image Forgery Detection	97.7
Image Forgery Detection with ELA and DenseNet121	96
custom CNN (Proposed Method 1)	*NA*
ELA + CNN (Proposed Method 2)	*100*
ELA + VGG16 (Proposed Method 3)	*100*
(r2cm)1-2	

Conclusions and Future Work

In conclusion, our investigation into image forgery detection using ELA combined with CNN and ELA combined with VGG16 models has given encouraging results. The ELA technique, which highlights inconsistencies in error levels introduced during image manipulation, serves as an effective pre-processing step to improve the performance of deep learning models used subsequently. The CNN and VGG16 architectures demonstrated robust capabilities in distinguishing authentic and manipulated images. The combination of ELA with these deep learning models has proven to be a strong strategy for detecting image alteration. However, the performance depends on the choice of hyperparameters and dataset quality. Besides, the ELA and CNN model is computationally light in comparison to the ELA and VGG16 model which is computationally heavy due to the large number of layers involved. Overall, our study contributes to the growing field of digital forensics and highlights the potential of ELA in the field of deep learning for accurate and reliable image forgery detection.

In the domain of image forgery detection, there is high scope for future enhancement and exploration. The use of more advanced deep learning architectures such as attention-based models or transformer networks, could potentially further refine the discernment of subtle manipulations in images. The integration of AI techniques could offer transparency in model decision-making, helping forensic experts understand and validate the detection outcomes. Additionally, investigating the robustness of detection models against adversarial attacks is required to strengthen their reliability in real-world scenarios. We can also consider exploring multimodal information and integrating it into our model to offer a more comprehensive approach to detecting forged content. Lastly, the creation of larger and more diverse datasets, incorporating a variety of forgery techniques, would aid in the training of the models with improved generalization capabilities. These techniques can aid significant advancements in the field of image forgery detection, ensuring its responsiveness to evolving practices in the digital realm.

References

[1] Accents Journals. "Title of the Paper." Available online: https://www.accentsjournals.org/paperInfo_online.php?journalPaperId=926&countPaper=251

[2] IEEE Xplore. "Title of the Paper." Available online: https://ieeexplore.ieee.org/document/10151341

[3] GitHub - casia2groundtruth. "Repository for CASIA2 Groundtruth." Available online: https://github.com/namtpham/casia2groundtruth

[4] ResearchGate. "Title of the Paper." Available online: https://www.researchgate.net/publication/358021554_Image_forgery_detection_using_Deep_Neural_Network