National College of Ireland

Medical Image Forgery Detection

MSc Research Project

M.Sc., in Cyber Security

Rithin krishna Dilipkumar
Student ID: 20199830

School of Computing
National College of Ireland

Supervisor: Mr. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……Rithin krishna Dilipkumar……

Student ID: ……20199830……

Programme: ……. M.Sc., Cyber Security…. **Year:** Sept 2021-Sept 2022

Module: …… **MSc Research Project**……

Supervisor: ……Mr. Imran Khan……

Submission Due Date: ……..15th August 2022……

Project Title: …… Medical Image Forgery Detection……

Word Count: ……6346…… **Page Count**……21……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: …… Rithin krishna Dilipkumar……

Date: ……15th August 2022……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Medical Image Forgery Detection

Rithin krishna Dilipkumar
Student ID 20199830

Abstract

Currently, the majority of businesses and organizations rely on internet services because of the improvements in technology and how simple they are to acquire and use. In the medical sector, digital photographs have also gained more significance than before. X-rays, CT scans, and MRI scans are just a few of the medical information that are now preserved and shared digitally. It has been demonstrated that both patients and medical professionals can more easily access and save digital photographs, making them more useful. Cybercriminals may have simple access to private patient information thanks to the ease with which medical photographs are available online, which might have extremely negative consequences. This study recommends using deep learning techniques to develop the Random Forest and ResNet-50 models, as well as algorithms like Watershed, to accurately detect manipulation in medical photographs. The major objective of this study is to correctly complete the research by achieving maximum accuracy utilizing faster deep learning algorithms and a big, current data collection.

1. Introduction

The picture, or visual, is one of the most vital communication tools. Images are used to communicate ideas in a clearer and more particular way. The human brain retains an image-based message better than any other sort of communication, as is common knowledge. Similar to how a coin has two sides, modern science may be employed constructively or destructively. These days, there are many options for free picture editing software. While some individuals utilize this tool to enhance and beautify their photographs, negative sections of society may use it to distort delicate images, maybe with serious repercussions. Photos are simple to get thanks to modern low-cost technology. Huge volumes of data can be collected, kept, and shared by everyone. Based just on appearance, humans have trouble telling if a picture is real or has been manipulated. Digitally created forgeries have dramatically increased across all major media outlets and on the Internet. This pattern undermines the dependability of digital photographs by highlighting significant faults. Every sector uses digital photos in some way to advance their operations, making work simpler and more efficient, and as we all know, the world is becoming increasingly digital. Digital images are frequently utilized in the healthcare sector to produce diagnostic tests, medical reports, and imaging studies (such as X-rays, MRIs, CT scans, ultrasounds, and PET scans).[10]

Imaging, as used in medicine, is the process through which specialists take photos of patients' bodies in order to diagnose them. This is carried out in order to trace the progression of any discovered medical symptoms as well as to diagnose diseases in people before symptoms ever arise. Comparatively speaking, analogy pictures made from film processing lack the accuracy that digital medical images have. It allows doctors to carry out extra procedures,

such 3D viewing, expansion, and reduction, to enhance diagnosis. They occupy less physical store space, are easier to modify, archive, save, and recover, and need less maintenance.

Digital medical imaging is becoming increasingly common as a result. Because consumers and application developers are not well-versed in cyber security, medical digital pictures are more susceptible to manipulation. As a result, it is crucial to develop methods to verify the accuracy and reliability of digital photographs, particularly when photos connected to the healthcare sector are used as evidence in court, in news reports, in medical records, or by insurance companies to provide financial help. These issues will be addressed, and a powerful system to identify fake medical images will be developed as a result of the study project.[11]

1.1 Background

Due to its extensive availability on internet platforms and the variety of devices that may access it, medical data has become more susceptible to cyber-attacks by criminals. The research tests that have been conducted so far have made it abundantly evident that medical image security is still not considered, that it is underdeveloped, and that it is disregarded. Attackers have not yet started to fully utilize these medical deficiencies as of yet. But in the near future, it's probably going to grow into a significant source of worry. In the past, deep learning tools and algorithms were discovered to be used to create fake movies and photographs, but in 2019 it was discovered that they may also be used to modify 3D medical scans. Medical data is an unstoppable target for cybercriminals since it is non-perishable. Hackers that have expertise planning their assaults depending on the return they will see on their investment because hacking takes a lot of time and work. Access to medical data has been effectively obtained, and those who have done so have benefited greatly. PACS, or picture archiving and communication system, is used by the majority of hospitals and medical research centres so that pictures from various diagnostic procedures, including MRIs, mammograms, and ultrasounds, may be viewed from different systems on-site or through the cloud. In more extensive installations, there may be a number of acquisition gateways and imaging equipment spread across several sites that are connected over the Internet. Throughout the course of our research, we discovered that many small medical practices all around the world use PACS software that is free and open-source but is not necessarily deployed securely.[18]

The study subject aims to create a precise and rapid algorithm to identify medical image piracy by carefully examining the body of prior research in this area and enhancing it with more effective approaches. These hazards related to medical image security, as well as the need to develop an effective and reliable technique for medical image forgery detection, are critical issues that need to be addressed in the realm of cybersecurity. These issues are the main focus areas for this research project.

1.2 Motivation

According to the information discussed above, all medical data has become easier to access as a result of technological advances. For example, the healthcare industry now stores and disseminates patient-related images like X-ray reports, CT scans, and reports that include results from various diagnostic tests electronically. The delivery of medical reports to patients is increasingly possible via email or other social media channels. Now that all medical information is accessible online, it is imperative to develop an effective algorithm that can detect fake medical images with the highest level of accuracy.

This is because the availability of all medical data online makes cybersecurity a need. We can see from the aforementioned experiments that while deep learning methods can help medical professionals diagnose disorders in more sophisticated ways, they can also be used by attackers to alter photographs in dangerous ways. My curiosity to find out more about how to spot tampering in medical photographs was sparked by the aforementioned trials.[12]

1.3 Research Question

How can we use a modern image recognition model called Random Forest and ResNet-50 to identify medical image forgery with high level of accuracy?

This research question is an effort to discover a more precise method of identifying doctored medical photographs. In order to address the healthcare sector's lack of security awareness, this research reviews recent studies and suggests a trustworthy approach for detecting doctored medical photographs. By applying more powerful and rapid deep learning models like Random Forest and ResNet-50, it aims to enhance counterfeit detection methodologies.

1.4 Research Objectives

The objective of this work is to close the knowledge gaps in the field of medical image forgery detection. The following parameters will be adequately archived at the conclusion of this study:

- The identification of medical image alteration is being investigated using a variety of contemporary approaches and algorithms, making this research extremely useful. In the most recent investigation of medical image tampering, Random Forest and ResNet50 were employed.
- Thorough literature review of the work done in the field of medical image fraud detection and the machine learning approaches utilized for it. This study we also compare other machine learning approaches as well as photo forensic tools with literature surveys.

- Given that medical equipment and data are easily manipulated and have widespread access, medical data security is an issue that needs more focus. Medical data integrity is incredibly important since it is directly related to people's lives. Small mistakes may have major repercussions that affect not just common people but also corporations and governments that are connected to them either directly or indirectly. This work is crucial because it tries to create a system that can accurately and effectively detect the manipulation in medical images.
- The methods utilized in this study do not in any way violate the privacy of individuals or organizations and have the stated goal of benefiting society. By not disclosing any identifying information, data received from a single individual, for instance, will be kept anonymous. Additionally, research data will be protected and kept secure, with no unauthorized individuals being able to access it. The goal of doing this is to guarantee that the study is carried out in a completely ethical manner.

A variety of tasks, such as recommendation engines, picture classification, and feature selection, may be accomplished using random forests. Using the most votes possible for categorization and the average for regression, it constructs decision trees from many data. It outperforms other algorithms in classification problems. Convolutional Neural Networks are a kind of deep neural networks, and ResNet-50 is a pretrained machine learning model for image categorization that may be utilized as a cutting-edge model.

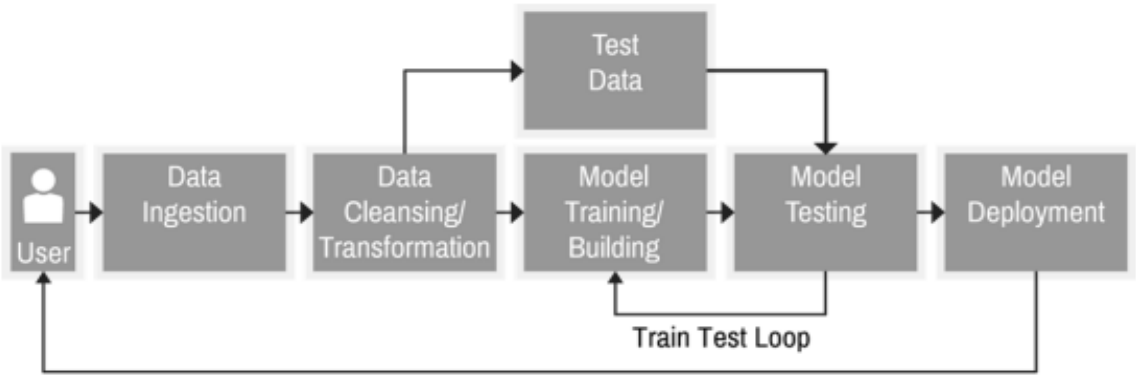

Figure 1: Methodology of Machine Learning

2. Related Work

2.1. Convolutional Neural Network-Based Extended Forgery Detection Framework for COVID-19 Medical Data

Joeseph paul cohen (2020) discusses about this study which uses the Error Level Analysis (ELA) approach, which analyzes the data's noise patterns, to identify forgeries in COVID-19-related medical photos using a Neural Network Model dubbed the Convolutional Neural Network. The ELA uses a compression approach to identify medical picture alteration. The longevity and quality of the images decide how much compression is used. Used deep

learning model: A Convolutional Neural Network was used to categorize and compare the photographs in order to spot frauds. Out of the 400 total pictures, 200 were real images and 200 were modified. Testing was done on the remaining 144 images. The research in the aforementioned journal found that this method had an accuracy rate of 92 percent, but deep neural networks of the CNN variety are most frequently applied to the analysis of visual data. ResNet-50 is a fifty-layer deep neural network that was trained with n images, therefore which has an higher chance of providing an better accuracy rate.

2.2 Comparison between different convolutional neural network frameworks for image classification.

As proposed by Sheldon Mascarenhas (2021), over the past 20 years, advances in artificial intelligence have made significant progress. Machine learning is currently a hot topic due to the rapid advancements in AI. We can extract, comprehend, and train data using algorithms and programming approaches thanks to machine learning. Deep learning is a notion that emerged as a result of machine learning. It employs algorithms to build an artificial neural network, use it to evolve and learn, and then use it to make decisions on its own. When deep learning is used to execute the process of classifying photos into sets of various categories, company productivity is increased since time and labor are saved. The accuracy of the VGG16, VGG19, and ResNet50 architectures have been compared while all three of these models are used to address the identical picture categorization issue. Based on the analysis, we have come to the conclusion that ResNet50 is the optimal architecture. In comparison to the proposed research, we use methods like watershed together with ResNet 50 and Random Forest algorithms, to try and get more promising results and accuracy rates. VGG-16 is a simple stack of convolutional + max-pooling layers that is unable to extract complex patterns like ResNet-50 and Random Forest models. A pre-trained Convolutional Neural Network (CNN) image categorization model is called ResNet-50.

2.3 Using Random Forest and+ watershed transformations for mapping.

Qingsheng Liu (2020) discusses the most important method for examining the development, invasion, and preservation of quasi-circular vegetation patches (QVPs) is to identify them and keep track of their pattern dynamics. A practical method to identify the QVPs is to use high resolution satellite remotely sensed data. By combining the random forest classification and watershed transformation image segmentation techniques, this work employed two-seasonal CBERS04 pansharpened multispectral pictures to detect the QVPs. The research's accuracy level was poor when these two methods were used, and we were able to find a similarly low accuracy level in the present proposed study as well. As a result, utilizing ResNet50 has demonstrated to have higher accuracy levels than Random Forest and watershed algorithms.

2.4 Comparison with digital watermarking.

Farah Deeba (2020) discusses on Digital watermarking, is the procedure used to safeguard the secret data embedded in digital media in order to maintain the ownership of the media data. To make the watermark active and resistant to removal by various assaults, many methods have been developed. In this paper, we used deep learning to generalize digital watermarks and remote ownership verification of DNN models based on embedded watermarks. Despite the clear

benefits of the watermarking method, active detection calls for specialized technology or programs to incorporate the authentication token inside the image prior to it being transmitted. The primary benefit of deep learning systems is their capacity to automatically extract complicated representations of data via end-to-end training from raw data, therefore greatly lowers the labour-intensive process of manually designing features.

2.5. Comparison with photo forensic tools.

Ehsan Nowroozi (2020) discusses the use of image forensics is essential in both criminal and civil court cases. Machine learning techniques are being used more and more in picture forensics. However, machine learning-based systems also come with a variety of drawbacks and weaknesses. It is clear from this study that employing photo forensics techniques only won't get the greatest results. Numerous algorithms based on statistical analysis and pattern recognition have been used in image forensics; more recently, as computing power has increased, ML techniques, particularly deep learning, have received additional attention. These techniques have proven successful in numerous image forensics competitions. In recent years, ML/DL-based picture forensics techniques have received a lot of attention. For a variety of visual forensics applications, techniques based on DL have consistently shown outstanding results.

3. Research Methodology

The study methodology here adopts Arpita Halder's (2021) recommended machine learning workflow. This method of study was chosen since it is both understandable and effective. The execution is very functional and flexible, enabling the accomplishment of the intended outcome in line with the research topic.

The machine learning and deep learning models are piece of software that searches for patterns in data to better carry out the tasks it is assigned. Any procedure that depends on a collection of facts or rules may be automated using machine learning. Artificial intelligence and deep learning as every operation looks for methods to better the resources at hand and the results based on historical data, architectures are a hot issue in business right now. These architectural explanations detail the important steps in converting unstructured data into training sets of data that can be used by a system to make choices. They also describe the many layers that make up the machine learner-cantered method. The fundamentals of machine learning and deep learning are illustrated in the following diagram.[17]

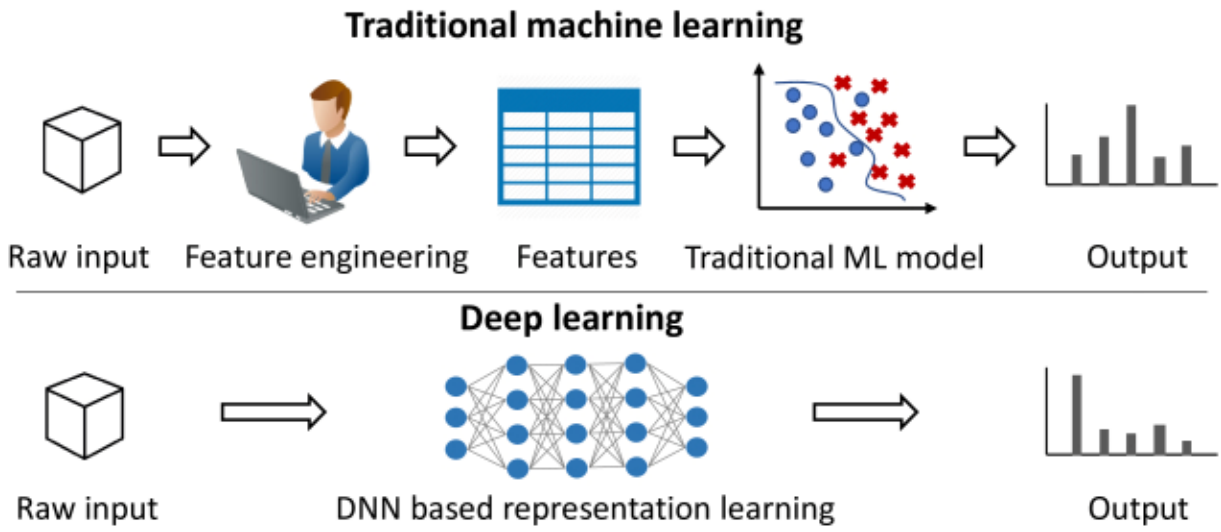

Figure 2: Implementation of Machine learning and Deep learning

3.1 Dataset Extraction

The dataset is downloaded to the computer and put into the local system so that the application may execute it to train and test the data. The collection, which includes about 100 CT scan pictures, is available to the public. Images that are both fraudulent and real are included in the data. A cancer's location and categorization are shown in each row of the csv file, along with whether it is real, false, or removed. There are four different classes. If the image is labelled as TB, then it's True-Benign (A location that actually has no cancer), If the image is labelled as TM, then it's True-Malicious (A location that has real cancer), If the image is labelled as FB, then its False-Benign (A location that has real cancer, but it was removed), If the image is labelled as FM, then it's False-Malicious (A location that does not have cancer, but fake cancer was injected there).

3.2 Data pre-processing

The dataset used for this research technique is made up of CT scan pictures of human lungs. No two photographs may be in the same orientation or have the same attributes because of the sheer number of images in the dataset. For this reason, pre-processing of the photos is necessary so that we may treat each image identically and carry out testing and training effectively. The pre-processing procedure entails converting RGB colors to grayscale, shrinking the image, eliminating image blurring, etc. Additionally, the images will be rotated and cropped to conform to the unified design. We use the Gaussian denoising approach to attempt to clean up the pictures' noise. To obtain the edges of the pictures, canny edge detectors are also used. Additionally, binary processing is done in order to transform the picture to a binary representation.

3.3 Visualization

Visualization is the stage when we plan how the graphs will be plotted in the software, and the data for testing is selected in accordance with this knowledge. This fundamental phase is followed by the data testing, making the visualization a crucial stage in the flow diagram.

3.4 Dataset splitting
We are prepared to divide the data at this point so that each algorithm may be trained on its individual set of data. In order to compare the photos and produce the output, we will take a smaller collection of data from the training set and send it to the testing set.

3.5 Define algorithm model
We must decide on the methods we'll utilize in the machine after we have finalized the data for splitting. Here, we're going to employ two algorithms: ResNet50 and random forest. Not all of the algorithms are employed at once. In order to determine whether an image is legitimate, we first run a certain algorithm—either ResNet50 or random forest—do the training and testing, and then assess the correctness of the image. After that, we repeat the process with the second algorithm and examine the results. The procedure for both algorithms is thus the same but is carried out in various phases.

3.6 Training the data
The need for training arises from the need to educate our algorithms of the intended use of the data. The data must become used to algorithms before it can effectively carry out the purpose it was intended for. Our algorithms have been taught to distinguish between an image that has been modified and one that has not in this study.

3.7 Cross-validation
The data are cross-validated in the following step, which compares and verifies the comparison between the photos to determine which is a false and which is the original, following training and testing. The metrics are obtained since this result will be used as the final output that is shown.

4. Design Specification

The most effective machine learning models for determining if the presented data is real or not are random forest and ResNet50, according to studies on the subject topic. The dataset is used to train and test them so they can deliver the intended outcomes. As seen in the list below, a thorough architecture for each machine learning method is presented.

4.1 Random Forest

Regression and classification problems are frequently solved using the machine learning method known as random forest. The greatest number of votes are used for classification and the average is used for regression as it builds decision trees from a variety of data. Being ability to accept data sets containing both dependent and independent variables, as in classification and regression tasks, is one of the Random Forest Algorithm's key characteristics. It performs better than the competitors in terms of classification issues. Given its efficacy, Random Forest is a high-performance method that is regularly used in many different fields. It has the ability to work with binary, constant, and organized data.[14] The following figure shows the detailed architecture of the Random Forest Model:

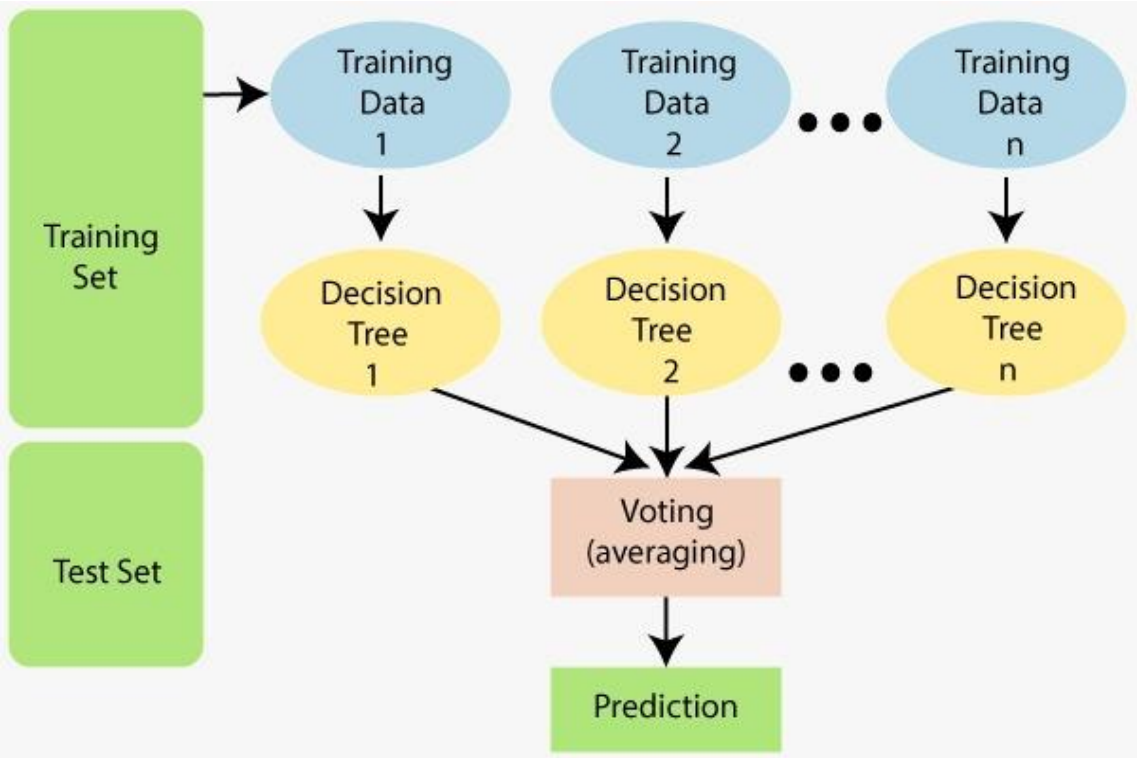

Figure 3: Random Forest architecure

4.2 ResNet50

A network may contain thousands of layers and yet function properly because to the ResNets-50 design, which made it possible to train extraordinarily deep neural networks. In order to increase accuracy, ResNets-50 was used to the picture recognition task. The design known as ResNet-50 is focused on residual neural networks and stands for residual network. What distinguishes a residual network are the identifying links. Identified connections are used to direct the input to each residual block's conclusion. There are five stages in the ResNet-50 model specifically, and each level has a unique residual block. Each residual block is consisting of three layers containing convolutions of 1x1 and 3x3 on each layer. A fundamental concept is residual blocks. Each layer in conventional neural networks talks to the one above it. Every layer inside a network containing remaining blocks connects with the layer above it as well as the levels that are situated two to three hops away. These connections are referred to as identity connections. The graphic below shows the detailed architecture of the ResNets-50 Model:[13]

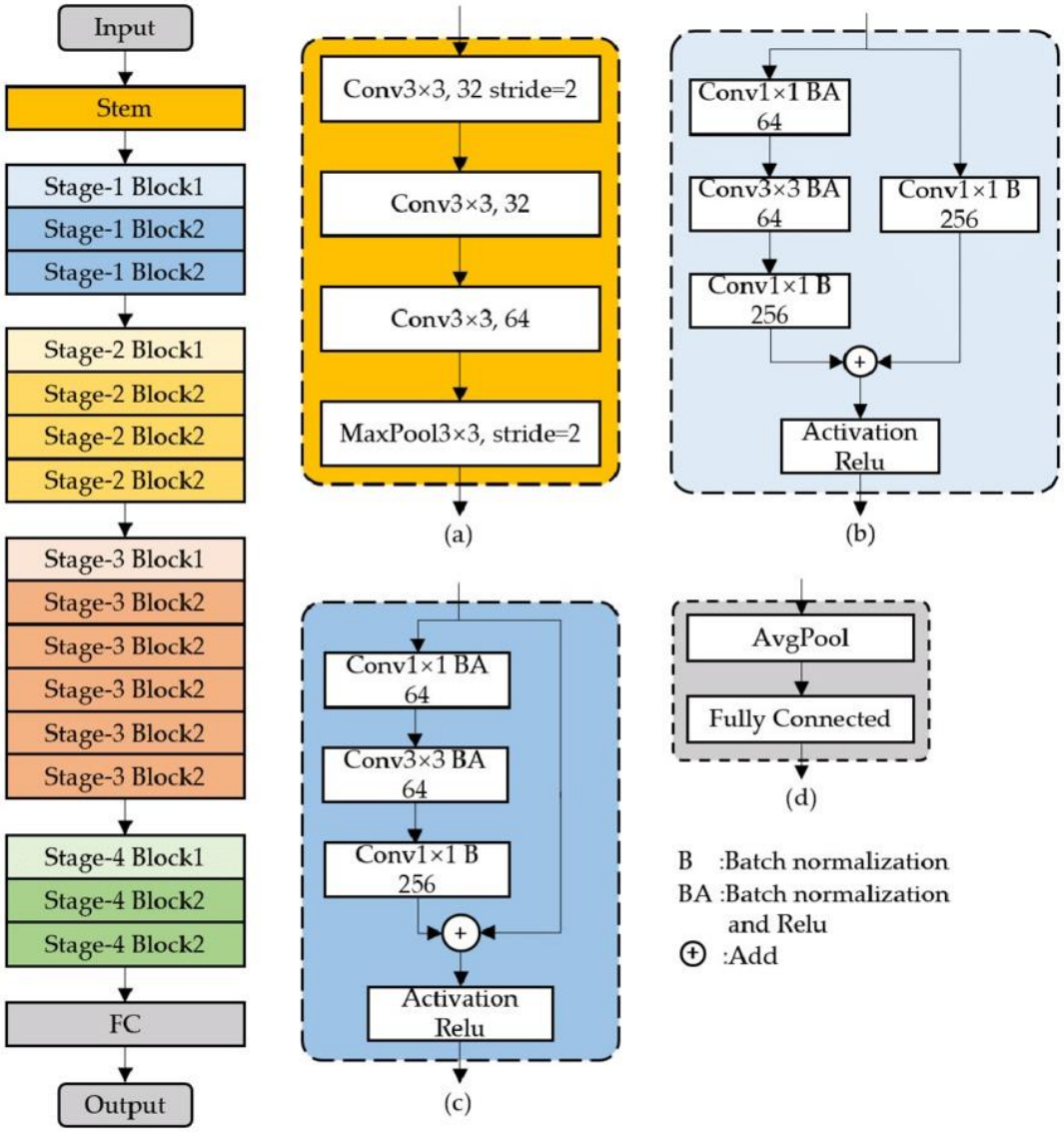

Figure 4: ResNet-50 architecure

4.3 Rectified-Adam Optimizer

In contrast to Joeseph Paul Cohen's (2020) earlier investigations, the proposed research uses the Rectified-Adam optimization technique, which is more efficient . Compared to Stochastic Gradient Descent Optimizer, it is more efficient since it instantly and automatically adjusts to the learning rate. Rectified-Adam also makes use of the second moment average of the grades (the uncentered variance). The method generates an exponential growth rate for the grade and the squared grade, and the coefficients beta1 and beta2 determine how quickly these moving averages depreciate. Moment estimates are skewed towards zero when the starting value, as well as the 1 and 2 values of the moving averages, are close to 1.0. (preferred). Computing biased estimates first, followed by estimates with bias correction, eliminates this prejudice.[15]

4.4 Dataset Information

Two sets of 100 CT scan images make up the dataset. One set has 80 CT scans, whereas the other set only includes 20. They are 3D CT scans of human lungs, some of which have undergone alterations by having real cancer removed and fake cancer added. The purpose of this dataset is to distinguish between genuine and fake cancers and to identify areas where diagnostic scans have been manipulated. With the use of this information, it will be possible to determine if medical scans have been manipulated and to discriminate between true and fraudulent malignancies. For each test, an actual truth csv table is available. The position (x, y, and z [slicing#]) and classification of each item in the csv file correspond to a cancer that is either true, false, or eliminated. 512x512 images make up a CT scan. The sequence usually includes 100 to 300 slices (the z axis). Cancers may occupy a large number of slices along the z-axis. Each pixel's value is known as its Hounsfield value (radiodensity). CT scans are captured using the DICOM standard.[16]

5. Implementation

5.1 Medical image forgery detection implementation

As discussed by Samir Elmuogy (2021) an efficient technique for CT scan images classification with the Methodology of deep learning and machine learning algorithms.
Putting the research proposal into practice, this section demonstrates the approach used to conduct research on medical image forgeries and the installation of the ResNet50 and Random Forest algorithms in the data resources in order to determine the highest accuracy rates.

- The jupyter notebook application is launched from the local host machine in the first stage using the PyCharm IDE.
- The jupyter notebook is loaded with the prepared dataset of the CT scans of human lungs.
- Since there are many photos in the dataset, it is not required for them to all share the same pixels and colour scale. Instead, all of the images are transformed to a single uniform scale based on the pixels and colour scale they contain.
- The selected algorithms Random Forest and ResNet-50 are defined and, after this, the dataset is divided into two parts for testing and training purposes, respectively.
- The optimizer (Rectified-Adam) utilized in this study is also specified after the specification of algorithms.
- The model is tested and trained after the optimizer has been defined. The model is trained utilizing training data, and then the functioning validation is carried out using the testing data.
- With the help of the results, the accuracy is checked, and if the required accuracy is not attained, testing and training are repeated until it is accomplished.

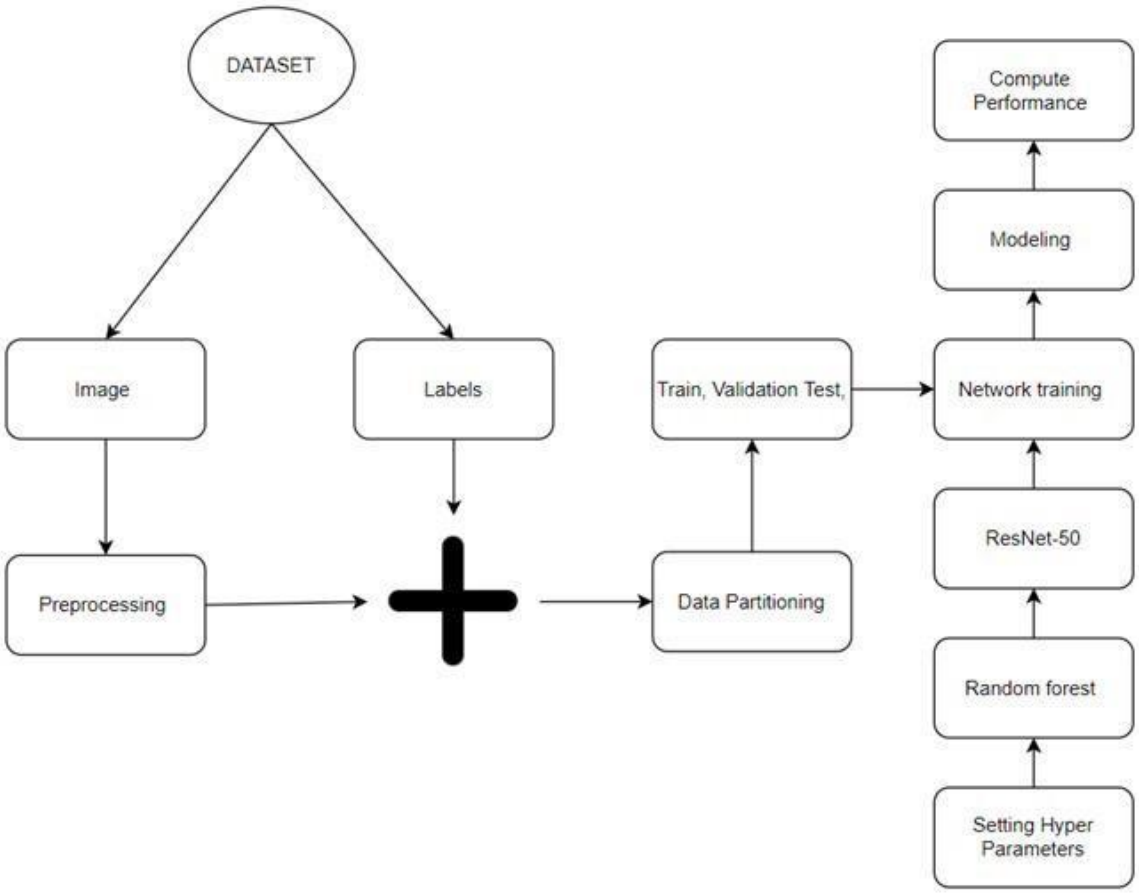

Figure 5: Implementation of Random Forest and ResNet50 in medical image forgery detection

5.2 Tools & Language used for implementation:

PyCharm 2022.2: In order to establish a suitable environment for effective Python, web, and data science development, PyCharm is a specialized Python Integrated Development Environment (IDE) that offers a wide range of crucial tools for Python developers.

Jupyter notebook 6.4.12: It is an interactive tool that runs and edits the code through a browser. The process of troubleshooting is made easy since it performs and displays each line's result immediately after the execution. Other features include data cleansing, statistical modelling, data visualization, and many more.

Python 3.7: It is an interpreted object-oriented programming language. Because to its dependability, clarity, and usability, it is very simple to utilize. For the majority of projects, it is recommended for performing algorithms and comparing datasets. Python is more widely used because it is more straightforward than other programming languages. Python has a simpler and easier to write syntax, making it more effective and code-friendly.

TensorFlow library: is an end-to-end open-source machine learning platform with an emphasis on deep neural networks that offers a collection of procedures for creating and training models using Python.

Scikit-learn library: The most effective and reliable Python machine learning library is called Scikit-learn. Through a consistent Python interface, it offers a variety of effective methods for statistical modelling and machine learning, covering classification, regression, grouping, and dimensionality reduction.

Pandas: It is a very powerful tool in Python used for data manipulation and analysis

Matplotlib: It is a comprehensive Python package that aids in the creation of visual plots and graphs for the outcomes attained in the application of machine learning models.

Numpy: When working with arrays is required, Python uses this library function. Additionally, it supports several mathematical operations including algebra and matrices.

6. Evaluation

When we carry out the application of the study in a constrained context, we carry out the evaluation of a model by providing experimental data. This is done to determine whether the outcomes satisfy our predefined standards, including matching features like being viable and dependable, among others. The researcher will be able to determine whether the accuracy matches the intended accuracy by doing the implementation under controlled circumstances and determining whether the experiment was successful.
Healthcare data security is a problem that needs increased attention since medical equipment and data are easily manipulated and often accessed. Since medical data is so intimately linked to people's lives, it is especially crucial to maintain data integrity. Small mistakes may have big impact on not just normal people but also the governments and organizations they engage with directly or indirectly. Because it tries to provide a trustworthy and efficient method for spotting fake medical images, this research is crucial. Research observations are the results of actual research execution under supervised circumstances. The experimental data presents us with attainable and quantifiable results. As a result, the researcher is able to conduct experiments in a trial-and-error manner until the requisite accuracy is obtained. This research proposal's experiment will be conducted using the following criteria:

- The archived result in this study is validated using a 5-fold cross validation method.
- The data is separated into five equal parts according to this procedure, therefore the 100 CT scan images available will be evenly divided into those five parts.
- One portion of the separated parts is chosen to serve as the test set, with the remaining portions serving as training models.
- We learn the four distinct parameters, from the training result such as:
  False-positive

False- negative

True- positive

True- negative

- From this the average sensitivity and specificity is taken respectively from the calculations done to the average of the results of the 5 records

Precision: It displays the actual positive values that were found among the estimated positives.

$$\text{Precision} = TP / TP+FP$$

Recall: Indicated by this number is the expected positive deducted from the overall positive value.

$$\text{Recall} = TP / TP+FN$$

F1-Score: By averaging the Precision and Recall values, this score is determined.

$$\text{F1 score} = 2*(\text{Precision}*\text{Recall})/ (\text{Precision} + \text{Recall})$$

6.1 Experiment 1

The classification report and confusion matrix for the Random Forest algorithm implementation is as shown below:

```
print(classification_report(y_test, y_pred))
```

	precision	recall	f1-score	support
fake	0.00	0.00	0.00	108
real	0.48	1.00	0.65	100
accuracy			0.48	208
macro avg	0.24	0.50	0.32	208
weighted avg	0.23	0.48	0.31	208

Figure 6 classification report of Random Forest algorithm

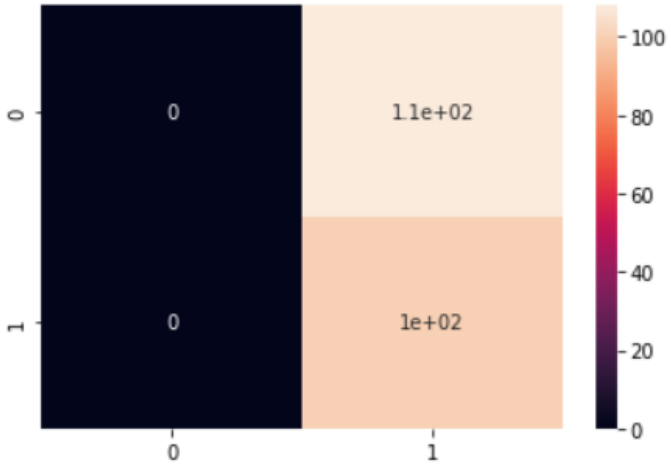

Figure 7: Confusion matrix for Random Forest algorithm

From the given figures we can conclude that the algorithm Random Forest gives us a much less accuracy rate than the algorithm ResNet50

6.2 Experiment 2

The sample image used for training, accuracy plot and confusion matrix for ResNet50 algorithm implementation is as shown below:

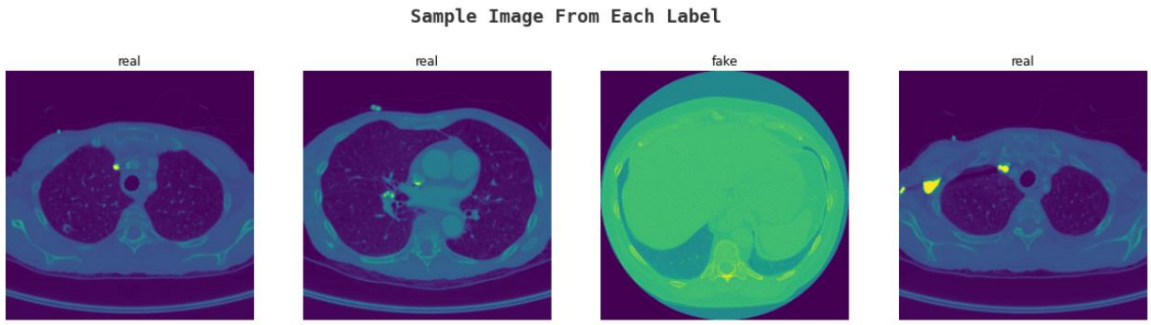

Figure 8: Display of sample image for training the model.

```
<matplotlib.legend.Legend at 0x2a49dd4db88>
```

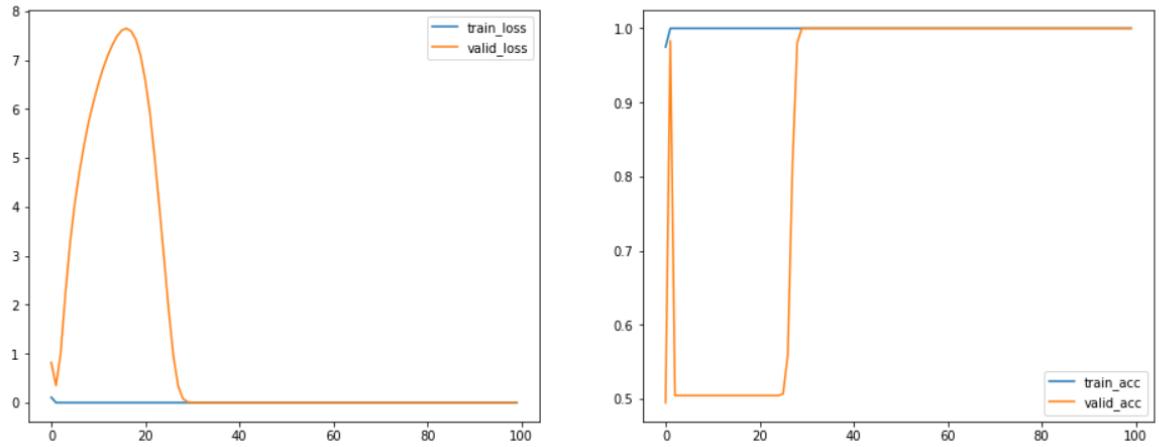

Figure 9: Accuracy plot of ResNet50 algorithm

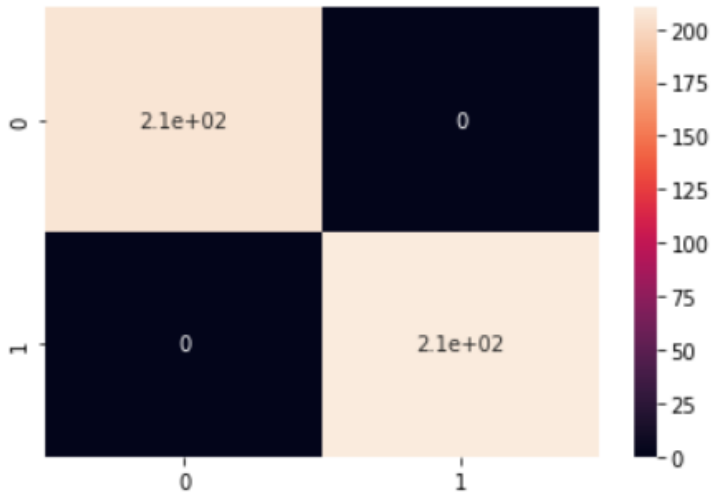

Figure 10: Confusion matrix for ResNet50 algorithm

From the given figures we can conclude that the algorithm ResNet50 has more level of accuracy rate when compared to algorithm Random Forest.

6.3 Discussion

The project's execution has taught us that ResNet50 is more effective than Random Forest in detection of the forged medical image. The plots of the confusion matrix, accuracy graph and classification repot for both of these methods that were acquired during program execution provide evidence in favour of this. ResNet50 is having an accuracy rate of 100% and the random forest is determined to have a 48% accuracy rate. We may infer from this that having ResNet50 allows us to evaluate medical image forgeries more effectively. All of the goals outlined at the start of the study process were accomplished, and the end result was satisfactory.

6.3.1 Comparison of Machine Learning Models implemented

Model Implemented	Accuracy	Precision	Recall	F1 Score
Random Forest Algorithm	0.48	0.23	0.48	0.31
ResNet50 Algorithm	1.0	1.0	1.0	1.0

A different training subset is created using the random forest algorithm using replacement from a sample of training data, and the results are determined by majority vote whereas ResNet50, a deep learning system, with extra layers and a ReLU, deep learning algorithms are effective in speeding up training. Additionally, it makes use of a method known as LRN, which aims to increase the algorithm's capacity to store data in memory and how quickly it consumes it. ResNet50 employs a variety of characteristics and methodologies, and as a result, the output is highly accurate. Also changing in dataset can bring in variations in the level of accuracy rate

because the amount of data in every dataset differs as well as the image quality and format can also play a major role.

7. Conclusion and Future Work

Medical image forgery is one of the unexplored areas of cyber security. As demonstrated in this study, medical pictures and data are crucial since they include information about the lives of patients. Any alterations to these images run the risk of misdiagnosing the patient's condition, which might have catastrophic consequences. Some people use doctored medical images to trick insurance providers or pose as disabled in order to get job offers. This is dishonest and morally repugnant. Therefore, it is essential to provide a reliable method for spotting fake photos in the medical field. Because the information is tied to people's lives, which is vital, influencing in the health industry is not only unethical but might also have devastating results. Healthcare professionals are not currently required by law to confirm the validity of medical images. Double-checking the accuracy and editing of any medical images is advised. The main objective of this study is to develop a highly accurate and trustworthy method for identifying medical image manipulation, which may lower the likelihood that patients will receive the incorrect diagnoses as well as any offense that might be committed using altered images and have disastrous repercussions.

This study applied two different algorithms from machine learning and deep learning methods to find out the best accuracy rate in detection of forged medical images and good result was obtained. ResNet50 stood out among them as having a substantially higher detection rate for medical image counterfeiting. As a result, the research was successful in achieving all of the initially stated goals. Because more deep learning algorithms can produce findings with higher accuracy than convolutional machine learning algorithms, the research emphasizes this point.

7.1 Limitations

Due to time constraints, host system restrictions, and a lack of access to huge datasets with the necessary licenses and permissions for research usage.

7.2 Future Work

In the future, a larger number of algorithms can be evaluated and contrasted for improved accuracy, and novel combinations of algorithms and methodologies will be used and evaluated based on the time and resources available. Provided additional time in the future, the usage of bigger datasets or numerous datasets may be incorporated. We may examine and evaluate the differences in accuracy across various datasets with the use of several different datasets. More production will result in greater understanding of how to effectively address the problem of media forgery. In this approach, it is possible to develop a more positive perspective on the issue.

References

[1] Gill, Sajid & Sheikh, Noor & Rajper, Samina & Abidin, Zain & Zaman, Noor & Ahmad, Muneer & Abdur Razzaq, Mirza & Alshamrani, Sultan & Malik, Yasir & Jaafar, Fehmi. (January 2021). Extended Forgery Detection Framework for COVID-19 Medical Data Using Convolutional Neural Network. DOI:10.32604/cmc.2021.016001. [online]. Available at: https://www.researchgate.net/publication/351392409_Extended_Forgery_Detection_Framework_for_COVID-19_Medical_Data_Using_Convolutional_Neural_Network

[2] S. Mascarenhas and M. Agarwal, (2021) "A comparison between VGG16, VGG19 and ResNet50 architecture frameworks for Image Classification". International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), 2021, pp. 96-99, doi: 10.1109/CENTCON52345.2021.9687944. [online]. Available at: https://ieeexplore.ieee.org/document/9687944

[3] Qingsheng Liu. (2020). "Random forest and watershed transformations for mapping quasi-circular vegetation patch using fused multispectral CBERS-04 images". IOP Conf. Ser.: Mater. Sci. Eng. 768 062008. [online]. Available at: https://iopscience.iop.org/article/10.1088/1757-899X/768/6/062008

[4] Farah Deeba, She Kun, Fayaz Ali Dharejo, Hameer Langah, and Hira Memon. (2nd February 2020). "Digital Watermarking Using Deep Neural Network". [online]. Available at: https://pdfs.semanticscholar.org/8d7e/d4d0f080cbfbbf10227f48a13bd233a8a651.pdf

[5] Ehsan Nowroozia, Ali Dehghantanhab, Reza M. Parizic, Kim-Kwang Raymond Chood. (19th October 2020). "A Survey of Machine Learning Techniques in Adversarial Image Forensics". arXiv:2010.09680v1 [cs.CR]. [online]. Available at: https://arxiv.org/pdf/2010.09680.pdf

[6] Daming Li, Lianbing Deng, Brij Bhooshan Gupta, Haoxiang Wang, Chang Choi. (2019). “A novel CNN based security guaranteed image watermarking generation scenario for smart city applications". ISSN 0020-0255. [online]. Available at: https://www.sciencedirect.com/science/article/pii/S0020025518301452

[7] Arpita Halder, Bimal Datta. (19th July 2021). "COVID-19 detection from lung CT-scan images using transfer learning approach". IOP publishing Mach. Learn.: Sci. Technol. 2 045013. [online]. Available at: https://iopscience.iop.org/article/10.1088/2632-2153/abf22c

[8] Samir Elmuogya, Noha A. Hikalb, Esraa Hassanc. (2021). "An efficient technique for CT scan images classification of COVID-19". DOI:10.3233/JIFS-201985. [online]. Available at: https://content.iospress.com/download/journal-of-intelligent-and-fuzzy-systems/ifs201985?id=journal-of-intelligent-and-fuzzy-systems%2Fifs201985

[9] Vinay Arora, Eddie Yin-Kwee Ng, Rohan Singh Leekha, Medhavi Darshan, Arshdeep Singh. (2021). "Transfer learning-based approach for detecting COVID-19 ailment in lung CT scan". ISSN 0010-4825. [online]. Available at: https://www.sciencedirect.com/science/article/pii/S0010482521003693?via%3Dihub

[10] S.Prayla Shyry, Saranya Meka, Mahitha Moganti, (July 2019). "Digital Image Forgery Detection." ISSN: 2277-3878, Volume-8, Issue-2S3. [online]. Available at: https://www.ijrte.org/wp-content/uploads/papers/v8i2S3/B11210782S319.pdf

[11] Shwetha B Basavarajappa, S. V. Sathyanarayana. (December 2016). "Digital image forgery detection techniques: a survey." DOI:10.19101/TIS.2017.25003. Available at: https://www.researchgate.net/publication/311957994_Digital_image_forgery_detection_techniques_a_survey

[12] Shoshanna solomon, (4th April 2019). "Israeli researchers show medical scans vulnerable to fake tumors". [Online]. Available at: https://www.timesofisrael.com/israeli-researchers-show-medical-scans-vulnerable-to-fake-tumors/

[13] Nina Danielsen. (22 November 2019). "Simple Image Classification with ResNet-50". [online]. Available at: https://medium.com/@nina95dan/simple-image-classification-with-resnet-50-334366e7311a#:~:text=ResNet-50%20is%20a%20pretrained,applied%20to%20analyzing%20visual%20imagery

[14] Gustavo Santos. (4 October 2021). "Understanding Random Forest's hyperparameters with images". [online]. Available at: https://towardsdatascience.com/understanding-random-forests-hyperparameters-with-images-9b53fce32cb3

[15] Paperswithcode. (2021). "Rectified Adam stochastic optimizer". [Online]. Available at: https://paperswithcode.com/method/radam

[16] Mirsky, Yisroel and Mahler, Tom and Shelef, Ilan and Elovici, Yuval. (2019). "CT-GAN: Malicious tampering of 3D medical imagery using deep learning/Dataset of lung cancer Diagnosis". [Online]. Available at: https://www.kaggle.com/datasets/ymirsky/medical-deepfakes-lung-cancer

[17] Priya Pedamkar. (2020). " Machine Learning Architecture". [Online]. Available at: https://www.educba.com/machine-learning-architecture/

[18] Christiaan Beek. (11 March 2018). "McAfee Researchers Find Poor Security Exposes Medical Data to Cybercriminals". [online]. Available at: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/