SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal

DETECTION OF FORGERY IMAGE USING CNN

Vemula Pavani Siva Prathyusha[1], Arepalli Rajesh[2]
[1]M.Tech Student, Sri Vasavi Engineering College, Tadepalligudem, West Godavari, Andhra Pradesh
[2]Sr.Assistant Professor, Sri Vasavi Engineering College, Tadepalligudem, West Godavari, Andhra Pradesh

ABSTRACT
The advancement of technology in every aspect of the current age are leading to misuse of data. Therefore, Researchers face the challenging task to identify these manipulated forms of data and distinguish the real data from the forged data. Splicing is one of the most common techniques used for digital image tampering; a selected area copied from the same or another image is pasted in an image. Image forgery detection is considered a reliable way to verify the authenticity of digital images. This method needs to be able to correctly solve several subtasks similar to segmentation, classification, localization. To reduce Human efforts, in this paper will Detect the Forgery part of the Image using Images and CNN, Deep Learning and Python. A variety of tools are frequently used to falsify images, resulting in the spread of misinformation. This increases the severity and frequency of image forgeries. In recent years, convolution neural networks (CNNs) have received much attention, and if has also influenced the field of image forgery detection. However, most image forgery techniques based on CNN that exist in the literature are limited to detecting a specific type of forgery either image splicing or copy-move.

KEYWORDS: *Image Detection, CNN Classification, Forgery Image, Digital Image, Falsify Images*

1. INTRODUCTION

Digital images have an important role in many fields such as in newspapers, digital forensics, scientific research, medicine, and so forth. Capturing images has been increasingly popular in recent years images are essential in our daily lives because they contain a wealth of information, and it is often required to enhance images to obtain additional information. Nowadays the usage and sharing of digital images on social media platforms is also widespread. Digital images are considered one of the main sources of information. Considering the excessive use of image sharing through various social media platforms such as WhatsApp, Instagram, Telegram, and Reddit, differentiating between real and forged images is a challenging task. The availability of many image editing software applications is making it more difficult to detect the authenticity of an image day by day. There are generally two approaches that image manipulation can be categorized into, as follows: 1. Active approach; 2. Passive approach. With the active approach, a watermark or digital signature is embedded when the image is created. While using these embeddings, whether the image has been tampered with or not is analyzed at later stages. Copy move and splicing are the commonly employed approaches for passive image forgery.

Copy Move: -Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature..



Splicing: - Splicing is one type of tampering that combines different regions of same or separate sources to create a composite fake image



(i) Authentic images (ii) Spliced image

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal

CONVOLUTIONAL NUERAL NETWORKS (CNN)

ConvNets are made to handle data that is presented as numerous arrays, such as a colour image made up of three 2D arrays that each includes the pixel intensities for the three different colour channels. 2D for spectrograms of images or audio. ConvNets, which take advantage of the properties of natural signals, are based on four core ideas: local connections, shared weights, pooling, and the use of numerous layers. A typical ConvNet's architecture is divided into various stages. Early stress detection is preferable in the IT industry. In order to gauge employee stress levels, we must first construct a web page to collect employee information. To identify this kind ofstress, upload an image of an employeewho appears angry, disgusted, fearful, happy, neutral, sad,or surprised.

2. LITERATURE SURVEY

Chen et al. presented an approach of median filtering forensic technique built on CNN for digital image forgery detection. The CNN network architecture used in their scheme consisted of eight layers by introducing a filter layer as the input layer. Through alternative convolution and pooling layers, numerous features were obtained to aid hierarchical learning process by the layers and then classify. This technique can be regarded as the first of its kind which used amalgamation of median filtering and CNN framework. The researchers were able to show significantly improved results for copy-move, cut-pasting forgeries and detecting median filtering from low resolution and Joint Photographic Experts Group (JPEG) compressed images as compared to other well-known image forensic tools that worked on hand-designed features..

Rao and Ni introduced a simplistic (ten-layered) CNN based deep learning approach which relied on automatic utilization of red-green-blue colour (RGB) images as input to train a hierarchical depiction. The technique proved equally efficient for copy-move and splicing forgeries. The novelty of the method was automatic learning of features for two forgery types, i.e., copy-move and splicing..

Yang et al. presented an improved method for digital image forensics. The technique was based on the idea of taking care of both categories of smooth filtering, i.e., linear and non- linear, and was specially focused to detect the forged images which had been post-treated with filtering performed to reduce the border discontinuity. The presented CNN framework consisted of six layers before the classifier for the output. The approach showed robustness against degradation of images by JPEG compression. However, it was vulnerable against the cut-paste forgery not post-processed with smooth filtering.

Soni et al. proposed a hybrid detection method by initial localization of key-points via SURF SURF-based features along with the utilization of maximally stable extremal regions around each matched key-point to find out the better localization of forged regions

Meena et al. sed Gaussian-Hermite Moments as feature extraction technique. Matching of similar blocks was done by lexicographical sorting. This technique enabled to detect the forgery in the presence of variouspost-processingattacks.

Chen et al. proposed a robust CMIFD algorithm that considered the fractional quaternion Zernike moments as a feature and a modified patch match algorithm as a feature matching algorithm.

Yerushalmy A new approach to detecting forgery in digital photographs is suggested. The method does not necessitate adding data to the image (such as a Digital Watermark) nor require other images for comparison or training. The fundamental assumption in the presented approach is the notion that image features arising from the image acquisition process itself or due to the physical structure and characteristics of digital cameras, are inherent proof of authenticity and they are sensitive to image manipulation as well as being difficult to forge synthetically. Typically, such features do not affect image content nor quality and are often invisible to the inexperienced eye. The approach presented in this work is based on the effects introduced in the acquired image by the optical and sensing systems of the camera. Specifically, it exploits image artifacts that are due to chromatic aberrations as indicators for evaluating image authenticity.

Fridrich, Soukal, Lukás, Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content, and detecting forgeries will only increase. Detection of malicious manipulation with digital images (digital forgeries) is the topic of this paper. In particular, we focus on detection of a special type of digital forgery – the copy-move attack in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. In this paper, we investigate the problem of detecting the copy-move forgery and describe an efficient and reliable detection method. The method may successfully detect the forged part even when the copied area is enhanced/retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG. The performance of the proposed method is demonstrated on several forged images.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal

3. EXISTING SYSTEM & ITS LIMITATIONS

The development of deep learning has led to improving methodologies where state- of-the-art methods, such as CNN, Mobile Net, and ResNet50v2, automatically extract the potential features, having been trained on large datasets. Some of the examples of CNN-based feature extractions are deep features utilized for image quality assessment [6], skin lesion classification or person re-identification. These extracted features are adapted into the inherent structural patterns of the data. This is the main reason behind their non-discriminative and robust architecture compared to the hand-engineered features. In this paper, motivated by the deep learning technique.

LIMITATIONS OF EXISTING SYSTEM

The main problem in existing system is, it takes more time to train the model.

1) It produce inaccurate results when pixel values are low.
2) In the practical training process, the model has small complexity.
3) Inconsistent Detection – Sometimes fore-ground object will influence the background object which leads to Inconsistent Detection.
4) Less Accuracy
5) Low Efficiency

4. PROPOSED MODEL & ITS ADVANTAGES

The major contribution of the projected method is the primary detection of the given image is illustrated or not. When the detection of image illustration is done, employing a convolution neural network(CNN), we examine the existence of splicing forgery or copy-move. When copy move is found, then additional processing is carried out for finding forged areas.

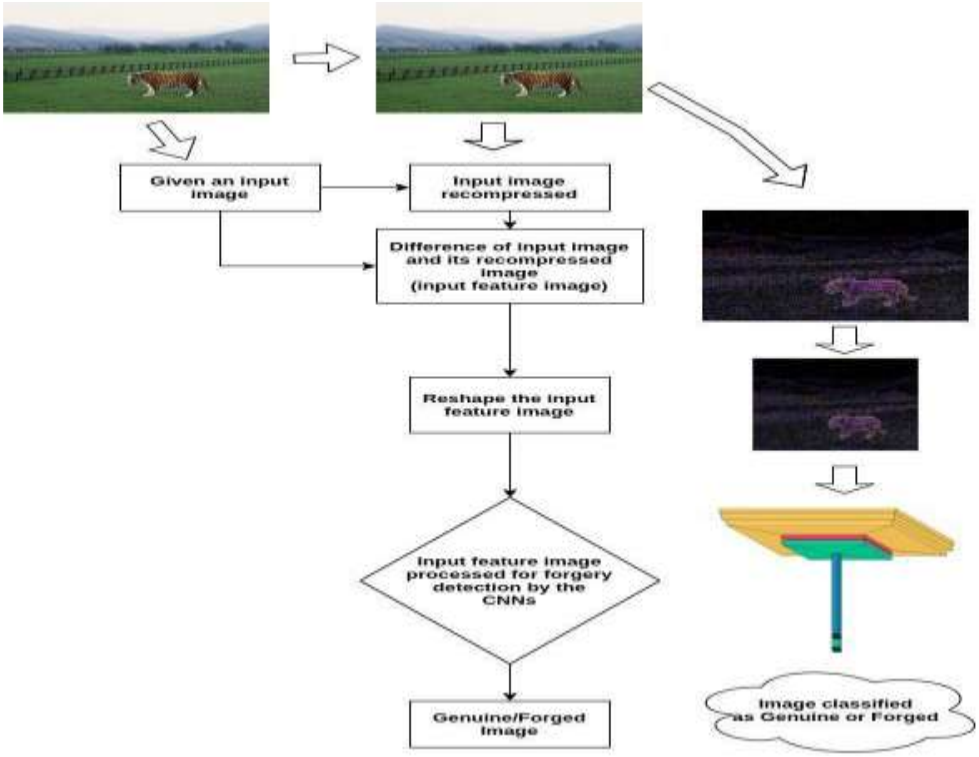
ADVANTAGES OF THE PROPOSED SYSTEM

1) We initialized our model with meaningful pre-trained weights.
2) It was developed in such a way that it removes the nonlinearity, hence clearing a path from the input to the output as a means of an identity connection.
3) High accuracy
4) High efficiency

5. SYSTEM ARCHITECTURE

PROPOSED ARCHITECTURE

WORK FLOW DIAGRAM



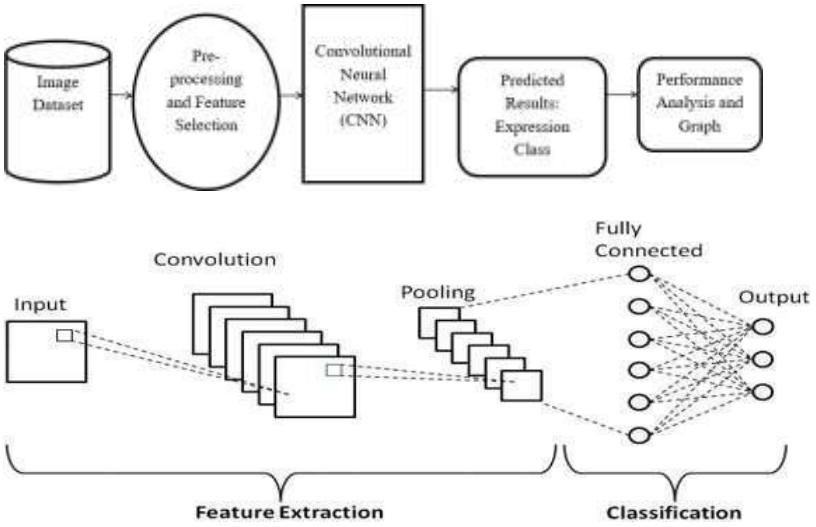
SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal

CNN ARCHITECTURE

A CNN architecture is composed of two basic components:

1. A convolution tool that extracts and isolates the various elements of the image foranalysis (a process known as feature extraction); &
2. There are numerous pairs of convolution or pooling layers in the feature extractionnetwork.

Convolutional Layers



Three main types of layers make up the CNN: fully-connected (FC), pooling, and convolutional layers. When these layers are combined, a CNN architecture is produced. In addition to these three layers, two other essential elements are defined below: the dropout layer and the activationfunction.

We will utilize the sequential model from the Keras library to build the model. The layers will be added after that to create the convolutional neural network. 32 filters and a kernel size of 5.5 wereemployed in the first 2 Conv2D layers. When the pool size of the MaxPool2D layer is set to (2,2),it will pick the highest value from each 2 × 2 pixel area of the image. The image's dimensions willdecrease as a result by a factor of 2. The dropout rate in the dropout layer was maintained at 0.25, meaning that randomly selected neurons account for 25% of the population. We reapply these three layers with a few tweaks to the parameters. Next, we apply a flatten layer to turn 2-D data into a vector in 1-D space. Following this layer are a dense layer, a dropout layer, and another dense layer.Seven nodes are produced as the Forgery image Detection by the last thick layer. This layer uses the soft max activation function to estimate which of the seven possibilities has the highest probability by providinga probability value.

Apply the model and plot the graphs for accuracy and loss

The fit function will be utilized to apply the model after it has been constructed. It will produced. The accuracy and loss graphs will then be drawn. Our training has an accuracy rate of 87.34%.

Accuracy on Test Set

We got an accuracy of 98.45%. on test set.

Saving and Reusing the Trained Model

The primary step is to store both trained and test models after extracting the best features required. The file formats are .h5 and .pkl and are easily reused when requiresd to integrate in themachine learning projects. The production ready files are stored in different file formats and verifying the files which are useful to setup the environment. The trained models are imported and modules are dumped and extracted from .pkl (pickle) files.

6. IMPLEMENTATION STAGE

In this stage we try to use Python as programming language to test the performance of our application. The application is divided into number of modules and then coded for deployment.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal

Implementation Steps

Implementation Steps are given below:

1) **Dataset collection**: Collect a dataset of authentic and manipulated images. Ensure that the manipulated images are varied and represent different types of manipulations, such as copy-move, splicing, and retouching
2) **Data pre-processing**: Pre-process the images to make them ready for the CNN. Resize the images to a standard size, convert them to grayscale, and normalize the pixel values.
3) **Data splitting**: Split the dataset into training and testing sets. The training set is used to train the CNN, and the testing set is used to evaluate the performance of the trained CNN.
4) **CNN architecture selection**: Choose an appropriate CNN architecture, such as VGG- 16 or ResNet , for the image forgery detection task.
5) **CNN model building**: Build the CNN model in Python using the chosen architecture. Train the CNN using the training set and validate it using the testing set.
6) **Model deployment**: Deploy the trained CNN model to detect image forgery in new images.
7) **Taking the input**: Input image is given through the user Interface.
8) **Displaying the output**: Output image displayed in a way whether it is forged or not.

7. RESULT AND CONCLUSION

RESULT

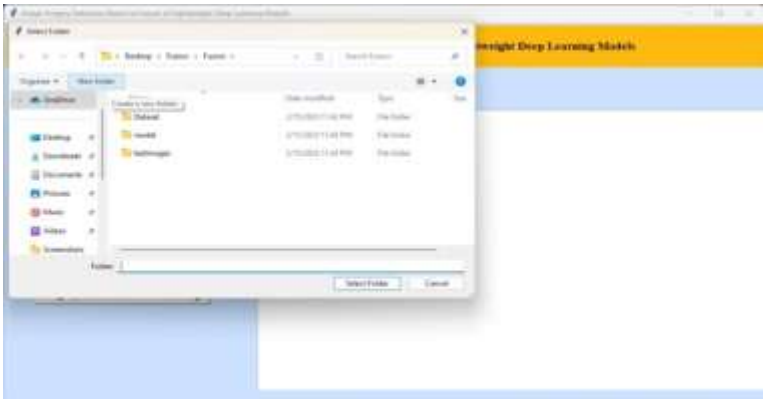
HOME PAGE

The interface of the web page will be as shown below.



Explanation

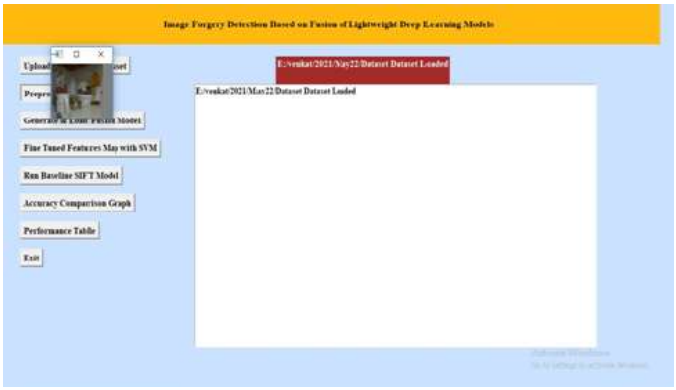
In above screen click on 'Upload MICC-F220 Dataset' button to upload data set and get below output



Explanation

In above screen dataset loaded and now click on 'Preprocess Dataset' button to read all images and normalize them and get below output

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal



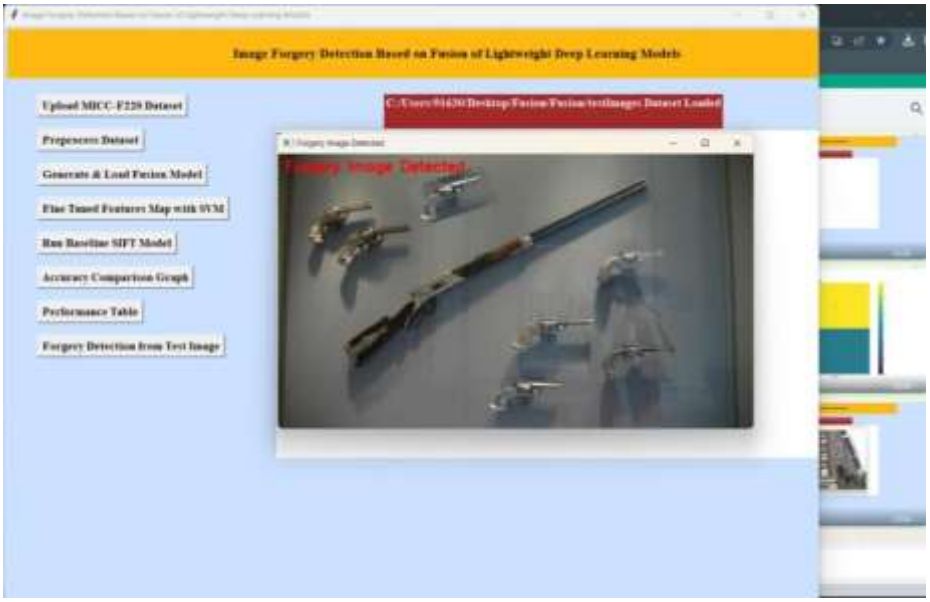
Explanation

After uploading the input image and I fit is original image then output is displayed as followed.



Explanation

After uploading the input image and if it is forge damage then output is displayed as followed.



SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 4 | April 2025 - Peer Reviewed Journal

CONCLUSION

Image forgery detection is a very challenging problem. In this era of technological advancement, we need to be able to distinguish between real and tampered images. In this study, we proposed a deep learning-based approach for image forgery detection. The proposed model is based on ResNet50v2 architecture, which uses residual layers; thus, using this architecture increases the detection rate of tampered images. The use of transfer learning enabled us to train our model more efficiently, as we initialized our proposed model by meaningful assigning weights. This reduced the training time and complexity of the model and makes the architecture more efficient. The results of the comparison with the existing methods show the superiority of the proposed system. The proposed system will help in the image manipulation detection domain and also paves the way for future research in detecting multiple types of image forgery manipulations**.**

FUTURE SCOPE

One of our future works is to expand our training dataset to enhance the generalization ability of our model. As of now, we have concentrated on Image forgery detection only. In future, we will try to detect the forged part and will highlight that particular part in the Output image.

REFERENCES

1. *Zhang Y, Goh J, Win LL, Thing VL. Image region forgery detection: a deep learning approach. SG-CRC 2016; 2016: 1-11.*
2. *Goh J, Thing VL. A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection. International Journal of Electronic Security and Digital Forensics 2015; 7 (1): 76-104.*
3. *He Z, Lu W, Sun W, Huang J. Digital image splicing detection based on Markov features in DCT and DWT domain. Recognition 2012; 45 (12): 4292-4299*
4. *Chang IC, Yu JC, Chang CC. A forgery detection algorithm for exemplar-based in painting images using multi-region relation. Image and Vision Computing 2013; 31*
5. *(1):57-71.*
6. *Bianchi T, Piva A. Image forgery localization via block-grained analysis of JPEG artifacts. IEEE Transactions on Information Forensics and Security 2012; 7 (3): 1003-*
7. *1017.*
8. *Wang W, Dong J, Tan T. Exploring DCT coefficient quantization effects for local tampering detection. IEEE Transactions on Information Forensics and Security 2014;9 (10): 1653-1666.*
9. *Khan A, Sohail A, ZahooraU, Qureshi AS. A survey of the recent architectures of deep convolutional neural networks. arXiv 2019; preprint arXiv:1901.06032*
10. *Hadji I,Wildes RP. What do we understand about convolutional networks? arXiv2018; preprint arXiv: 1803.08834.*
11. *Rao Y, Ni J, Zhao H. Deep learning local descriptor for image splicing detection and localization. IEEE Access 2020; 8: 25611-25625.*
12. *Popescu AC, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing 2005; 53 (10): 3948-3959. doi: 10.1109/TSP.2005.855406*