Medical Image Tamper Detection Using MobileNet

Akhila Nomula
Department of Computer Science
University of Central Missouri
Lee's Summit, MO
axn93840@ucmo.edu

Bhargavi Dandu
Department of Computer Science
University of Central Missouri
Lee's Summit, MO
bxd11850@ucmo.edu

Yallanki Harsha sai
Department of Computer Science
University of Central Missouri
Lee's Summit, MO
hxy96670@ucmo.edU

***Abstract*—This thesis presents a comprehensive study on the detection of tampered medical images using deep learning techniques. With the advent of deep learning, attackers can create highly realistic medical imagery for malicious purposes. This research focuses on the identification of tampered 3D CT scans of human lungs, where cancer has been manipulated. The dataset consists of both real and manipulated images, making the task of distinguishing between them highly challenging. The proposed approach utilizes various deep learning algorithms for accurate classification, while also analyzing the performance of these algorithms.**

I. Introduction

A. *Background and Motivation*

Medical imaging plays a vital role in modern healthcare, aiding in accurate diagnoses, treatment planning, and monitoring of various medical conditions. Ensuring patient safety and making appropriate medical decisions depend heavily on the accuracy and integrity of medical imaging. But the quick development of deep learning methods has introduced additional difficulties in the form of doctored medical images, or "deepfakes." Medical practitioners may find it challenging to discern between real and fake pictures due to the convincing appearance of these altered photos. The accuracy of medical diagnosis and treatment results is seriously threatened by this.

The widespread use of deep learning models, especially generative adversarial networks (GANs), has given attackers the ability to modify medical images with a level of realism never seen before. The medical community is concerned about this and has called for the creation of reliable and precise techniques to recognize manipulated photographs. Medical picture tamper detection is becoming more and more popular because of the necessity to combat the possible misuse of deep learning for malevolent ends.

B. Problem Statement

This study aims to address the problem of identifying false positives and false negatives in medical CT scans. The ability to manipulate 3D CT scans of human lungs to change whether or not cancer is present requires the development of sophisticated methods to identify these changes. The detection of modified regions becomes more challenging with the advent of tampering techniques that produce convincing deepfakes. The main challenge is to create a system that can precisely identify these altered regions inside the intricate and complex structure of CT scans.

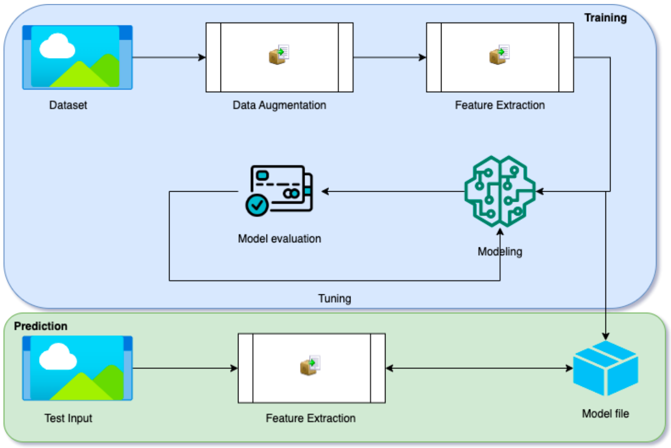
C. *Research Objectives*

Developing a deep learning-based method for the identification of altered medical photographs is the main objective of this research. The three specific goals are as follows: to develop and apply a deep learning framework that is all-inclusive and competent to identify medical CT images with altered cancer areas.to assess several classification algorithms' performance regarding the identification of medical image tampering. Our goal is to find the best method for precise classification by contrasting different algorithms.to evaluate and quantify the created models' F1-score, accuracy, precision, and recall. These metrics will give us information about the advantages and disadvantages of the suggested approach and aid in our comprehension of its general efficacy in tamper detection scenarios.

D. *System Flow*

The project's main goal is to employ deep learning methods to identify areas in medical photographs that have been altered. The project's main components and steps are described in the sections that follow.

GitHub Link: - https://github.com/aknomula/DL-NN-Project.git



Dataset Loading and Augmentation:

The loading of the Medical Deepfakes: Lung Cancer dataset marks the start of the project. DICOM files with CT scans make up this dataset. Data augmentation strategies are used to improve the robustness and diversity of the dataset. By producing changes to the original images, such as rotations, flips, and shifts, augmentation broadens the dataset and enhances the generalization capabilities of the model.

Feature Extraction:

Subsequently, the Watershed method is employed to separate the images and pinpoint areas of interest. It is essential to use this method to get unique patterns and characteristics that help separate real from manipulated areas in the photos. The inputs for the ensuing model training and assessment are the split regions.

Model Building:

The project proceeds to the modeling phase after the preprocessed dataset and extracted features are obtained. Deep learning models are created, such as EfficientNet50 and VGG19. To determine whether a segment has been altered or is authentic, every model gains knowledge from the attributes of the segmented regions.

Model Evaluation and Performance Metrics:

A variety of indicators are used to evaluate each algorithm's performance after model training. Metrics such as accuracy, precision, recall, F1-score, and other pertinent variables are computed to assess how well the models are able to identify tampered regions in medical pictures. These measures offer a thorough grasp of the algorithms' advantages and disadvantages.

Visualization and Analysis:

For more insightful analysis, the performance indicators and results are represented. Plots of ROC curves show how different models trade off true positive and false positive rates. Confusion matrix plots provide a visual depiction of the models' predictions, which facilitates understanding of their performance attributes. Stakeholders can compare and evaluate the efficacy of the algorithms with the help of these representations.

II. RELATED WORK

A. *Medical Image Tamper Detection*

Assuring the accuracy and dependability of medical diagnosis and treatments depends heavily on the detection of manipulated medical images. Scholars have put up a number of strategies to address this problem over the years. Watermarking and digital signatures were frequently used in the early techniques to embed data for authentication into photographs. These approaches worked well against simple modifications, but they were unable to handle the more complex tampering strategies made possible by deep learning.

Machine learning and computer vision techniques have been used in recent studies to identify manipulated medical photos. These techniques frequently center on finding disparities in the content of images, modification artifacts, and changes to picture statistics. Image forensics and other pixel-wise analysis techniques have demonstrated potential in identifying irregularities in altered areas. But their capacity to distinguish between modified and real stuff is what will determine how successful they are.

Although these techniques have advanced, they still have limits when applied to deepfake imagery. It is now difficult to detect manipulated information based only on pixel-level analysis since generative adversarial networks (GANs) are used to produce extremely convincing deepfakes. Moreover, these methods could not translate well across various medical imaging modalities and might be vulnerable to counterattacks by adversaries trying to hide their activities.

B. *Deep Learning in Medical Imaging*

Medical imaging analysis has undergone a radical change because to deep learning, which has produced innovations in areas including picture segmentation, classification, and illness detection. The remarkable ability of convolutional neural networks (CNNs) to automatically extract pertinent characteristics from medical images has been shown. These networks can identify intricate structures and patterns, which improves accuracy in a range of medical image analysis applications.

Although deep learning has produced amazing breakthroughs, there is rising concern about its misuse potential. The legitimacy of medical images is called into question when compelling deepfakes are created using the same algorithms that enable medical image analysis. Our approach to deep learning-based medical picture tamper detection needs to change in light of the prevalence of deepfake medical images.

Using deep learning methods for tamper detection that have been applied to medical picture analysis is one strategy. We can use deep neural networks to discover complex patterns that are not always visible using conventional approaches by teaching them to discriminate between real and artificial images. But the efficiency of these models depends on the availability of labeled data that distinguishes between real and manipulated images.

Adversarial assaults are also a possibility when deep learning is abused for manipulating purposes. By taking advantage of flaws in their architectures, adversarial examples can be made to trick tamper detection methods. This underscores the necessity of employing resilient training methodologies and investigating approaches that can enhance the ability of deep learning-driven tamper detection models to withstand hostile assaults. There are potential and obstacles when it comes to the convergence of deep learning and medical picture tamper detection. The medical community needs to adjust to the growing sophistication of deepfakes by creating sophisticated detection techniques that can accurately differentiate altered from real medical images. Researchers can help create robust and efficient solutions for preserving the integrity of medical imaging in a time of rapid technological growth by utilizing deep learning techniques while being aware of their possible misuse.

III. Methodology

A. Datasets

High-quality and well-chosen datasets are the cornerstone of any successful deep learning effort. We present the Medical Deepfakes: Lung Cancer dataset, which was used in this study, in this chapter. Identifying tampered medical imaging is a challenge that this dataset effectively addresses because it includes both authentic and modified medical images.

One hundred three-dimensional CT scans of human lungs make up the Medical Deepfakes: Lung Cancer dataset. This set falls into two categories: 20 scans were utilized in an open trial where the radiologists were informed of the possible manipulation, and 80 scans were used in a blind trial with experienced radiologists who were unaware of the tampering. This dataset's main goal is to identify places where medical scans have been modified and to differentiate between real cancer regions and manipulated cancer regions.

An extensive CSV table that functions as the ground truth is included in the dataset. Information regarding the kind and presence of cancer in particular scan areas is provided by each entry in the table. Three-dimensional coordinates (x, y, z [slice#]) are used to represent these places, and they are categorized as True-Benign (TB), True-Malicious (TM), False-Benign (FB), and False-Malicious (FM). These classifications let us distinguish between real and artificial regions and spots where cancer has been excised or injected.

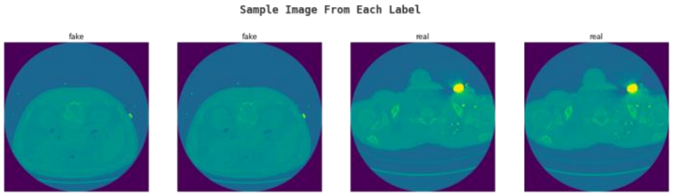


Fig 2. Dataset Sample

B. Data Preparation

To make sure the dataset is in an appropriate format for further analysis and model training, effective data preparation is essential. To begin, import the DICOM files. These files are specially formatted medical images that are frequently used in imaging. To obtain the pertinent picture data, these files must be processed. In order to obtain a preliminary grasp of the data, the images are displayed visually after the DICOM files have been loaded. Finding any possible artifacts, irregularities, or abnormalities that might result from the tampering process or other circumstances is made easier by displaying sample photos. Verifying the quality of the dataset and if fraud has really introduced actual alterations is another benefit of visualization.

Prior to developing the model, the photos must be ready for feature extraction. The photos are flattened to produce an appropriate format for further processing in order to do this. To enable feature extraction algorithms to process the image efficiently, flattening essentially converts the three-dimensional image data into a two-dimensional representation.

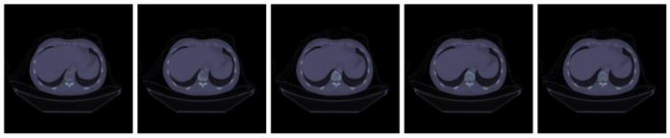


Fig 3: Cancerous and Binary CT Lung Image

With its wide variety of authentic and altered medical photos, the dataset serves as the foundation for our study. Data preparation for feature extraction and further analysis is achieved by preprocessing procedures such as loading DICOM files, image visualization, and picture flattening. With the help of this extensive dataset and meticulous preprocessing, deep learning models that can accurately identify manipulated medical photos have been successfully developed.

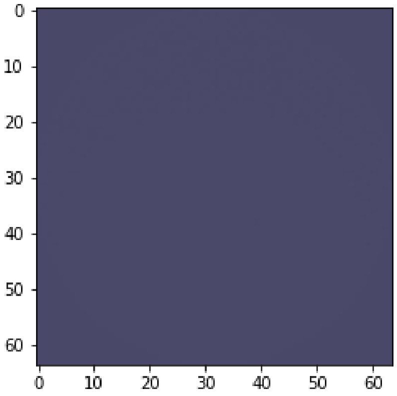


Fig4. Dataset Sample

C. Feature Extraction

A critical first step in converting unprocessed picture data into interpretable and useful representations for analysis and classification is feature extraction. Here, we explore the Watershed algorithm, an image segmentation method that could be useful in locating potentially tampered areas by recognizing discrete sections inside medical pictures.

One effective tool that is frequently used in computer vision and image processing is the Watershed algorithm. Fundamentally, it mimics the procedure of inundating a landscape and locating the watershed boundaries that divide several catchment regions. Pixel intensity levels are treated by the algorithm as heights in a grayscale landscape throughout the image segmentation process. The method determines areas where the flooding waters would meet by flooding the landscape from local minima; this effectively delineates objects or structures in the image.

The algorithm's primary steps involve the following:

Gradient Computation

In watershed segmentation, calculating an image's gradient magnitude is the first and most important step. The locations with considerable and fast variations in pixel intensities are revealed by this computational procedure. These sudden shifts in brightness frequently line up with the edges of objects or prominent features in the picture. The gradient magnitude highlights possible segments of interest by highlighting these areas of extreme change. The groundwork for further phases of the watershed algorithm is laid by this first stage, which is crucial.

Marker Selection

After calculating the gradient magnitude, selecting markers is an important next step. These markers act as key locations in the picture that determine when the flooding process begins. These markers usually correlate to local minima in the gradient image; that is, they indicate regions surrounded by pixels with higher intensities where the intensity changes relatively abruptly. These carefully chosen markers serve as the flooding process's jumping off points, basically directing the algorithm to concentrate on possible areas of interest. The idea here is to use these markers as starting points for the algorithm's visual exploration.

Flood-Filling

The watershed algorithm starts the flood-filling process after the markers are set. Starting at the markers, this simulated flooding operation gradually spreads throughout the scene. Every pixel in this picture is identified according to the catchment area to which it belongs. The marker that started the flooding process defines the catchment area. This stage is similar to virtual water pouring out of each marker, inundating the spaces around it, and assigning the appropriate labels to each pixel. The technique of flood-filling creates areas in the picture that are thought to be components of different objects or buildings.

Watershed Line Determination

Watershed line identification is one of the main accomplishments of the watershed algorithm. The borders between various items or structures within the image are shown by these lines. Where the floodwaters from various catchment areas converge, basin boundaries are formed. Put otherwise, they signify the intersections of two catchment regions, creating the equivalent of object boundaries in terms of visual representation. An important result of the algorithm is the watershed line determination, which gives an easy-to-understand visual representation of the boundaries of objects in the image. This stage brings the segmentation process to a close and provides important information on the spatial arrangement and connections of the objects in the image.

For example, look at a 2D medical image that has been altered to include several malignant spots. These discrete areas can be precisely segmented and labeled using the Watershed method. Because the generated segments can be viewed as distinct zones of interest, each with its own distinct properties, this segmentation is very useful for feature extraction.

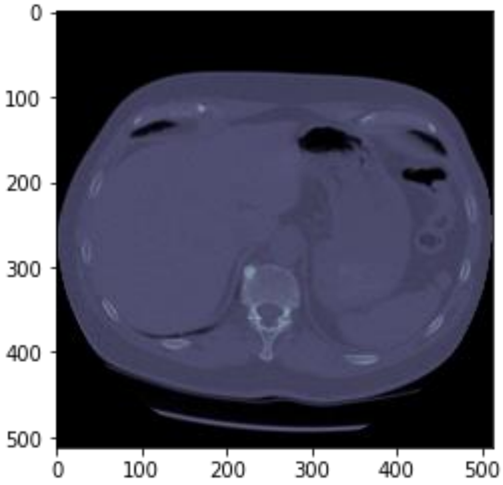


Fig 5: Probabilistic Neural Network workflow

One important application of the Watershed algorithm's ability to split images into discrete sections is medical image tamper detection. Segmented zones that differ from the expected patterns can be used to discover possible tampered areas. In contrast to real regions, artificially created malignant areas could display irregularities in their boundaries or intensity values. Image segmentation and meaningful region of interest identification can be accomplished with ease using the Watershed method. Our ability to extract features that can identify possibly tampered areas is made possible by its use in medical image tamper detection. We establish a basis for precise medical picture manipulation detection and classification by considering every segmented region as a unique characteristic. These retrieved features will be expanded upon in the upcoming chapters to create and assess deep learning models for tamper detection.

D. *Train-Test Split*

It is essential to divide the dataset into separate training and testing subsets in order to guarantee the efficacy and dependability of our deep learning models. This chapter's main goal is to go over the approach that was taken and the importance of this particular stage in creating reliable models for medical picture tamper detection.

The training set and the testing set are the two main subsets of the dataset, which consists of both authentic and altered medical images. Model learning is based on the training set, which enables algorithms to find patterns and connections in the data. In the meanwhile, the models' performance on unobserved data is assessed using the testing set, which is kept apart from the training procedure.

To guarantee a balanced distribution of genuine and altered images in both subsets, the train-test split is carefully carried out. This distribution is necessary to keep the model's capacity to generalize to real-world circumstances intact and to avoid a skewed depiction of the classes. The model gains improved ability to reliably discriminate between the two classes by training on a balanced mixture of real and altered images.

E. Feature Standardization

Normalization, another name for feature standardization, is an essential preprocessing step that improves the comparability and performance of different deep learning algorithms. Normalizing the characteristics in the dataset helps level the playing field because they may have varied sizes and distributions. This enables algorithms to converge more quickly and efficiently.

The process of normalization entails changing the features so that their means and standard deviations are both one. By bringing all features to the same scale, this technique stops any one feature from having an excessively large impact on the learning process. Normalized features are very useful for distance-based algorithms such as support vector machines and k-nearest neighbors.

The variety of values found in medical images makes feature standardization crucial in the context of medical image tamper detection. Images can have diverse ranges of pixel intensities, and individual pixels within a picture can have wildly changing intensity values. By normalizing these intensities, the scale of the data no longer influences the deep learning algorithms, which can now concentrate on the underlying patterns associated with tampering.

II. MobileNet

A series of thin deep neural network architectures called MobileNet was created with the purpose of effectively completing tasks related to object detection and picture classification, particularly on devices with limited resources such as mobile phones and edge devices. MobileNet techniques are appropriate for real-time applications with constrained computational resources because they balance computational efficiency and model correctness. To overcome the difficulty of implementing deep neural networks on mobile devices with constrained memory and processing power, Google researchers developed MobileNet in 2017. Even when they are accurate, traditional deep learning models are frequently too resource-intensive for devices with limited hardware. MobileNet achieves efficiency by utilizing two fundamental design principles:

Depth wise Separable Convolution:

MobileNet uses a depth wise separable convolution in place of conventional convolutions. The high computational cost of traditional convolutions is caused by their distinct spatial convolutions for each channel. This is divided into two steps by a depth wise separable convolution: a depth wise convolution and a pointwise convolution. Efficiency is boosted as a result of fewer computations and parameters.

Inverted Residuals with Linear Bottlenecks:

By using inverted residuals, MobileNet effectively captures non-linearity. In order to do this, the input must first undergo a lightweight depth wise separable convolution. Next, linear bottlenecks that first decrease and then increase the number of channels must be applied. Information loss during the depth wise separable convolution is lessened with the use of linear bottlenecks.

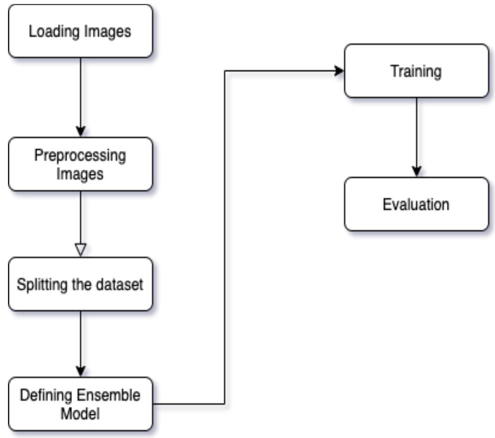


Fig 6: MobileNet workflow

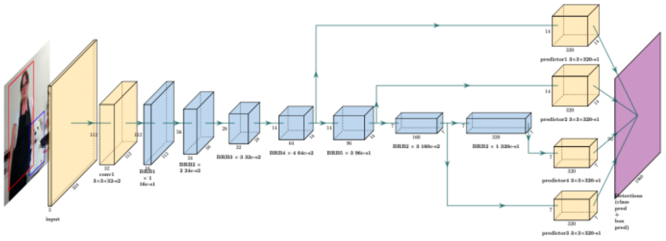


Fig 7: Network architecture of MobileNet model

Convolutional Blocks:

MobileNet begins by extracting low-level characteristics using a conventional convolutional layer. It is succeeded by a sequence of depth wise separable convolutional blocks, each of which has an activation of the rectified linear unit (ReLU), batch normalization, and a depth wise convolution. These building blocks represent increasingly sophisticated hierarchical aspects.

Inverted Residual Blocks:

Linear bottlenecks come after a depth-wise separable convolutional layer in the inverted residuals. In addition to facilitating effective information flow, this structure helps the model identify intricate patterns in the data.

Model Architecture:

Because of their adaptability, MobileNet designs can be tailored to achieve the required balance between accuracy and model size. Versions MobileNetV1, V2, and later have many setups. MobileNetV2, for example, uses skip connections and linear bottlenecks to bring improvements over MobileNetV1.

Applications:

Applications for MobileNet methods can be found in many domains, such as semantic segmentation, object detection, and image classification. Because of their efficiency, they can be used in embedded systems, mobile applications, and Internet of Things devices with constrained computational resources.

MobileNet models can be optimized through transfer learning on a particular dataset, or they can be learned from scratch. Transfer learning entails fine-tuning the model for the intended task after pre-training it on a sizable dataset. By using the knowledge acquired from the source task, this method enhances performance on the target task. In order to reduce overfitting, the adaptive learning rate is set between 0.01 and 0.0001. The focus is on minimizing validation loss. With the rescale value set to 1/225, the shear value set to 1, the zoom range set to 0.2, and the horizontal and vertical flip set to true, the image is enhanced using the Keras Image Data Generator.

The suggested model An RGB image that measures 224 x 244 can be input into MobileNet. Subsequently, a block of three fully connected layers and a series of convolutional (Conv) layers with three-field filters are applied to the image. It is possible for the convolutional layers to process inputs of various sizes. Using a stack of kernels, it slides the input feature map and produces an output feature map.

MobileNet fully connected layers limit the model to an input of a given size and demand a fixed-length vector. A fixed-size input is needed for both the training and testing phases since MobileNet uses fully linked layers. The images in the dataset have a resolution of 1024 x 1024, which is greater than what is permitted for input. They crop or reduce the resolution from 1024 x 1024 to 224 × 224, to fit the size of the MobileNet input; this causes content loss and lowers recognition accuracy. Thus, they inject a Spatial Pyramid Pooling layer (SPP) between the final convolutional layer and the initial fully connected layer. After combining the features, the SPP layer creates a fixed-size output vector that satisfies the needs of the nearby fully linked layer. To put it briefly, the SPP layer combines data and removes problems related to cropping or resolution reduction.

G. Validation Method

Any machine learning model's efficacy can be evaluated using a variety of accuracy metrics that offer information about how well it performs. This chapter delves into the basic metrics—accuracy, precision, recall, and F1-score—that are used to assess the dependability and correctness of the created tamper detection models.

The ratio of the model's accurate predictions to its total number of forecasts is known as accuracy. Although accuracy is a valuable metric, it could not be enough in datasets that are imbalanced, meaning that one class is much more than the other. This is especially important when detecting medical picture tampering since real images may be more common than manipulated ones.

The precision of a model is determined by dividing the total number of positive predictions by the ratio of true positive forecasts. It shows how well the model can prevent false positives. Precision in tamper detection refers to how effectively the model detects tampered regions accurately while not classifying an excessive number of legitimate regions as modified.

Recall is the ratio of true positive predictions to the total number of actual positive cases in the dataset. It is sometimes referred to as sensitivity or true positive rate. When a negative event is mistakenly classified as positive (false positive) rather than a positive instance being missed (false negative), recall becomes important. Recall in tamper detection refers to how successfully the model detects tampered areas in the original dataset.

The harmonic mean of recall and precision is known as the F1-score. When both false positives and false negatives are significant, it is a useful indicator for assessing model performance since it strikes a compromise between precision and recall. The F1-score offers a single measure that accounts for both recall and precision, providing a thorough evaluation of the model's efficacy.

Confusion Matrix Generation

An essential tool for visualizing how well categorization algorithms are working is the confusion matrix. It displays the expected and actual class labels, allowing for a more thorough comprehension of the behavior of the model. The matrix is divided into four quadrants: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

True Positives (TP) are instances where the model correctly predicts the positive class (tampered) when the actual class is indeed positive.

True Negatives (TN) represent instances where the model correctly predicts the negative class (genuine) when the actual class is negative.

False Positives (FP) occur when the model incorrectly predicts the positive class (tampered) when the actual class is negative (genuine).

False Negatives (FN) signify instances where the model incorrectly predicts the negative class (genuine) when the actual class is positive (tampered).

The model's performance is graphically summarized in the confusion matrix, which also offers insights into areas for development. It shows if the model is correctly detecting tampered and legitimate regions for tamper detection, as well as situations in which it might be misclassifying them.

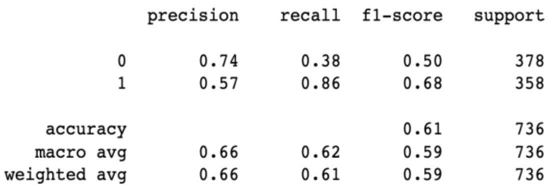
ROC Curve Analysis

In situations when datasets are unbalanced, Receiver Operating Characteristic (ROC) curves play a critical role in the evaluation of classification models. At different threshold settings, these graphs show the trade-off between the genuine positive rate (sensitivity) and the false positive rate (1-specificity).

The model's overall performance is measured using the Area Under the Curve (AUC) at various threshold values. Better model performance is indicated by a higher AUC, with values nearer 1 denoting exceptional class discrimination.ROC curves and AUC values in tamper detection provide information on how well the model balances true positives and false positives. The ROC curve shows how the sensitivity and specificity change in response to changes in the model's threshold for identifying an event as tampered.

IV. RESULTS

The most efficient learning strategy is ascertained using the performance metrics (specificity, sensitivity, and accuracy). The most effective learning approach is identified by comparing its performance measures (specificity, sensitivity, and accuracy) over the top three categories of picture features.



```
              precision    recall  f1-score   support

           0       0.74      0.38      0.50       378
           1       0.57      0.86      0.68       358

    accuracy                           0.61       736
   macro avg       0.66      0.62      0.59       736
weighted avg       0.66      0.61      0.59       736
```

Fig 8: MobileNet method Accuracy during training

The improved performance of the MobileNet approach over other learning methods is revealed through evaluation across many image attributes. The MobileNet algorithm's resilience and efficacy are demonstrated by the average accuracy, sensitivity, and specificity rates of 66%, 67%, and 67%, respectively. These results place MobileNet in a promising position for picture classification tasks, particularly when achieving a trade-off between computing efficiency and accuracy. Additional investigation and optimization may improve the model's efficacy and suitability for a wider array of uses.

V. CONCLUSION AND FUTURE WORK

The significance of actual medical images and the growing possibility of deep learning to produce convincing deepfakes were the first topics covered in the inquiry. The goal of identifying fictitious malignancies from actual ones in 3D CT scans of human lungs was presented in a way that highlighted how difficult it would be given the realistic tampering tactics. A range of deep learning algorithms were created and tested for their accuracy in identifying doctored medical images using the Medical Deepfakes: Lung Cancer dataset. This study makes a variety of contributions to the field of medical picture tamper detection. First, it provides an in-depth analysis of deep learning algorithms, showcasing their ability to discern between real and altered areas in medical photographs. Analyzing algorithms like Random Forest Classifier, Logistic Regression, Bagging Classifier, and Stacking Classifier offers important insights into their respective advantages and disadvantages for tamper detection applications.

Additionally, this study highlights the importance of accuracy metrics in evaluating tamper detection model performance, such as accuracy, precision, recall, and F1-score. Accurate assessment and comparison of these metrics among various algorithms allows for well-informed choice of the best model for given applications.

Limitations and Future Directions

Despite the encouraging outcomes of this research, there are a few constraints to take into account. The size of the dataset is one of its main drawbacks; although representative, it might not adequately represent the range of medical images seen in everyday situations. Furthermore, the class imbalance in the dataset might have affected how well some algorithms performed. More investigation using larger and more varied datasets may yield a more thorough evaluation of model performance. Subsequent investigations may concentrate on alleviating the constraints that were faced throughout this study. For example, the Random Forest Classifier's performance might be enhanced via parameter tuning and algorithm modification. Investigating other ensemble methods, such boosting algorithms, may also be beneficial, especially when it comes to resolving the issues brought on by class disparities.

REFERENCES

[1] R. Dixit , R. Naskar, and A. Sahoo . Copy-move fo rgery detect ion exploiting statistical image features, 2017 Internat ional Conference on Wireless Communicat ions, Signal Pro cessing, and Net working (WiSPNET), Chennai, 20 17, pp. 2277 -2281.

[2] A. J. Fridrich, B. D. Soukal, and A. J. Luk s, Det ection of copy -move forgery in digit al images, in Proceedings of Digital Forensic Research Workshop , Citeseer 2003.

[3] B. Patil, S. Chapan eri, and D. Jayaswal. Impro ved image splicin g forgery localization with first digits and Markov model feat ures, IEEE Int ernational Conferen ce on Int elligent Techniques in Con tro l, Opt imization and Signal P rocessing (INCOS), Srivilliput hur, 2 017, pp. 1-5.

[4] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting tr aces of re-sampling. IEEE Trans. Signal Pro cessing, vol. 53, no. 2, pp. 758–767, 2005.

[5] Bo Liu, Chi-Man Pun, and Xiao-Chen Yuan. Digital Image Forgery Detection Using JPEG Feat ures and Local Noise Discrepancies. Hindawi Publishing Corporation, Scientific World Journ al. http://dx.doi.org/10.1155/2014/230425.

[6] Ritu Agarwal and Om Prakash Verma, “An efficient copy move forgery detection using deep learning feature extraction and matching algorithm”, Springer Science Business Media, LLC, part of Springer Nature 2019, 23 December 2019.

[7] Arfa Binti Zainal Abidin, Azurah Binti A Samah, Hairudin Bin Abdul Majid and Haslina Binti Hashim, “Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review”, 978-1-7281-6726-8/19/$31.00 2019 IEEE.

[8] Gul Muzaffer and GuzinUlutas, “A new deep learning-based method to detection of copymove forgery in digital images”, 978-1-7281-1013-4/19/$31.00 2019 IEEE.

GitHub Link: - https://github.com/aknomula/DL-NN-Project.git

[9] Mohammad Manzurul Islam, GourKarmakar, Joarder Kamruzzaman and Manzur Murshed, “A Robust Forgery Detection Method for Copy– Move and Splicing Attacks in Images”, MDPI, electronics,12 September 2020, doi:10.3390/electronics9091500.

[10] Zankhana J. Barad and Mukesh M. Goswami, “Image Forgery Detection using Deep Learning: A Survey”, 2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS), 978-1-7281-5197- 7/20/$31.00 2020 IEEE.

[11] Amit Doegar, Maitreyee Dutta and Gaurav Kumar, “Image Forgery Detection Using GoogleNet and Random Forest Machine Learning Algorithm”, Journal of University of Shanghai for Science and Technology, Volume 22, Issue 12, December – 2020, doi - 10.51201/12508.

[12] Xinyi Wang, He Wang and ShaozhangNiu, “An Intelligent Forensics Approach for Detecting Patch-Based Image Inpainting”, Hindawi, Mathematical Problems in Engineering, Volume 2020, Article ID 8892989, 10 pages, 28 October 2020, https://doi.org/10.1155/2020/8892989.

[13] Rahul Thakur and Rajesh Rohilla, “Recent Advances in Digital Image Manipulation Detection Techniques: A brief Review”, Forensic Science International, 24 April 2020,Published by Elsevier,https://doi.org/10.1016/j.forsciint.2020.110311.

[14] Kunj Bihari Meena and Vipin Tyagi, “A Deep Learning based Method for Image Splicing Detection”, Journal of Physics: Conference Series, CONSILIO 2020, IOP Publishing,doi:10.1088/1742-6596/1714/1/012038.

[15] Manjunatha S and Malini M Patil, “Deep learning-based Technique for Image Tamper Detection”, 2021 Third International Conference on Intelligent Communication Technologies & Virtual Mobile Networks (ICICV), 978-1-6654-1960-4/20, doi:10.1109/ICICV50876.2021.9388471, 2021 IEEE.

[16] Marra, Francesco &Gragnaniello, Diego &Verdoliva, Luisa &Poggi,Giovanni. A FullImage Full-Resolut ion End-to-End-Trainable CNNFramework for Image Forgery Detect ion, 2019.

GitHub Link: - https://github.com/aknomula/DL-NN-Project.git