e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

INTELLIGENT MEDICAL IMAGE FALSIFICATION DETECTION

Yashvanth SK[*1]

[*1]Student, Department Of MCA, PESITM, Shimoga, Karnataka, India.

ABSTRACT

The paper addresses “In order to evaluate the efficacy of the proposed technique, CHEST X-RAY data is modified with various types of forgeries, and subsequently, the CNN model is utilized to identify any data tampering. By applying the CNN model to CHEST X-RAY information that has been altered with diverse forgeries, the efficacy of the suggested CNN model in detecting data tampering is evaluated. Through experimentation on CHEST X-RAY information that has been altered different forgeries, the proposed CNN model is put to the test for detecting any data manipulation. The assessment of the suggested approach involves testing it on CHEST X-RAY information that has undergone various forgeries, then employing the CNN model to identify any tampering. The assessment of data manipulated with different forgeries is executed utilizing the suggested technique, followed by the application of a CNN model to detect any data tampering. This examination involves the manipulation of CHEST X-RAY data with different forgeries, followed by the introduction of a CNN model to identify any data tampering. By examining CHEST X-RAY data altered with various forgeries, The suggested approach is evaluated, and the CNN model is deployed to detect any potential data manipulation. The testing of the suggested algorithm is conducted on CHEST X-RAY information that has been altered with diverse forgeries, followed by employing a CNN model to determine any data manipulation."

Keywords: Chest X-Rays, Data Tampering, Forgery Detection, Medical Imaging, Image Manipulation, Health Data Integrity.

I. INTRODUCTION

Altering the origin of an element, data, or entity is known as forging or manipulating. The appearance of increasingly complex methods of counterfeiting due to Processing data digitally has led to to a loss of trust in digital images, posing a growing threat to the accuracy authenticity of photographs. Efforts have been focused on developing new strategies combat various forms of data forgery in recent years. Digital data has become a significant source of information on the internet, making it easy to manipulate because of the rapid expansion of digital software. The emergence of new image editing tools allows for the creation of forged data by adding or removing elements to deceive viewers. Consequently, verifying the authenticity of digital content, especially photographs, has become crucial. Picture forensics has evolved as a vital discipline for evaluating the the caliber and dependability of digital images.

The suggested approach We plan to Apply deep learning technologies, like CNN and VGG16, in the suggested system to construct the model. We will be gathering the COVID-19 healthcare picture datasets from kaggle.com for this project. Methods of deep learning are applied. to preprocess and train the gathered datasets. The online application that we have created allows the user to upload an image and has the ability to categorize the outcome.

Developing a computer-aided detection (CAD) tool for iterative forgery image detection, including a detailed description of its formation procedures. This covers feature selection and extraction.and classification of normal images to assist in the early and more exact detection of tampered images. This Design Document pertains to a foundational system aimed at demonstrating the feasibility of developing a system that offers fundamental functionality for large-scale production. The document highlights the significance of creating and editing documents. The system will linked with existing systems and will mainly include a document interaction that simplifies document interactions and manages document objects. This document specifies the design requirements for "Image Forgery Detection..

II. LITERATURE SURVEY

The study [1] aims to summarises existing efforts on picture and document forgery detection, including their methodology, results, and comments. It serves as a survey to kick off work on detecting forgeries in Arabic administrative documents by analysing and putting together a training picture dataset.

The paper [2] highlights that In the context of dual image compression, a proficient deep learning technique is introduced to identify fraudulent alterations in photographs. The model is optimized to distinguish between the authentic image and its recompressed variants. The suggested method is effective in identifying image forgeries that involve copy-move and image splicing. The overall validation accuracy of the experiment is 92.23%, which is quite encouraging. The suggested model determines the existence of image fraud through examining the many artifacts that are abandoned after photo fraud. The proficient model has a great degree of precision rate in detecting tampering.

The paper[3] This has prompted scientists to develop a number of methods for more precise identification altered photos. Conventional approaches to image forgery detection mostly rely on the extraction of basic features tailored to identifying a certain kind of fake. Recent research on Neural network-based forgery detection has proven to be quite successful in detecting false photos. Complex information can be extracted by neural networks. hidden information from photos, thus they provide higher accuracy.The majority of deep learning techniques employ fundamental CNN architecture, which is covered in this paper. Additionally, a comparison analysis of different deep learning techniques is covered, along with information on their benefits and drawbacks

The paper [4] This suggests that the Structure might not always work. consistently across various changing an entirely false picture. Due to the proximity of several incredibly dynamic programming initiatives, it becomes challenging to distinguish between authentic and fraudulent content.This will attract the necessary understudy to adjust additional attributes of altered zones and guarantee improved accuracy for balanced region control across various image file formats.

Objectives:

The project's goal is to introduce A new decision-making tool for the identification of image forgery. This research focuses on evaluating The efficiency of convolutional neural networks and VGG 16 In terms of precision and accuracy, and speed in predicting image forgery. Compared to Densent and VGG 16, the CNN classifier demonstrates superior performance.To classify the type of covid 19 and covid 19 using a image.

1. To determine thermal image processing feasible to detect tampered image using ela.
2. Applying the deep learning algorithms to forecast the better result
3. Comparision study

III. METHODOLOGY

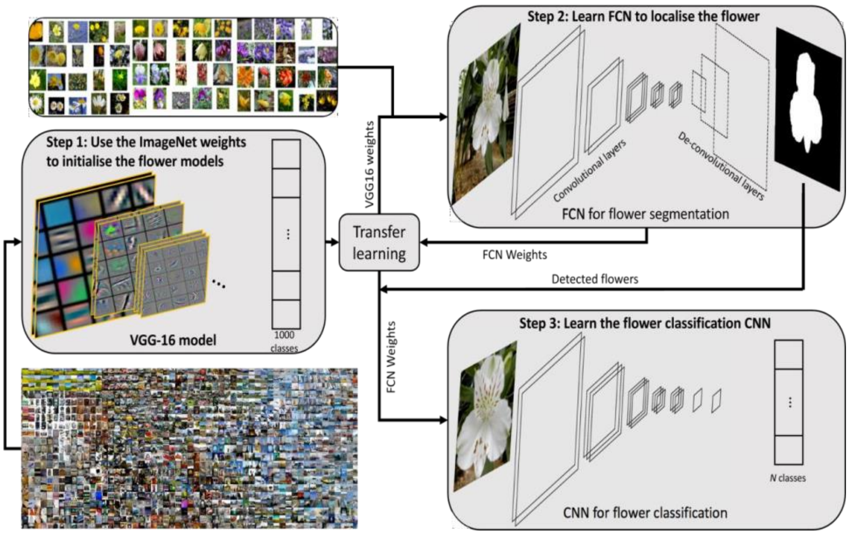

Step 2: Learn FCN to localise the flower
Convolutional layers
De-convolutional layers
FCN for flower segmentation
Step 1: Use the ImageNet weights to initialise the flower models
VGG-16 model
1000 classes
VGG16 weights
Transfer learning
FCN Weights
Detected flowers
FCN Weights
Step 3: Learn the flower classification CNN
N classes
CNN for flower classification

Fig 1: System Architecture

The process begins with leveraging a pre-trained VGG-16 model, which has been trained on the ImageNet dataset comprising 1000 classes. The pre-trained weights from this model are used to initialize the flower classification models. This step utilizes the concept of transfer learning, where knowledge gained from a large and diverse dataset (ImageNet) is transferred to a more specific task (flower classification). After initialization with ImageNet weights, a Fully Convolutional Network (FCN) is trained to perform flower segmentation. This involves identifying and localizing the flower within an image. The FCN consists of convolutional and deconvolutional layers that process the input image to produce a segmented output, where the flower is highlighted. This step is crucial for isolating the flower from the background, which aids in accurate classification. The final step involves training a Convolutional Neural Network (CNN) specifically for flower classification. Using the segmented flowers from the previous step, this CNN is trained to distinguish between different flower classes. The model architecture includes several convolutional layers, which progressively extract features from the images, followed by fully connected layers that perform the final classification into N flower classes. This figure demonstrates a comprehensive workflow for flower classification using transfer learning. By first initializing with ImageNet weights, then performing segmentation to isolate flowers, and finally training a specific CNN for classification, the method aims to enhance accuracy and efficiency in recognizing different types of flowers. This approach highlights the effectiveness of transfer learning and the sequential training of segmentation and classification networks in tackling specific image recognition tasks.

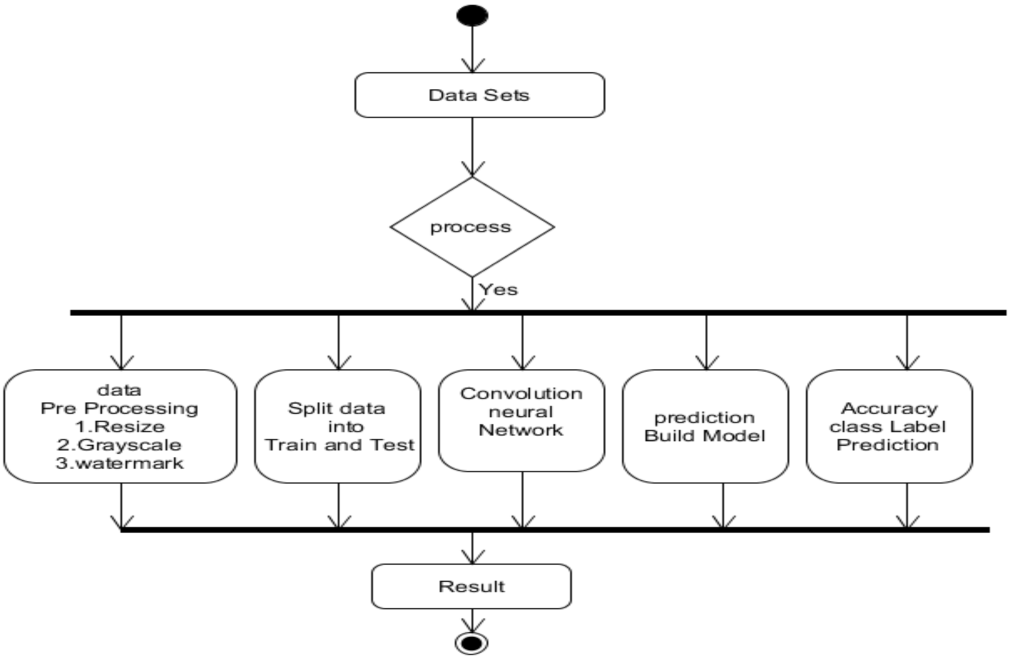


Fig 2: Block Diagram

This block diagram outlines a smart healthcare image forgery detection system. Starting with noise reduction using Weiner and regression filters, the process enhances the image quality before normalization. A CNN then extracts critical features, which are further processed by a Residual Network to ensure accurate detection of any image forgeries. This comprehensive workflow ensures that medical images are verified for authenticity, enhancing the reliability of healthcare diagnostics.

The process starts with acquiring an image, typically a medical image such as a chest X-ray, which is subject to verification for authenticity. The input image undergoes initial noise reduction using a Weiner filter. This step aims to minimize noise and enhance the image quality, making it easier to detect any tampering. The result is an estimated noisy image where some noise remains, but the image is significantly improved for further processing. The estimated noisy image is then processed through a regression filter, which further refines the image by reducing noise and enhancing important features, ensuring any subtle forgeries can be detected. The regression-filtered image is normalized, adjusting the pixel values to a standard scale. This step ensures consistency and improves the performance of subsequent neural network models. The normalized image is passed through a Convolutional Neural Network (CNN). The CNN is tasked with extracting features from the image, learning patterns, and identifying any anomalies that might indicate forgeryThe output from the CNN is then processed by a Residual Network (ResNet). ResNets enhance the learning capability by allowing gradients to flow more effectively through the network, which helps in detecting subtle forgeries by using skip connections to retain information from earlier layers. Finally, the processed data from the Residual Network is used to make a decision. This decision involves determining whether the image has been tampered with or is authentic, based on the features and patterns learned by the neural networks.

Error level analysis:

Error level analysis, a method used to detect manipulated images, involves saving them at a specific quality level and then comparing this with the compression level . Initially, when a JPEG file is saved, it undergoes compression for the first time. Most popular photo editing software like Adobe, Gimp, and Lightroom support JPEG compression. If an image is edited using these tools, it will undergo compression once again. The original picture taken with a digital camera has been compressed twice - first by the camera itself and then by editing software. While the image may look the same to the naked eye, this approach can reveal the discrepancies between the fake image and the authentic one. Swap the manipulated image with the original one. Calculate"Dark and black hues. Shifting this picture file again will degrade its quality. Editing the initial image will trigger ELA detection. The average difference between Y (brightness) and CrCb (color difference) quantization tables. The digital camera does not automatically adjust the image based on a specific quality level (high, medium or low).

IV. ALGORITHMS USED

Convlutional neural network(CNN):

A Convolutional Neural Network (CNN) is an advanced method in deep learning that proves highly efficient for detecting and processing images. It comprises multiple layers, such as convolutional pooling, and fully connected layers. The fundamental element of a CNN is the convolutional layer, which employs filters on the input image to identify characteristics like edges, textures, and shapes. Following this, the results from the convolutional layers move to pooling layers, which reduce the spatial dimensions of the feature maps while retaining crucial information. Subsequently, the output from the pooling layers is directed through one or more fully connected layers, dedicated to the task of prediction or classification of the image. LeCun and colleagues introduced the convolutional neural network (CNN) for recognizing handwritten text, which has proven highly effective in tasks like image recognition, detection, and segmentation. CNN demonstrates great proficiency in classifying large-scale images through its three key layers: the convolutional layer, pooling layers, and fully connected layers. Among these layers, the most crucial are the convolutional and pooling layers. The convolutional layer captures features through the combination of image regions with multiple filters, while the pooling layer reduces the output map size, preventing overfitting. In comparison to BP networks, CNN models contain substantially fewer neurons, parameters, and connections, making CNN more efficient at similar levels of performance.

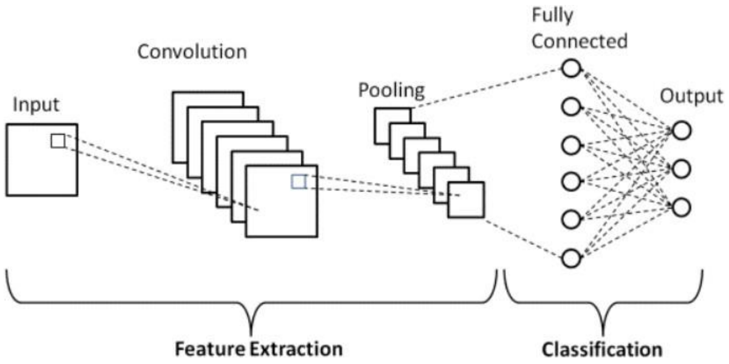


Fig 3: CNN Architecture

VGG 16 Algorithm:

VGG16, a convolutional neural network (CNN) architecture, emerged victorious in the 2014 ILSVR (Imagenet) competition, solidifying its status as one of the most powerful vision model designs to date. What sets VGG16 apart is its emphasis on utilizing convolution layers with a 3x3 filter, a stride of 1, and consistently employing the same padding, along with maxpool layers using a 2x2 filter and a stride of 2. This structural consistency carries through the entire architecture, culminating in two fully connected layers (FCs) and a softmax function at the output stage. In the realm of forensic imagery, the analysis of metadata plays a crucial role in validating the authenticity of image data."

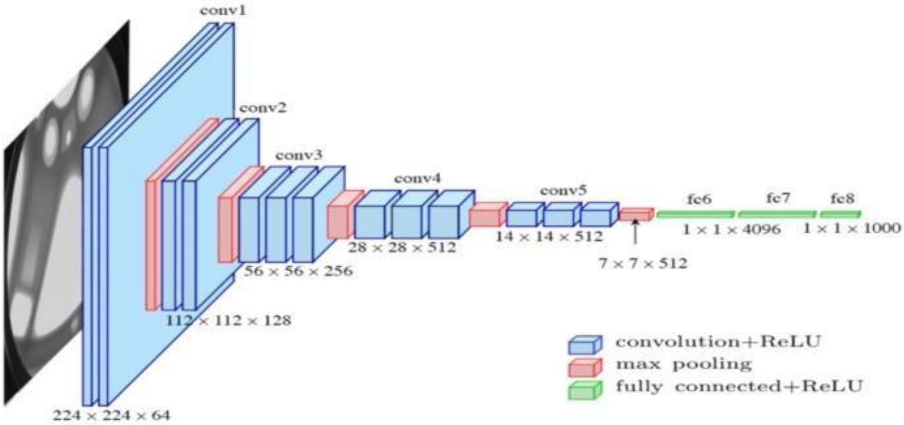


Fig 4: VGG 16 Architecture

V. RESULTS AND DISCUSSION

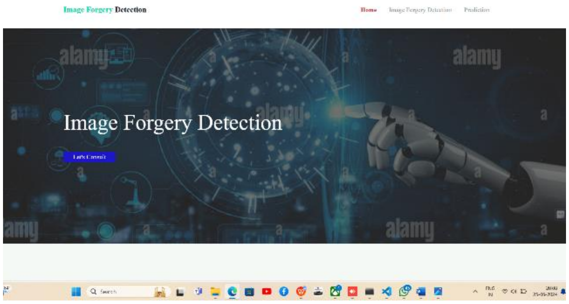
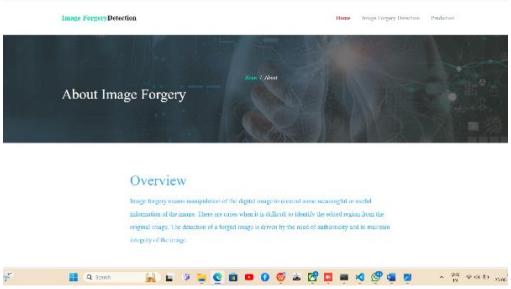


Image Forgery Detection

Module 1: Home page

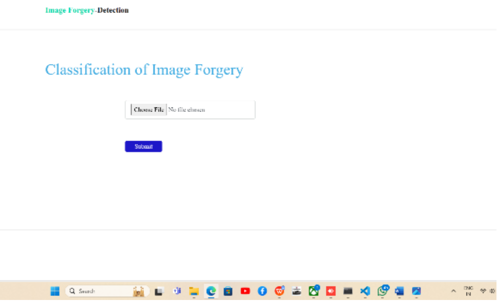


About Image Forgery

Overview

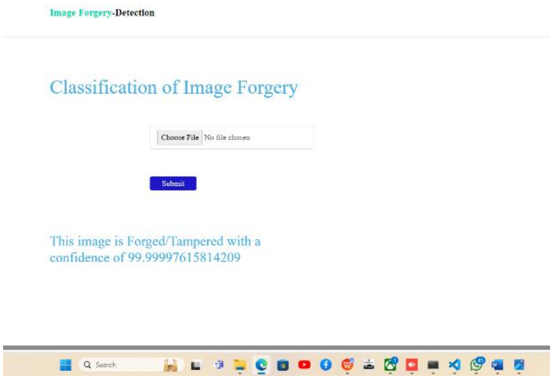
Image forgery means manipulation of the digital image to conceal some meaningful or useful information of the image. There are cases when it is difficult to identify the edited region from the original image. The detection of a forged image is driven by the need of authenticity and to maintain integrity of the image.

Module 2: About page



Classification of Image Forgery

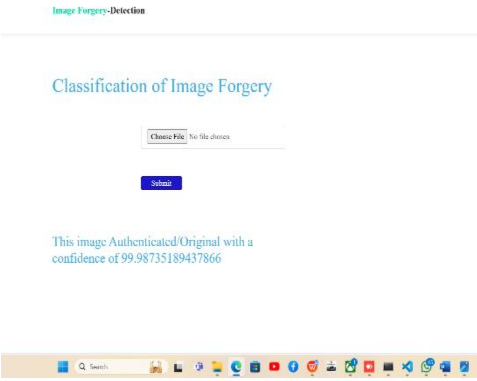
Module 3: Prediction page



Classification of Image Forgery

This image is Forged/Tampered with a confidence of 99.99997615814209

Module 4: Forged/Tampered Image



Classification of Image Forgery

This image Authenticated/Original with a confidence of 99.98735189437866

Module 5: Normal Image Page

VI. CONCLUSION

In this study, we addressed the issue of distinguishing authentic images from counterfeits through the utilization of deep learning techniques. We have introduced a fresh approach utilizing Error Level Analysis and Convolutional Neural Networks within the realms of machine learning and computer vision to effectively the aforementioned challenges. Prior to determining the framework for training the recognition system, we segregated the dataset into categories of unaltered and modified photographs. Opting for VGG 16 due to its superior performance in training with limited datasets, we employed this model for our training process. Upon completing 100 epochs, our experiment yielded the highest levels of training accuracy at 92.2% and validation accuracy at 88.46%. To further enhance accuracy and data quality, a variant of CNN architecture will be explored in our upcoming research.

VII. FUTURE ENHANCEMENT

The future enhancement of this project is Implementation of Generative Adversarial Networks (GANs) Use GANs to create sophisticated forgery detection systems. GANs can be used both to detect and generate forgeries, thereby improving the system's ability to recognize subtle alterations. Integration of Transformer Models: Leverage transformer models for better image processing capabilities. Models like Vision Transformers (ViTs) can be adapted for forgery detection, providing improved accuracy and efficiency

VIII. REFERENCES

[1] Marco Zanardelli1 · Fabrizio Guerrini1 "Image forgery detection: a survey of recent deep-learning approaches", 2017 IEEE International Conference on Power, Department of Information Engineering, CNIT - University of Brescia, Via Branze 38, 25134 Brescia, Ital, 2022.

[2] Syed Sadaf Ali Recompressing images and using deep learning to detect image forgeries. Information 10(09): Werghi, N.; Ali, S.D.; Saxena, N.; Ganapathi, I.I.; Vu, N.-S.

[3] Ritu Agarwal. Inf. Sci. 2020, 511, 172–191. Image Forgery Detection and Deep Learning Techniques: A Review. IEEE Xplore Part Number: CFP20K74-ART; ISBN: 978-1-7281-4876-\

[4] Using Machine Learning to Detect Malathi Image Forgeries. ISSN: 2278-3075; Volume 8 of the International Journal of Innovative Technology and Exploring Engineering (IJITEE)

[5] "Exposing Digital Image Forgeries by Illumination Colour Classification", Journal of Physics: Conference Series 1368 (2019) 032028 IOP Publishing doi:10.1088/1742-6596/1368/3/032028, "Digital image forgery detection using deep learning approach."

[6] Varsha Sharma, Swati Jha Science Int. 214 33-43 International Research Journal of Engineering and Technology (IRJET) Image Forgery and Its Detection Methodology: A Review

[7] Using super-BPD segmentation and DCNN, image copy-move forgery detection and localization Volume 3971, 2000, pages 152–163, Proc. SPIE, Security and Watermarking of Multimedia Content II

[8] L. Li, S. Li, H. Zhu, and X. Wu, Detecting copy-move forgery under affine transforms for image forensics, Computers and Electrical Engineering, 40(6) (2014) 1951–1962.

[9] C.-M. Pun and K.-C. Choi, Generalized integer transform based reversible watermarking algorithm using efficient location map encoding and adaptive thresholding, Computing, 96(10) (2014) 951-973.

[10] X.-C. Yuan and C.-M. Pun , A Geometric Invariant Digital Image Watermarking Based on Robust Feature Detector and Local Zernike Moments, Proceedings of the 9th International Conference Computer Graphics, Imaging and Visualization, Hsinchu, (2012).