IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CNN-Based Image Tampering Detection Model

Serene Das
Student of Computer Engineering
Usha Mittal Institute Of Technology
Mumbai, India

Vaishnavi Gagare
Student of Computer Engineering
Usha Mittal Institute Of Technology
Mumbai, India

Sonal Mhatre
Student of Computer Engineering
Usha Mittal Institute Of Technology
Mumbai, India

Prof. Samidha Vengurlekar
Department of Computer Engineering
Usha Mittal Institute Of Technology
Mumbai, India

***Abstract*—Image manipulation has become increasingly prevalent in today's society, with powerful editing tools allowing for easy and sophisticated changes to be made to digital images. However, this has also led to the misuse of digitally manipulated images for fraudulent, propaganda, and deceptive purposes. In response, deep learning algorithms, such as Convolutional Neural Networks (CNNs) have been developed accurately and efficiently for detecting various types of image forgeries, such as copy-move, splicing, retouching, and more. This paper outlines the key elements of the powerful image editing tools available, the misuse of digitally manipulated images, and the potential of deep learning algorithms for detecting image forgeries. Industry-standard image editing software like Adobe Photoshop and GIMP, have revolutionized the way digital images are edited and manipulated. These tools offer advanced features such as layers, filters, and masks, allowing precise and sophisticated changes to be made to images. For example, layers allow for different elements of an image to be edited separately, while filters provide a range of effects that can be applied to an image. As image manipulation techniques continue to evolve, the integration of deep learning with image processing holds great promise in ensuring the authenticity and credibility of images in the digital era.**

keywords *- Image Image Tampering, Machine Learning, Convolutional Neural Networks, Deep Learning, Tampering Methods, Detection Tools*

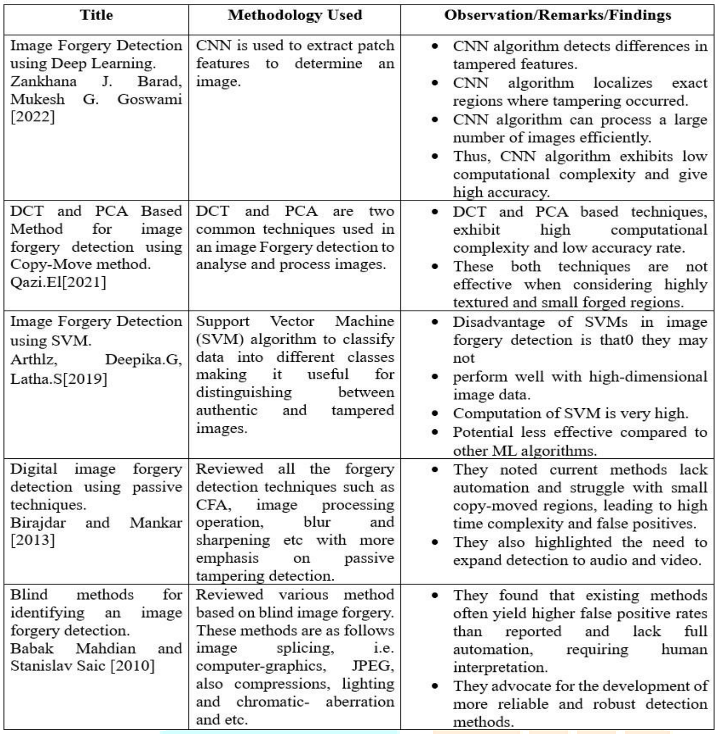
I. Introduction

Today, images play an important role in many fields such as medicine, education, digital forensics, sports, scientific research and media and have become an important source of information. Creating fake photos is very easy thanks to software such as Photoshop,GIMP,Android applications such as photohacker [9]. Basically, Image forgery or manipulation of an image is the deceptive alteration of visual content, containing digital images or video data, with the intent to mislead or deceive. If new content is copied from the same image itself, it is called copy drive tampering, and if new content is copied from different images, it is called image splicing.This manipulation blurs the distinction between what is authentic and what is invented, posing significant challenges across diverse fields such as forensics, journalism, and digital media authentication[8]. The motivations behind image tampering are diverse, including fraud, misinformation, and enhancement of visual appeal. Perpetrators may manipulate images to deceive individuals, sway public opinion, or create misleading content. Common methods of image tampering include copying, modifying, or re-contextualizing elements within images, resulting in the distribution of digitally altered content across online platforms. It greatly affects the reliability of visual information across various fields. In forensic investigations, tampered images can seriously compromise evidence accuracy, leading to unfair outcomes. Similarly, in journalism, forged images make news stories less trustworthy, reducing public faith in the media [1]. Therefore, Photo spoofing or image forgery detection is crucial for determining if a photo has been altered, relying on evidence to confirm its authenticity. To tackle this challenge, researchers are turning to advanced machine learning and deep learning algorithms.They have emerged as powerful tools for automating the detection of fake images.Significant progress has also been made in developing detection tools that leverage deep learning algorithms. These tools can achieve high accuracy and efficiency in identifying forged images[9]. In summary, image forgery detection plays a crucial role in safeguarding the integrity of visual information. By leveraging advanced technologies such as deep learning algorithms, researchers are making strides in developing effective detection tools. Continued research and innovation in this field are essential for preserving the trustworthiness of digital content.

II. Literature Survey

This literature review covers the latest advances in search of, machine learning techniques, deep learning techniques and detection tools.This review has been conducted over number of techniques to understand their methodology and their major shortcomings. The related work has been defined through the comparison table below :-

Table 2.1: Literature Survey of Image Forgery Detection

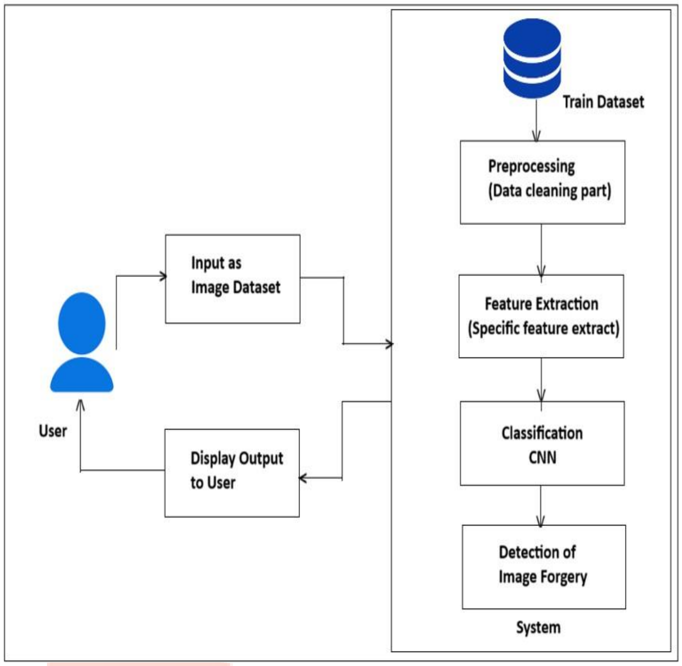


Title	Methodology Used	Observation/Remarks/Findings
Image Forgery Detection using Deep Learning. Zankhana J. Barad, Mukesh G. Goswami [2022]	CNN is used to extract patch features to determine an image.	• CNN algorithm detects differences in tampered features. • CNN algorithm localizes exact regions where tampering occurred. • CNN algorithm can process a large number of images efficiently. • Thus, CNN algorithm exhibits low computational complexity and give high accuracy.
DCT and PCA Based Method for image forgery detection using Copy-Move method. Qazi.El[2021]	DCT and PCA are two common techniques used in an image Forgery detection to analyse and process images.	• DCT and PCA based techniques, exhibit high computational complexity and low accuracy rate. • These both techniques are not effective when considering highly textured and small forged regions.
Image Forgery Detection using SVM. Arthlz, Deepika.G, Latha.S[2019]	Support Vector Machine (SVM) algorithm to classify data into different classes making it useful for distinguishing between authentic and tampered images.	• Disadvantage of SVMs in image forgery detection is that0 they may not • perform well with high-dimensional image data. • Computation of SVM is very high. • Potential less effective compared to other ML algorithms.
Digital image forgery detection using passive techniques. Birajdar and Mankar [2013]	Reviewed all the forgery detection techniques such as CFA, image processing operation, blur and sharpening etc with more emphasis on passive tampering detection.	• They noted current methods lack automation and struggle with small copy-moved regions, leading to high time complexity and false positives. • They also highlighted the need to expand detection to audio and video.
Blind methods for identifying an image forgery detection. Babak Mahdian and Stanislav Saic [2010]	Reviewed various method based on blind image forgery. These methods are as follows image splicing, i.e. computer-graphics, JPEG, also compressions, lighting and chromatic- aberration and etc.	• They found that existing methods often yield higher false positive rates than reported and lack full automation, requiring human interpretation. • They advocate for the development of more reliable and robust detection methods.

III. Proposed System

In this image forgery detection project, we begin with an input database primarily comprised of image datasets. Our training dataset, containing a vast array of images, is utilized to train the system. The preprocessing stage, focusing on data cleaning, ensures the accuracy of subsequent analyses by rectifying inconsistencies and outliers within the data [3] .Feature extraction, facilitated by the initial layers of a Convolutional Neural Network (CNN), automatically identifies crucial visual elements such as textures, shapes, and edges. These extracted features are then classified using a CNN, distinguishing between authentic and manipulated regions within the images [6]. Through training with a dataset comprising both authentic and manipulated images, the CNN learns to differentiate between the two categories. Loss function and backpropagation techniques are employed to refine the network's parameters, minimizing errors in identifying forgeries. The classification stage of a Convolutional Neural Network (CNN) involves teaching the network to categorize images into different classes or labels. This process helps the CNN distinguish between authentic and manipulated regions within images by learning patterns and features from the training data. Once trained, the CNN can accurately classify new images, allowing it to detect image forgeries effectively [9]. Following training, the CNN undergoes testing to evaluate its performance, utilizing metrics like accuracy, precision, recall, and F1-score to assess its effectiveness. Finally, the system detects image forgeries, presenting the outcomes to the user through visual or informational outputs, which may include details on manipulated regions, confidence scores, and relevant metadata.

Figure 3.1: System Architecture



IV. Methodology

CNN Model and Training Process: Convolutional Neural Networks are widely used in image forgery detection due to their ability to automatically learn features from images. In this overview, we have used a CNN architecture made up of different convolutional, Maxpooling, dense, dropout, and fully connected layers. Convolutional layers apply filters (kernels) that slide across the image, extracting low-level features like edges, textures, and colors. To avoid overfitting pooling layer is used which reduces the output map of the convolutional layer. During the training process common activation functions like ReLU (Rectified Linear Unit) were used that allow the network to learn more complex relationships between features and categorical binary cross-entropy loss functions were applied.Fully-connected layers connect all the neurons from the previous layer (often flattened from a feature map) to every neuron in the current layer. The hidden layers incorporated a combination of convx2DL, Max pooling, dropout, flatten, and dense layers for enhanced feature extraction and model regularization Dataset preparation: By training and testing the CNN model using the CASIA V1.0 Dataset, we were able to extend the analysis of the model in this study. To train a robust model for detecting manipulated images, our dataset incorporates a diverse range of tampered photos, including splices, CFA artifacts, and copy-move forgeries. We further divided the data into training and testing sets to ensure the model's generalizability. The categorical cross entropy loss function, SGD optimizer, and a learning rate of 0.01 and were used to train the model. Image Forgery Detection Tools: Image forgery detection tools utilize various techniques to identify forged images[10]. These forgery tools can be used to enhance the accuracy and reliability of image authentication and forensic analysis. Tools:

- **ELA**: It works by highlighting differences in the error levels present in various regions of an image after compression.
- **Copy-move**: It detects regions within an image that have been copied and pasted from one location to another
- **Compression Detection**: Process of identifying inconsistencies or anomalies in the compression characteristics of an image that may a indicate tampered region.
- **metadata analysis**: Metadata provides information about various aspects of an image, such as its creation, modification history, and even the device used to capture it.
- **CFA(Color Filter Array) artifact detection**: This involves the use of Convolutional Neural Networks to identify and mitigate artifacts introduced by the Bayer filter array commonly used in digital cameras.
- **Noise inconsistency**: It refers to the challenge of detecting noise characteristics in different parts of the image that do not match.
- **String Extraction**: In the context of image forgery detection, ”string” typically refers to specific visual patterns that indicate manipulation.
- **Image extraction**: It involves training a CNN to automatically extract features from images that are indicative of tampering.

V. Result and Analysis

We propose a new system Convolutional Neural Network in machine learning and computer vision to solve the problems above. After being trained on an expanded dataset with manipulated images, we report percentage accuracy in forgery detection. After analysis of the model, we got the best accuracy of training 97.60 percentage and 97.60 percentage validation by going through 32 epochs after testing, with a training loss of 0.0805 and testing loss of 0.0682.

Table 5.1: COMPARISION WITH OTHER MODELS

DATASETS	MODELS ACCURACY		
	CNN [Proposed]	VGG-19 [7]	ResNet [10]
Training Images (Authenticate, Tampered)	97.60%	95.2%	83.22%
Testing Images (Authenticate, Tampered)	97.60%	92.8%	30.66%

Additionally, we have built a detection model in which the person performing the analysis of the tampered image will be aware of the forgery type performed on the original image, the use of a specific detection technique will work here. This system analyzes uploaded images for signs of manipulation, including Double JPEG Compression, Copy-Move forgery, CFA- artifacts, and potential Error Level Analysis. It additionally retrieves textual content and meta-data contained within the image. The user interface features a clear layout with an image upload area, a results display box, and ten interactive buttons with helpful instructions for easy navigation. Notably, the system operates entirely on the user’s device, eliminating the need for an internet connection.

Figure 5.2: CNN Prediction

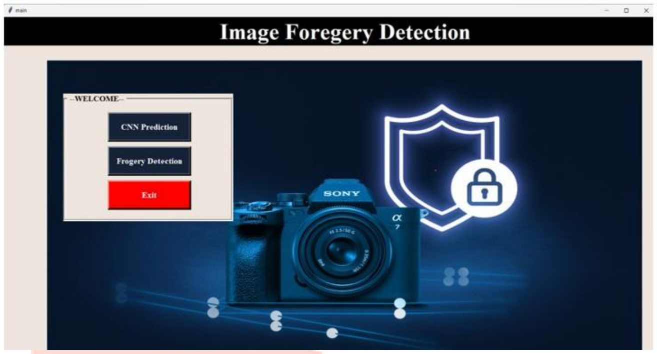


Figure 5.3: Detected Image is Forged

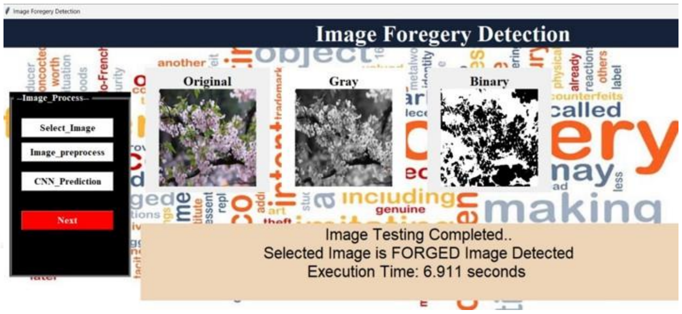
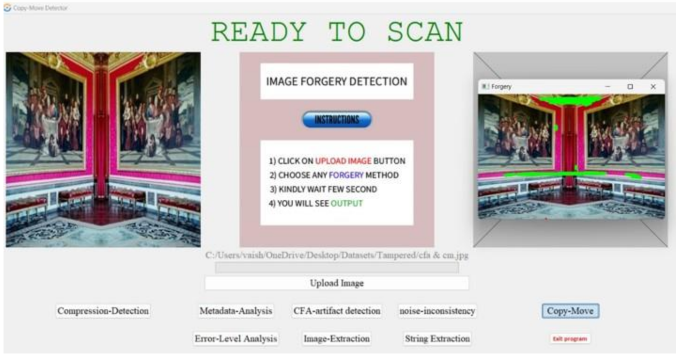


Image Testing Completed..
Selected Image is FORGED Image Detected
Execution Time: 6.911 seconds

Figure 5.4: The detection tool identifies instances of copy-move in input image



1) CLICK ON UPLOAD IMAGE BUTTON
2) CHOOSE ANY FORGERY METHOD
3) KINDLY WAIT FEW SECOND
4) YOU WILL SEE OUTPUT

C:/Users/vaish/OneDrive/Desktop/Datasets/Tampered/cfa & cm.jpg

VI. CONCLUSION

The survey on ”Image Forgery Detection using Deep Learning” offers a thorough exploration of the ever-evolving domain of detecting manipulated images. It delves into various methodologies, challenges, advancements, and applications about the use of deep learning techniques for identifying forged images. Through its findings, the survey not only sheds light on the intricacies of image manipulation detection but also provides valuable insights into combating such manipulations[9]. By highlighting pathways to combat manipulation, the survey contributes to preserving the authenticity of visual content in the digital landscape. Moreover, it emphasizes the importance of ethical and responsible technology use, serving as a guiding beacon in navigating the complexities of the digital age. As the field continues to progress, this survey stands as a foundational resource, fostering innovation and deepening understanding in the ongoing quest for credible and trustworthy visual communication. Its insights will continue to shape research endeavors and inform practices aimed at maintaining integrity and reliability in visual media.

VII. FUTURE SCOPE

In the future, CNN models will advance to detect tampering more accurately, especially with real-time integration for immediate identification. Specialized architectures will emerge to counter new tampering techniques like deepfakes, ensuring reliability. Ethical considerations are vital in deploying these technologies responsibly. CNN-based detection systems will see wider adoption in journalism, law enforcement, and social media, promoting authenticity. Regulator frameworks will evolve to guide ethical use, ensuring transparency and accountability. Overall, these advancements will bolster efforts to combat misinformation and safeguard the integrity of visual media.

REFERENCES

[1] Dr.N P Nethravathi1, Bylla Danny Austin2, Dadireddy Sai Praneeth Reddy3, Grandhi Venkata Naga Satya Pavan Kumar4, Guduru Karthik Raju5 (2023)Image Forgery Detection Using Deep Neural Network © 2023, IRJET — Impact Factor value: 8.226 ISO 9001:2008 Certified Journal

[2] Z.J.Barad and M.M.Goswami, ”Image Forgery Detection using Deep Learning: A Survey, ”2020 6th International Conference on Advanced Computing Communication Systems(ICACCS), Coimbatore, India, 2020, pp. 571-576, doi:10.1109/ICACCS48705.2020.9074408.

[3] Image Forgery Detection Using Analysis of CFA Artifacts Yogesh Katre 1, Prof. Gajendra Singh Chandel, International Journal of Advanced Technology in Engineering and Science Volume No.02, Special Issue No. 01, September 2014.

[4] J. Ouyang, Y. Liu, and M. Liao, ”Copy-move forgery detection based on deep learning, ”2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics(CISP-BMEI),2017,pp.1-5, doi:10.1109/CISP-BMEI.2017.8301940.

[5] I. B. K. Sudiatmika et al, ”Image for- gery detection using error level analy- sis and deep learning, ”Telkomnika, vol. 17, (2),pp. 653-659, 2019. Available: https://www.proquest.com/scholarly- journals/image-forgery detection-using- error-level/docview/2213049537/se- 2? accountid=49663.

[6] B.Soni,P.K.Das, and D M.Thounaojam,“ Improved block-based technique using surf and fast key points matching for copy-move attack detection,” in 2018 5th International Conference on Signal Processing and Integrated Networks(SPIN).IEEE,2018, pp. 197–202.

[7] Karen Simonyan 1 and Andrew Zisserman 2, ”Very Deep Convolutional Networks for large-scale Image Recognition. ”Published as a conference paper at ICLR 2015

[8] A Study on Image Forgery Detection Techniques [Shijo Easowa*, Dr. L. C. Manikandanb], International Journal of Computer (IJC) (2019) Volume 33, No 1, pp 84-91

[9] Dr.V.Jayapradha 1, M.Reddy Kumar 2, K.Vamsi 3, N.V.Subba Reddy 4 (2022)Image Forgery Detection Using CNN, IJPR — www.ijrpr.com ISSN 2582-7421

[10] K. He, X. Zhang, S. Ren, J. Sun, Deep residual learning for image recognition, Proceedings of the IEEE conference on computer vision and pattern recognition (2016) 770–778

IJCRT