Medical DeepFake Prediction Using Deep Learning (False Cancerous Image Detection)

Submitted By:

NAME	ID
Gulam Sarwar	1821700042
Rafid Ahmed	1831395642

Supervisor:

Dr. Mohammad Monirujjaman Khan
Associate Professor
Department of ECE

Submission Date: 28th November, 2022

1. Background Study of The Research Topic

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 on 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 Networks or CNN, another kind of machine learning, is incorporated into the process. GANs identify and fix any deepfake problems throughout 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 in manually evaluating 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 in 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.

2. Description of The Problem Being Solved (Problem Statement)

One of the most deadly and well-known diseases is cancer. It affects not only the victims but as well as their families, friends, and society as a whole. There have been some new advances that try to predict the severity of lung cancer in an individual by analysing certain parameters collected from their medical data, thanks to significant advancements in Artificial Intelligence and Deep Learning. This study analyses the different frameworks (CNNs, GAN, etc.) and algorithms utilized in some of the most current and notable research on the subject of predicting medical deepfake. Aside from the comparative analysis, this research also presents a few ways that look into certain non-traditional factors that could be useful in the task of detecting and predicting deepfake from MRI and CT scan data.

3. 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 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.

4. Objective of The Project

The objective of this system is to develop a system that can detect fake lung cancer. The percentage of accuracy needs to be good enough to be acceptable. The system needs to be cost-friendly 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.

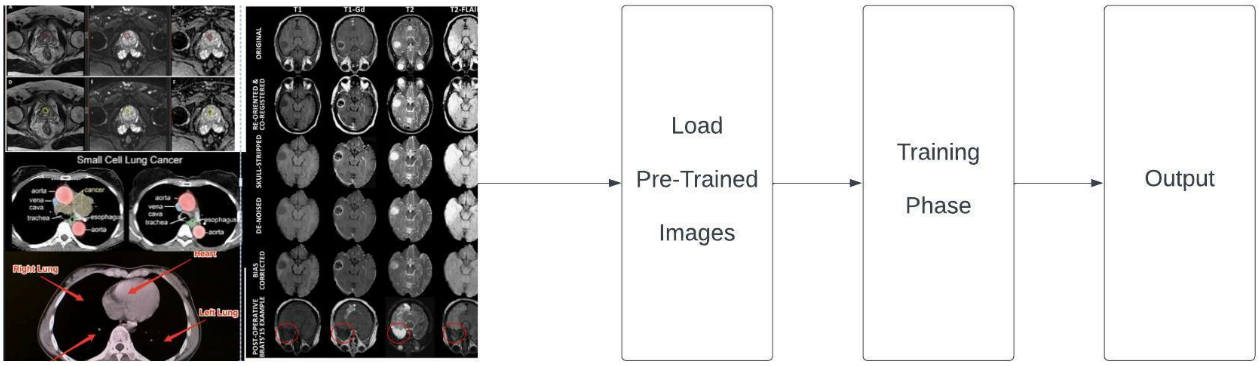
5. Feasibility Study Indicating Possible Solutions

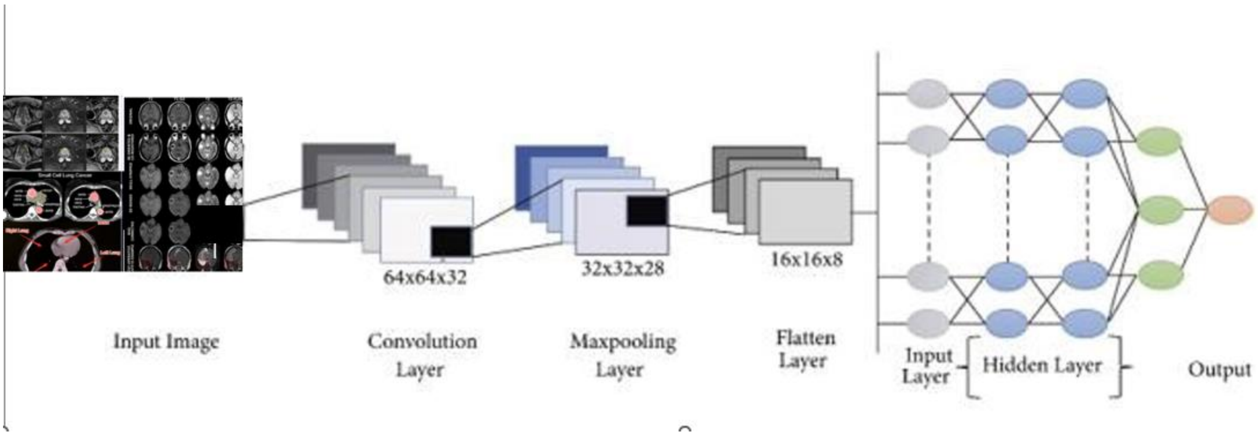
To develop our system, we will be using deep learning. Deep learning is a machine learning and artificial intelligence (AI) technique inspired by human learning. Data science, which covers statistics and predictive modelling, contains deep learning as a major component. Throughout developing our system, we will be using either KNN or CNN model. We will be applying VGG16 architecture in our model. Also, we will use deep pooling, flattened, Dense, fully connected layers, etc. For performance analysis, we will use a 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.

6. Output of The Project or Expected Results of The Project

We're going to run a variety of models through their paces one by one. Because we want to create a system that can identify lung cancer, we'll require Magnetic Resonance Imaging (MRI) and Computerized Tomography (CT) scans of lung cancer patients. We want to see if the data we've gathered and the data that has lately been submitted match, and if they do, we want to respond. We aim for an accuracy percentage between 94 and 98 percent. To ensure that the training data was unaffected, we would attempt to select a dataset containing clear pictures.

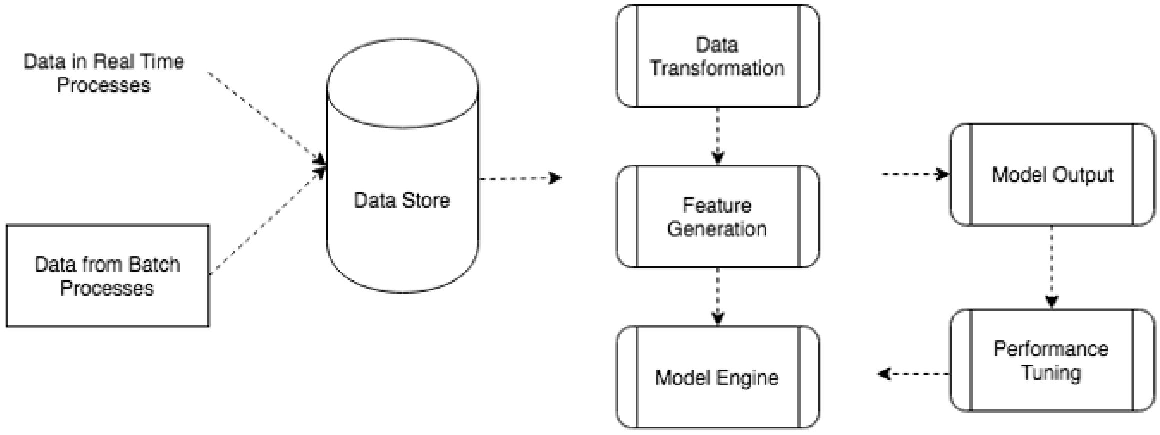
7. Detailed Diagrams For The Complete System and All Subsystems





8. Explanation of the functioning of the complete system, and all subsystems

9. Diagrams Drawn using software showing the layout of the systems



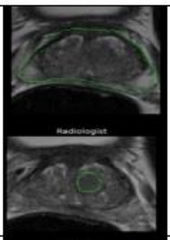
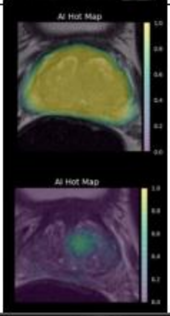
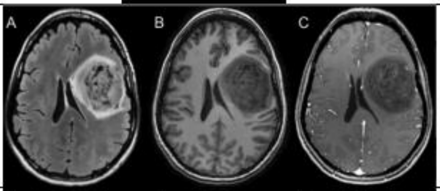
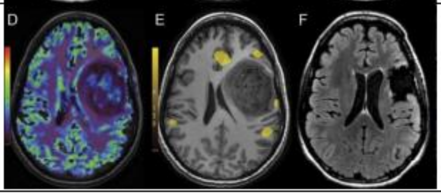
10. Diagrams drawn using MS Word or MS Visio showing flow chart for processing

Not Applicable.

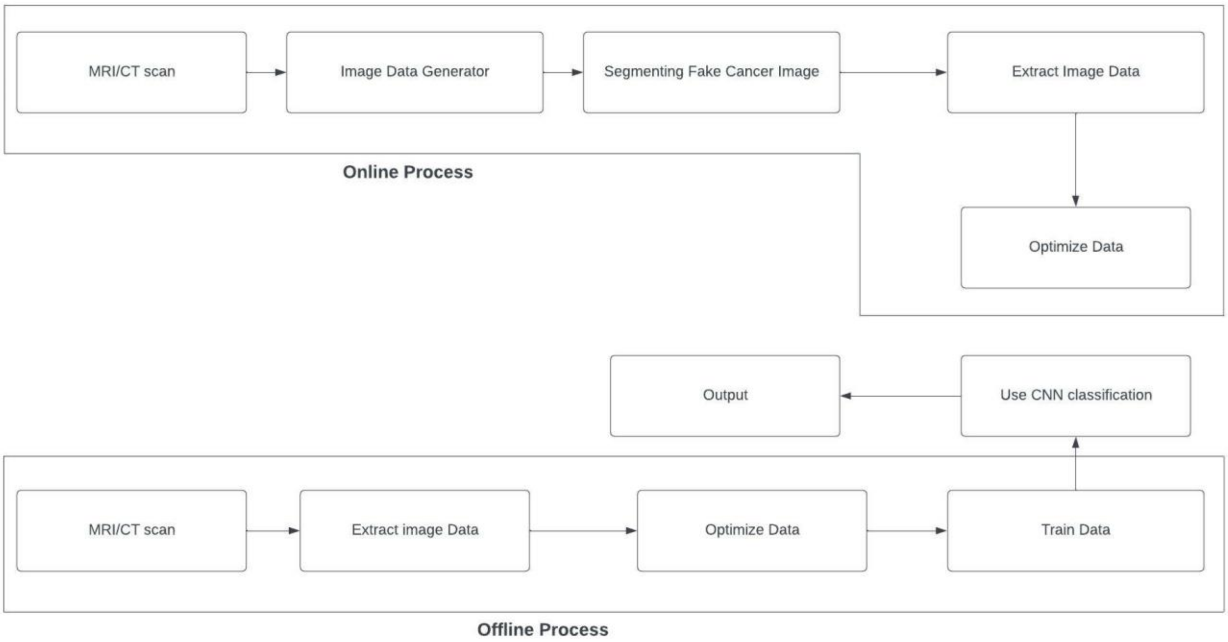
11. Graphs drawn using MS Excel

Not Applicable.

12. Figures and graphs showing inputs and outputs, as applicable

Topic	Input	Output
Magnetic Resonance Imaging (MRI)		No
Magnetic Resonance Imaging (MRI)	 AI Hot Map 1.0 0.8 0.6 0.4 0.2 0.0 AI Hot Map 1.0 0.8 0.6 0.4 0.2 0.0	Yes
Computerized Tomography (CT) Scan		No
Computerized Tomography (CT) Scan		Yes

13. Tables Showing Input and Output Data



14. 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 by 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.

15. Major Milestones

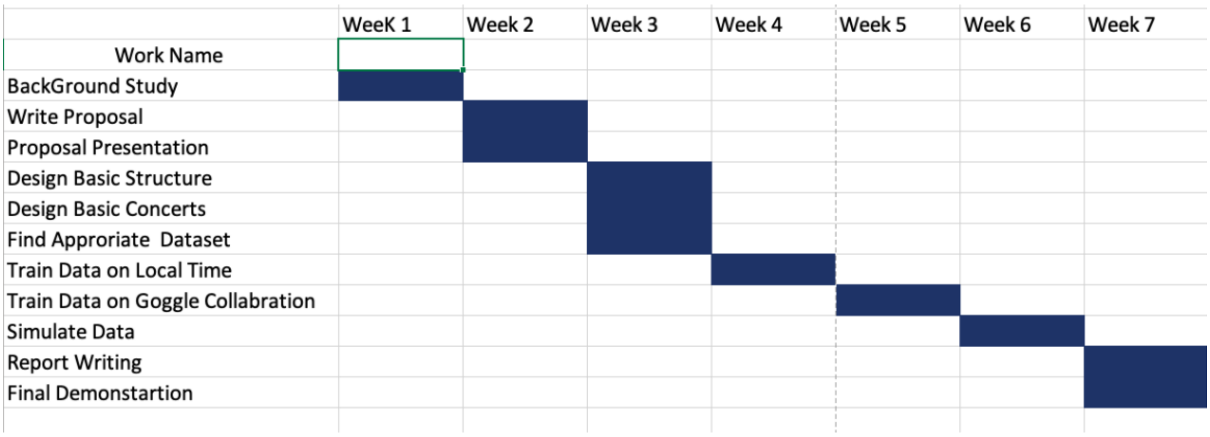
- Background Study
- System Design Requirements
- System Design Analysis
- Dataset Collection
- Training
- Testing
- Predict
- Implementation

16. Bill of Materials Required to Build the Software System, and the Approximate Cost

We need an extended graphics card RTX 4090:	242,000 Tk
Need additional ram 16 GB:	22,000 Tk

Google collaboration access to unlock new possibilities for **10 months**:	9,900 Tk
Total Cost:	**273,900 Tk**

17.Grantt Charts Showing the Expected Timeline of Progress & Milestones



	WeeK 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7
Work Name							
BackGround Study	■						
Write Proposal		■					
Proposal Presentation		■					
Design Basic Structure			■				
Design Basic Concerts			■				
Find Approriate Dataset			■				
Train Data on Local Time				■			
Train Data on Goggle Collabration					■		
Simulate Data						■	
Report Writing							■
Final Demonstartion							■

18. Required software tools

Two software applications will be used. The first is named Google Colaboratory, and the second is called Jupyter Notebook. Python is going to be the programming language of choice. The model training and validation will be carried out using Anaconda Navigator and Jupyter Notebook.

The Google Colaboratory, or "Colab" for short, is a product from Google Research. Collab is a Python editor for the web that allows anyone to develop and run Python programs. Machine learning, data analysis, and education are all areas where it comes in handy. Professors can use Google Collaboration Applications to give new communication and collaboration options to their students. Several of the many online applications geared toward efficiency and collaboration (Thompson, 2008) are appropriate for higher education, allowing undergraduates to learn how to use cloud computing software and prepare for the workforce.
Jupyter Notebook is an online tool that allows you to create and share documents with code, visuals, and text. It's useful for data science, statistical modeling, machine learning, and a variety of other tasks. We want to use this because Jupyter Notebook can connect to a variety of kernels, allowing you to program in a variety of languages. A Jupyter kernel is a program that handles a variety of requests (code execution, code completions, and inspection) and responds.

Python is a dynamically semantic, interpreted, object-oriented high-level programming language. Its high-level built-in data structures, together with dynamic typing and dynamic binding, make it perfect for Rapid Application Development and as a scripting or glue language for connecting existing components. Python's concise, easy-to-learn syntax prioritizes readability, which lowers software maintenance costs. Modules and packages are supported by Python, which fosters program modularity and code reuse

19. Target Population

The people of Bangladesh are our target audience. People in Bangladesh are largely unaware of the illness. Through our efforts, we will be able to assist the citizens of our nation in comprehending what it is and how it affects them. If lung cancer can be detected in a short period and at an early stage in a person's body, our doctors will be able to treat the patient more effectively. As a result, the number of people diagnosed with lung cancer will steadily decline. As a result of our research, we anticipate being able to identify lung cancer at an early stage.

20. What makes the solution an 'Innovation'

Until now, every paper regarding that topic that we've read has had an accuracy rate of less than 90%. However, we are working with an extremely efficient dataset in our scenario. As a result, we'll aim to create a system that can help people. We'll use multiple models in this case. This will be a milestone for our project if we can get the highest accuracy while using multiple models. As a result, we might conclude that our solution is innovative.

21. Sustainability of the project

No adjustments will be required in the future for any of our models. Therefore, our project is sustainable. Since this is a software-based project, it will automatically update if the software changes in the future, unlike hardware projects.

As a result, we do not need to be concerned about the project's long-term viability.

22. Benefit from the project

We shall aim to anticipate lung cancer at an early stage in this project. People have a higher chance of benefiting from therapy if they are diagnosed with lung cancer early. In a couple of minutes, a prediction can be made. This reduces the time it takes to get a diagnosis, which enhances research while also potentially providing medical advantages. Receiving an early lung cancer diagnosis might help alleviate concerns regarding the cause of people's symptoms. They and their families may also make the most of their time together by making use of services and support programs. The likelihood of misdiagnosis due to human mistakes is also reduced when the accuracy rate is considered. Moreover, the likelihood of misdiagnosis due to a human mistake is also reduced when the accuracy rate is considered. As a result, the user will profit in terms of both time and accuracy.

23. Risk Factor

Medical forecasts are constantly at risk of being incorrect, which might lead to a misdiagnosis. We have no risks except that after implementing the algorithms, we may yield less accuracy. However, by working with huge datasets and pre-trained models to improve the accuracy rate, this will be lowered. As a result, the risk will be managed.

24. Unprivileged Women will benefit

Affirmative, our project will assist underprivileged individuals. Because many individuals in our nation are unable to easily get to the hospital. At home, they will be able to use a computer to determine the nature of their illness.

25. Disabled will benefit

Of course, our project will assist handicapped individuals. Because many individuals in our nation are handicapped and unable to easily get to the hospital. They will be able to identify their ailment using a computer while at home in this situation.

26. Impact on Environment, Social, Economic, Design

We can accomplish a lot of good things with this effort. With early detection, we can give patients new hope for a better life. Early treatment may be able to save his life and riches. It will be beneficial to have a social life. Our project has no negative environmental consequences. It will not hurt the environment in any way; It will be environmentally friendly.

28. Individual responsibilities for this project

Topic	Name
Find Appropriate Dataset	Rafid Ahmed Gulam Sarwar
Pre Process Image	Rafid Ahmed Gulam Sarwar
Train Data in Google Collab	Gulam Sarwar Rafid Ahmed
Implement Custom CNN model	Gulam Sarwar Rafid Ahmed

Test Model	Rafid Ahmed Gulam Sarwar

We have an equal contribution on this tasks.

29. Income Generation

The model can be utilized by hospitals and medical workers to improve their diagnosis of depression patients using the techniques used, such as trained models and algorithms. Human errors are less likely when the model does all of the forecastings. This might be an intriguing concept that encourages users to employ prediction algorithms in this way. It can be marketed or licensed to hospitals, or even offered to the general public if the market is ready to accept it.

30. Project Scalability

Of course, the project may be scaled up. Right now, we're just getting started with the models for our project. We can build apps connected to it in the future and increase our work. We may also use a larger dataset to broaden our scope of study. We can implement five algorithms and increase our work in the future because we are just implementing two algorithms today.

31. Existing Research Publications

In 2018, clinics and hospitals were hit with numerous attacks leading to significant data breaches and interruptions in medical services. An attacker with access to medical records can do much more than hold the data for ransom or sell it on the black market.

In this paper, we show how an attacker can use deep learning to add or remove evidence of medical conditions from volumetric (3D) medical scans. An attacker may perform this action to stop a political candidate, sabotage research, commit insurance fraud, perform an act of terrorism, or even commit murder. We implement the attack using a 3D conditional GAN and show how the framework (CT-GAN) can be automated. Although the body is complex and 3D medical scans are very large, CT-GAN achieves realistic results which can be executed in milliseconds.

To evaluate the attack, we focused on injecting and removing lung cancer from CT scans. We show how three expert radiologists and a state-of-the-art deep learning AI are highly susceptible to the attack. We also explore the attack surface of a modern radiology network and demonstrate one attack v ector: we intercepted and manipulated CT scans in an active hospital network with a covert penetration test.[11]

32. Conclusion

Deepfakes have begun to erode the trust of people in media content as seeing them is no longer commensurate with believing in them. They could cause distress and negative effects to those targeted, heighten disinformation and hate speech, and even could stimulate political tension, inflame the public, violence, or war. This is especially critical nowadays as the technologies for creating deepfakes are increasingly approachable and social media platforms can spread those fake contents quickly. This survey provides a timely overview of deepfake creation and detection methods and presents a broad discussion on challenges, potential trends, and future directions in this area. This study therefore will be valuable for the artificial intelligence research community to develop effective methods for tackling deepfakes.

33. Bibliography

[1] Aldahiri, Amani, et al. ‘Trends in Using IoT with Machine Learning in Health Prediction System’. Forecasting, vol. 3, no. 1, Mar. 2021, pp. 181–206. www.mdpi.com, https://doi.org/10.3390/forecast3010012.

[2] Alheeti, Khattab M. Ali, et al. ‘Intelligent Deep Detection Method for Malicious Tampering of Cancer Imagery’. 2022 7th International Conference on Data Science and Machine Learning Applications (CDMA), 2022, pp. 25–28. IEEE Xplore, https://doi.org/10.1109/CDMA54072.2022.00010.

[3] CT-GAN: Malicious Tampering of 3D Medical Imagery Using Deep Learning | USENIX. https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky. Accessed 2 Dec. 2022.

[4] Hicks, Steven A., et al. ‘Explaining Deep Neural Networks for Knowledge Discovery in Electrocardiogram Analysis’. Scientific Reports, vol. 11, no. 1, May 2021, p. 10949. www.nature.com, https://doi.org/10.1038/s41598-021-90285-5.

[5] Kapadia, Shashank. ‘6 Steps towards a Successful Machine Learning Project’. Medium, 3 Aug.2022,https://towardsdatascience.com/6-steps-towards-a-successful-machine-learning-project-3a56f59e2747.

[6] Mangaokar, Neal, et al. ‘Jekyll: Attacking Medical Image Diagnostics Using Deep Generative Models’. 2020 IEEE European Symposium on Security and Privacy (EuroS&P), 2020, pp. 139–57. IEEE Xplore, https://doi.org/10.1109/EuroSP48549.2020.00017.

[7]S. Ren, K. He, R. Girshick and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks", Proc. Adv. Neural Inf. Process. Syst., pp. 91-99, 2015.

[8] Mirsky, Yisroel. ‘Discussion Paper: The Integrity of Medical AI’. Proceedings of the 1st Workshop on Security Implications of Deepfakes and Cheapfakes, Association for Computing Machinery, 2022, pp. 31–33. ACM Digital Library, https://doi.org/10.1145/3494109.3527191.

[9] Sharafudeen, Misaj, and S. S. Vinod Chandra. ‘Medical Deepfake Detection Using 3-Dimensional Neural Learning’. Artificial Neural Networks in Pattern Recognition, edited by Neamat El Gayar et al., Springer International Publishing, 2023, pp. 169–80. Springer Link, https://doi.org/10.1007/978-3-031-20650-4_14.

[10] ‘Medical Deepfake Detection Using 3-Dimensional Neural Learning’. Artificial Neural Networks in Pattern Recognition, edited by Neamat El Gayar et al., Springer International Publishing, 2023, pp. 169–80. Springer Link, https://doi.org/10.1007/978-3-031-20650-4_14.

[11] Kim, D.W., Lee, S., Kwon, S. et al. Deep learning-based survival prediction of oral cancer patients. Sci Rep 9, 6994 (2019). https://doi.org/10.1038/s41598-019-43372-7

[12] Alabi, R. O., Almangush, A., Elmusrati, M., & Mäkitie, A. A. (2022). Deep Machine Learning for Oral Cancer: From Precise Diagnosis to Precision Medicine. Frontiers in oral health, 2, 794248. https://doi.org/10.3389/froh.2021.794248

[13] Pandia Rajan Jeyaraj, Bijaya Ketan Panigrahi & Edward Rajan Samuel Nadar (2020) Classifier Feature Fusion Using Deep Learning Model for Non-Invasive Detection of Oral Cancer from Hyperspectral Image, IETE Journal of Research, DOI: 10.1080/03772063.2020.1786471

[14] S. Ren, K. He, R. Girshick and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks", Proc. Adv. Neural Inf. Process. Syst., pp. 91-99, 2015.

[15] K. He, G. Gkioxari, P. Dollár and R. Girshick, "Mask R-CNN", Proc. IEEE Int. Conf. Comput. Vis., pp. 2961-2969, Oct. 2017.

[16] R. Dharani and S. Revathy 2021 J. Phys.: Conf. Ser. 1911 012006 [17] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li and L. Fei-Fei, "ImageNet: A large-scale hierarchical image database", Proc. IEEE Conf. Comput. Vis. Pattern Recognit., pp. 248-255, Jun. 2009.

[18] Kim, K., Li, S. & Cha, I. Nomogram for predicting survival for oral squamous cell carcinoma. Genomics Inform. 8, 212–218 (2010).

[19] Wang, S. J. et al. An oral cavity carcinoma nomogram to predict benefit of adjuvant radiotherapy. JAMA Otolaryngol. - Head Neck Surg. 139, 554–559 (2013).

[20] Saintigny, P. et al. Gene expression profiling predicts the development of oral cancer. Cancer Prev. Res. 4, 218–229 (2011).

[21] Chang, S.-W., Abdul-Kareem, S., Merican, A. & Zain, R. Oral cancer prognosis based on clinicopathologic and genomic markers using a hybrid of feature selection and machine learning methods. BMC Bioinformatics 14, 170 (2013).

[22] Missinglink,(2019) https://missinglink.ai/guides/neural-network-concepts/convolutiona;

[23] Ü. H. Ayan, "Diagnosis of pneumonia from chest X-ray images using deep learning," in Proceedings of the 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), pp. 1–5, Istanbul, Turkey, April 2019.

[24] J. Brownlee, Difference between a Batch and an Epoch in a Neural Network, Machine Learning Mastery, San Francisco, CL, USA, 2021, https://machinelearningmastery.com/difference-between-abatch-and-an-epoch/.

[25] Towardsdatascience, "The most intuitive and eauest guide for CNN," 2020, https://towardsdatascience.com/the-most-intuitive-and-easiest-guide-forconvolutionalneuralnetwork3607be47480#:%7E:text=Flattening%20is%20converting%20 the%20dat a, called%20a%20fully%2Dconnected%20layer.

[26] O. A. Hamid, L. Deng, and D. Yu, "Exploring convolutional neural network structures and optimization techniques for speech recognition," ISCA, vol. 11, pp. 73–75, 2013.

[27] J. Brownlee, "A gentle introduction to pooling layers for convolutional neural networks," Machine Learning Mastery, 2021. [28] J. Jeong, "The Most Intuitive and Easiest Guide for CNN," Medium, 2021.View at: Google Scholar

[29] S. Saha, "A Comprehensive Guide to Convolutional Neural Networks—theELI5 Way," Medium, 2021.View at: Google Scholar

[30] Tanriver G, Soluk Tekkesin M, Ergen O. Automated Detection and Classification of Oral Lesions Using Deep Learning to Detect Oral Potentially Malignant Disorders. Cancers (Basel). 2021 Jun 2;13(11):2766. doi: 10.3390/cancers13112766. PMID: 34199471; PMCID: PMC8199603.

[31] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and C. L. Chieh, "MobileNetV2: inverted residuals and linear bottlenecks," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 4510–4520, 2018.View at: Publisher Site | Google Scholar

[32] A. G. Howard, M. Zhu, B. Chen et al., "MobileNets: Efficient Convolutional Neural Networks for mobile Vision Applications," 2017.

[33]"GoogleColab".2022.Research.Google.Com.https://research.google.com/colaboratory/faq .html.

[34]Edwards, Jennifer T., and Credence Baker. "A case study: Google collaboration applications as online course teaching tools." MERLOT Journal of Online Learning and Teaching 6, no. 4 (2010): 828-838

[35] "Why You Should Be Using A Jupyter Notebook - Elucidata". 2022. Elucidata. https://elucidata.io/why-you-should-be-using-a-jupyter-notebook