Title of The Project: Medical DeepFake Prediction Using Deep Learning

(False Cancerous Image Detction)

Supervisor Name and Designation: Dr. Mohammad Monirujjaman Khan
Department Name and University Name: ECE NSU

Group Member Name & ID:

1. Gulam Sarwar (1821700042)
2. Rafid Ahmed (1831395642)

Submission Date: 13 - November - 202

Description of the problem being solved

The name "Deepfake" is derived from the underlying artificial intelligence (AI) technique known as "deep learning." Face swapping in video and digital content is done using deep learning algorithms, which, when given enormous amounts of data, educate themselves how to solve issues. As deep learning/AI improves at a rapid pace, It is critical to comprehend the security implications. Attackers can no longer be presumed to have restricted capabilities.

A deep learning AI algorithm called the autoencoder is tasked with watching the image to learn how the person appears from various perspectives and in various environments, and then mapping that person onto the person in the target video by identifying common features.
Convolutional Neural Network or CNN , another kind of machine learning, is incorporated into the process. GANs identify and fix any deepfake problems over the course of several rounds, making it more challenging for deepfake detectors to identify them.

The top cause of death in the world is cancer. The problems of combating cancer are being faced by both researchers and physicians. 96,480 fatalities from skin cancer, 142,670 from lung cancer, 42,260 from breast cancer, 31,620 from prostate cancer, and 17,760 from brain cancer are anticipated in 2019, according to the American Cancer Society (American Cancer Society, new cancer release report 2019). The best chance of saving many lives is through early identification of cancer. For these kinds of cancer diagnoses, visual inspection and manual procedures are frequently employed. It takes a lot of effort and is highly prone to mistakes to manually evaluate medical photos.

Deep generative networks have reinforced the need for caution when consuming various modalities of digital information in recent years. One method of creating deepfakes is to inject and remove fake reports from medical scans. Medical deepfakes can cause serious resource drains on hospitals or even fatalities if they go undetected. With a well-structured case study, this paper makes an effort to address the detection of such assaults.

Review of existing similar systems

Numerous assaults on clinics and hospitals in 2018 resulted in serious data breaches and disruptions to medical services. With access to medical records, a criminal can do far more than just demand a ransom or sell the information. In this research, we demonstrate how an attacker can modify or remove medical condition evidence from volumetric (3D) medical images using deep learning. This attack could be carried out by a perpetrator who wants to kill someone, sabotage research, perpetrate insurance fraud, engage in terrorism, or derail a political candidate. We put the assault into practice using a 3D conditional GAN and demonstrate how the CT-GAN framework may be automated. Despite the complexity of the human anatomy and the size of 3D medical imaging,Realistic results produced by CT-GAN can be executed in milliseconds. We concentrated on injecting and eliminating lung cancer from CT scans in order to assess the attack. We demonstrate how vulnerable to the attack three experienced radiologists and a cutting-edge deep learning AI are. We also investigate the attack surface of a contemporary radiology network and show one attack vector by using a covert penetration test to intercept and modify CT scans on a live hospital network.

Objective of The Project:

The objective of this system is developing a system which can detect fake cancer. The percentage of accuracy needs to be good enough to be acceptable. The system needs to be cost friendly as if so it can be widely used and as well as spread for distribution. So, people from poor countries can afford to use the system and medical institutions can widely use it upon need.

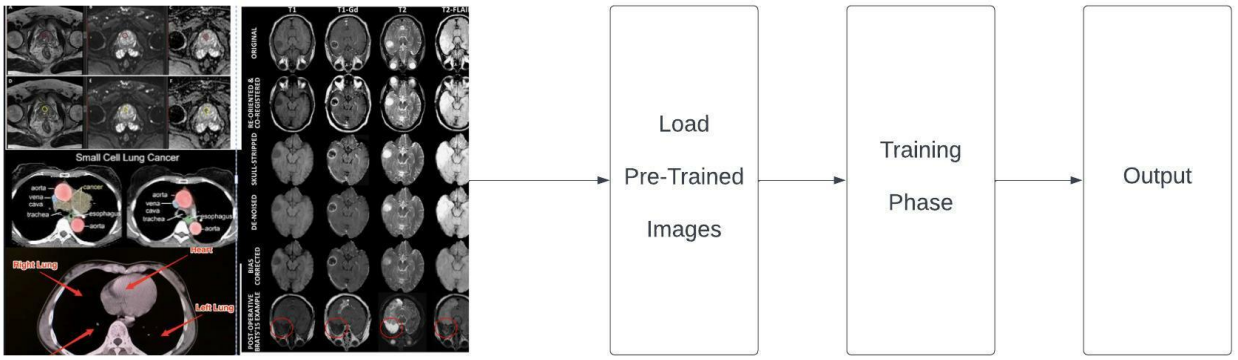
Feasibility Study Indicating Possible Solutions:

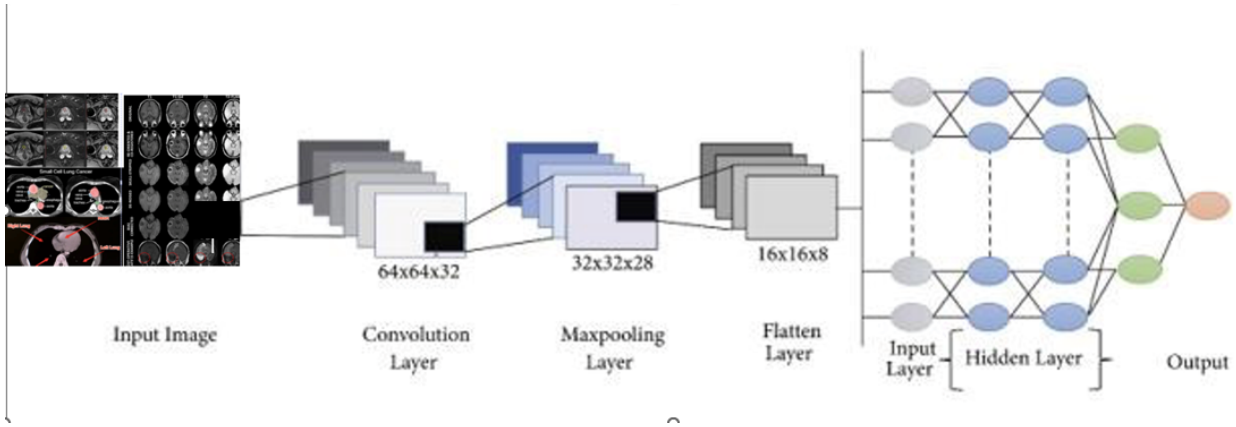
To develop our system, we will be using deep learning. Deep learning is a machine learning and artificial intelligence (AI) technique inspired by human learning. Data science, which covers statistics and predictive modeling, contains deep learning as a major component. Throughout developing our system, we will be using either KNN or CNN model. We will be applying VGG16 architecture in our model. Also, we will use deep pooling, Flatten, Dense, Fully connected layers etc. For performance analysis we will use confusion matrix such as true positive, true negative etc. For datasets we will be using kaggle. Our system will take data as input and then split, process, train the data and lastly provide a result with acceptable accuracy.

Solutions adopted and the reasons for that

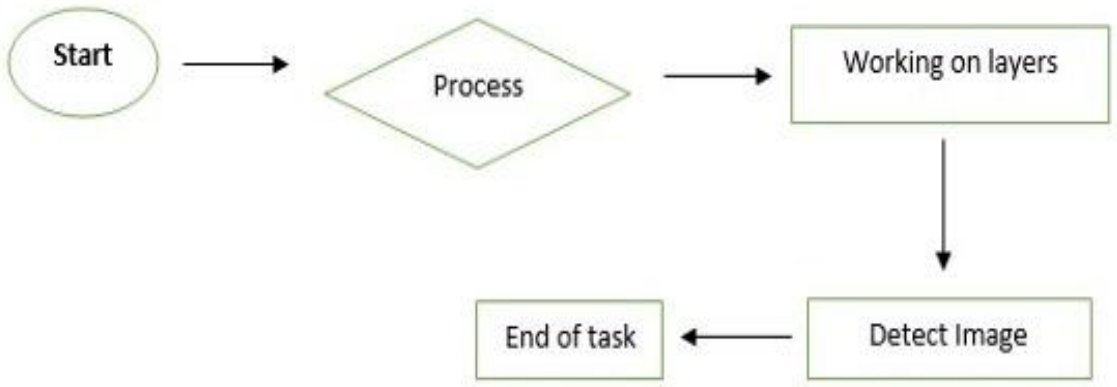
In recent years, numerous people have cried out for assistance while pretending to have cancer. To determine if they have cancer or not, we are employing deep learning technology.

Detailed diagrams for the complete system and all subsystems

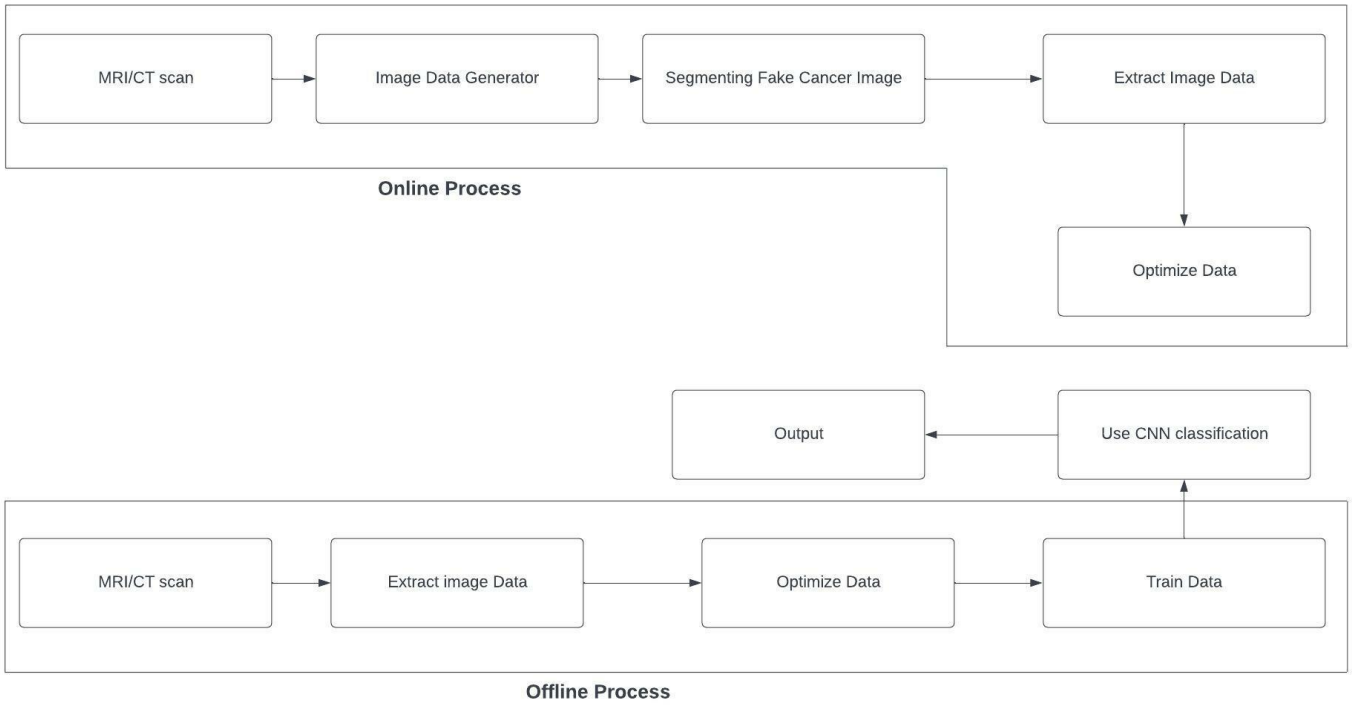




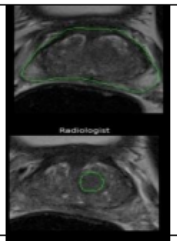
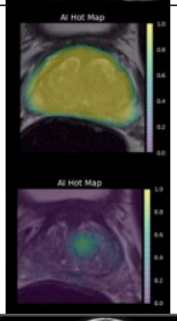
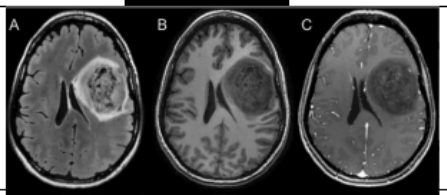
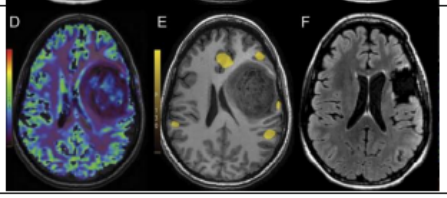
Diagrams drawn using MS Word or MS Visio showing flow chart for processing



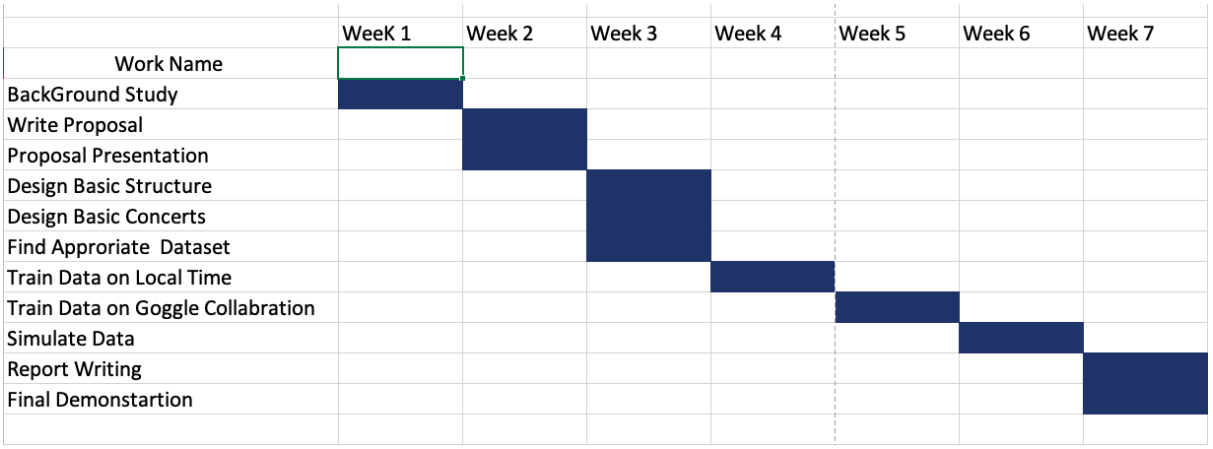
Figures and graphs showing inputs and outputs, as applicable



Tables showing input and output data, as applicable

Topic	Input	Output
Magnetic Resonance Imaging (MRI)		No
Magnetic Resonance Imaging (MRI)		Yes
Computerized Tomography (CT) Scan		No
Computerized Tomography (CT) Scan		Yes

MS Project charts including Gantt Charts showing the expected timeline of progress



Working Steps (Work plan):

A project work plan enables you to define a project's requirements, planning phases, objectives, and team members. This provides visibility to all parties involved, keeps project deliverables in one place, and keeps you on track to reach your objectives. There are some steps:

Background Study: The project background should provide information on why you want to carry out this project in this particular way. It must describe the existing situation and its difficulties, as well as the approach you intend to take to resolve them. These assumptions and explanations should be supported by reliable facts.

Proposal Writing: A project proposal is a written document that lays out everything stakeholders need to know about a project, including the schedule, budget, goals, and objectives. The facts of your project should be explained in your project proposal, and your idea should be sold so that stakeholders are interested in joining in the effort.

Present Proposal: The goal of the presentation is to give the evaluator an overview of your project, including both the product and the process. The talk is accompanied with project documents and a demonstration of the product (if any). It enables assessors to clear up any doubts they may have by, for example, asking questions on the spot.

Data Collection: Data collecting allows you to keep track of prior events so that we may look for recurrent trends using data analysis. You may create predictive models that search for trends and anticipate future changes based on those patterns. Because predictive models are only as strong as the data they're built on, good data collecting procedures are essential for creating high-performing models.

Train Data: Training data is the information used to teach an algorithm or machine learning model to predict the outcome you want it to. Test data is used to assess the performance of the algorithm you're using to train the machine, such as accuracy and efficiency.

Develop the System: The process of defining, creating, testing, and implementing a new software application or program is known as systems development. Internal development of custom systems could be part of it.

Testing: Software testing is the process of examining and verifying that a software product or application does what it is supposed to do. Testing has many benefits, including preventing flaws, saving development costs, and improving performance.

Report Writing: The final step is to write a project report. A project report is simply a document that comprises details about the project's overall status as well as specific areas of its progress or performance.

Major Milestones:

We've been studying the depths of our system for the past few weeks, learning new ideas and different types of algorithms. We finished our first report and gave our presentation this week.