Medicon Medical Sciences
Volume 6 Issue 3 March 2024
Article Type: Research Article
ISSN: 2972-2721

DeepFake Technology for Breast Cancer Dataset Generation Using Autoencoders and Deep Neural Networks

Suzan Anwar[1]*, Shereen Abdullah[2], Dalya Ali[3], Mardin Anwer[3] and Daniah Al-Nadawi[4]

[1]*Philander Smith University, LittleRock, Arkansas, USA*

[2]*Erbil Polytechnic University, Erbil, Iraq*

[3]*Salahaddin University, Erbil, Iraq*

[4]*Medical University of Lublin, Lublin, Poland*

***Corresponding Author:** Suzan Anwar, Philander Smith University, LittleRock, Arkansas, USA.

Received: February 20, 2024; **Published:** March 07, 2024

Abstract

In the emerging field of radiogenomics, the primary challenge is the high cost of genetic testing, which restricts access to large, paired datasets of imaging and genetic information. Such datasets are essential for the effective training of machine learning algorithms in radiogenomic analyses. This research aims to bridge the gap between gene expression in tumors and their morphological representation in MRI scans of breast cancer patients. In this work an advanced autoencoder for processing gene expression data, and the derived weights from this autoencoder utilized were then employed to initialize a supervised Deep Neural Network (DNN). This network extracted distinct morphological markers from each MRI scan. This study introduces an innovative approach that utilizes deepfake technology, employing dual Generative Adversarial Networks (GANs) to generate synthetic imaging data from a radiogenomic dataset. This synthetic data, nearly indistinguishable from real data, is produced using a supervised neural network and is aimed at enhancing breast cancer diagnostics. Notably, the proposed neural network, when enhanced with an autoencoder and dropout techniques, demonstrated superior predictive accuracy over linear regression models. Specifically, it reduced errors by an average of 1.8% in mean absolute percent error. These findings underscore that the images generated by the proposed model are virtually indistinguishable from authentic images and exhibit high reliability in applications through the PyTorch framework. The results of this study underscore the potential of the proposed methodology to significantly contribute to advancements in breast cancer diagnostics.

Keyword: Generative Adversarial Networks (GANs); Autoencoder; Radiogenomic; DeepFake; Supervised Deep Neural Network DNN

Introduction

Radiogenomics is an evolving discipline at the intersection of genomics and medical imaging, with a particular focus on cancer research. This field posits that the intrinsic biological variability within tumors is reflected in observable features in magnetic resonance (MR) images. As an emerging and valuable discipline, radiogenomics offers critical insights into disease mechanisms, predicts patient survival, and forecasts responses to treatments. Despite its potential, current radiogenomic techniques face significant limitations. They tend to focus either on genomic or imaging data, often overlooking the intricate relationship between genetic variations and their manifestations in human tissues and organs. This narrow focus results in a fragmented understanding of cancer, impeding the

development of comprehensive diagnostic and treatment strategies. Furthermore, the prohibitive cost of genetic testing limits access to large, paired datasets, essential for training effective machine learning models in radiogenomic analyses. Addressing these challenges, this study introduces a novel approach that leverages the power of Generative Adversarial Networks (GANs) and deep learning technologies. By fusing large-scale synthetic genomic data with existing realistic imaging data, the aim in this work is to revolutionize cancer diagnostics. The proposed methodology overcomes the current data limitations by generating synthetic imaging data that is nearly indistinguishable from genuine data. This advancement is pivotal in understanding the complex relationship between genetic makeup and its phenotypic expressions in cancer.

The application of deepfake technology in radiogenomics represents a significant leap forward. The proposed approach not only provides a cost-effective alternative to expensive genetic testing but also enriches the dataset for training more sophisticated machine learning models. This, in turn, promises to enhance the accuracy of cancer diagnostics, offering a more holistic view of the disease and paving the way for personalized treatment strategies.

Related Works

Radiogenomics is a discipline that melds genomic information with medical imaging data, with a particular focus on cancer research. Radiogenomic inquiries propose that the intrinsic biological variability within tumors manifests as observable features in magnetic resonance (MR) images. Radiogenomics is an emerging and valuable discipline, offering insights into the mechanisms of diseases, predicting patient survival, and forecasting responses to treatments. Current techniques for synthesizing data tend to focus on either genomic or imaging data, often overlooking the relationship between genetic variations and their manifestations in human tissues and organs. The fusion of large-scale synthetic genomic data with existing realistic imaging data promises to revolutionize areas like cancer diagnostics.

Gleaning molecular insights from formidable tumors, especially glioblastoma (GBM), typically requires invasive surgical measures. Such interventions become infeasible when tumors are in close proximity to pivotal brain areas. Regularly obtained medical imaging might pave the way for a non-intrusive method to decipher these molecular nuances [1-3]. Radiogenomic research posits that MR imaging can reveal biological heterogeneity in GBM [4], liver [5], lung [6], and breast [7] cancers. This suggests the potential of pinpointing image-driven features that echo the underlying tumor biology. Nevertheless, contemporary radiogenomic methodologies might not capture the intricate nonlinear dynamics inherent in gene expressions [8].

Oftentimes, due to the overwhelming dimensionality of radiogenomic datasets, studies restrict the breadth of features to evaluate, resorting to techniques like feature selection [4] or dimensionality reduction [3]. Neural networks, particularly multilayer perceptrons, champion nonlinear hierarchies, allowing the derivation of intricate features from expansive input data. The evolution of deep learning has spurred the advancement of deep neural networks that, courtesy of hardware enhancements and refined training protocols [9, 10], have consistently outstripped other methods across numerous machine learning challenges. In the biological domain, a myriad of deep learning techniques have recently been deployed, including convolutional neural networks [11], restricted Boltzmann machines, deep belief networks [12, 13], general deep neural networks [14], and autoencoders [15]. The rationale for their adoption hinges on their prowess to transform high-dimensional, foundational data into features pertinent for a specific predictive endeavor. In this investigation, harness deep neural network models to forge radiogenomic correlation maps that intertwine tumor gene expression profiles with their visual presentation in MR scans of GBM patients is used. Owing to their expansive representational capability, this work postulates that neural networks might unearth radiogenomic associations that are more telling than the extant pairwise or linear strategies [6-8].

The fields of radiomics and radiogenomics offer an all-encompassing perspective on tumor characteristics through imaging data. Radiomics involves the extraction of extensive quantitative information from medical images, which is then integrated with clinical and patient-specific data to build searchable, shared databases. Radiogenomics takes this a step further by merging genetic and ra-

diomic data [1-3]. Given that genetic testing is not accessible to everyone due to its expense, invasiveness, and time requirements, radiogenomics stands out as a viable alternative. This field is particularly useful for generating imaging surrogates connected to genetic markers, which can be employed to customize treatment plans and forecast treatment outcomes and early metastasis risks [4-9].

Limited research has explored the links between gene expression profiles and imaging features. This presents a significant gap, which this study aims to bridge. The proposed approach employs deepfake technology to generate either or both kinds of radiogenomic data. Deepfake technologies have garnered attention because of their ability to produce high-quality manipulated videos. These technologies are user-friendly and cater to a wide range of user expertise. Deep learning algorithms, including complex and high-dimensional data representation techniques, play a key role in their development. For instance, deep autoencoders have found extensive applications in image compression and dimensionality reduction [10-12]. Specifically, Style-GAN is a powerful deep learning algorithm employed for synthesizing highly realistic facial images, trained on the FFHQ dataset [13]. Subsequent improvements, like StyleGAN2, have further enhanced the realism of generated faces [14]. To advance deepfake detection methods, researchers are analyzing the unique traces left by different generative architectures in synthetic multimedia data. Zhang et al. [15] scrutinized artifacts introduced by GAN pipelines in the frequency domain, resulting in considerably improved classification outcomes. Guarnera et al. [16, 17] posited that each GAN architecture leaves a unique imprint on the images it generates, analogous to a creation fingerprint. Additionally, Cycle-GAN networks have been suggested for transforming unlicensed images, incorporating a cycle-consistency loss to align input and output images [18]. Various data-driven strategies aim to identify inconsistencies through categorization or anomaly detection rather than concentrating on a single artifact [19]. The Deep Convolutional Generative Adversarial Network (DCGAN) is a specialized form of GAN that utilizes certain architectural guidelines to stabilize the training process. It has shown noteworthy advancements in translating images from one form to another within the GAN architecture [20]. With the rise of Deep Neural Networks (DNNs) in cutting-edge AI, there has been a significant spike in the creation of manipulated or fraudulent multimedia content. Although multimedia alterations are not new, the ease with which human voices can be cloned and realistic human faces can be generated in images or videos has improved substantially. Among the techniques for generating such content, Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and Autoencoders (AEs) are the most commonly used. These methods are capable of overlaying facial images from one source onto a target image [21]. Sophisticated Long Short-Time Memory (LSTM) models have been employed to scrutinize the authenticity of various media files, including films and photos. Additionally, systems that are aware of temporal changes have been developed to automatically identify deepfake videos [22].

It's worth noting that deepfake videos found online differ substantially from those in academic datasets, primarily due to differences in content and the methods used for generation. These variations pose new obstacles for the detection of deepfake videos. Existing detection methods have also been criticized for their lackluster performance, sometimes attributed to racial biases [23]. Various technological solutions, such as automated deepfake identification systems, content verification, and preventive measures, are under review in this rapidly evolving field of security. While deepfakes can serve beneficial purposes, they also pose numerous risks. Strategies to counteract the negative impacts of deepfakes include legislative measures, corporate policies, educational programs, and the development of anti-deepfake technologies. Legal measures against malicious creators of deepfakes could be particularly effective, especially when applied internationally [24].

Current security measures in healthcare are insufficient, making the sector susceptible to attacks that could compromise the integrity and availability of medical data. As deep learning continues to advance, it is anticipated that more sophisticated algorithms will be developed for fraud detection. The Jekyll system is engineered to convert images from one condition to another while maintaining the individual's identity and could potentially be employed for removing diseases as well [25]. Synthetic Electrocardiograms (ECGs) have been generated using multiple publicly accessible, accurate ECGs. These synthetic ECGs pose no privacy concerns and can be shared for research purposes. When tested through the GE MUSE system using deepfake methods, 81.3% of the 150,000 synthetic ECGs were categorized as "normal". with the remainder classified as "non-normal". and none were deemed invalid [26]. In summary, this study delves into the role of deep learning in deepfake technology, the various methods of generating deepfakes, and multiple detection

strategies. Techniques for detecting fake images can be categorized into those using neural networks and those relying on handcrafted methods. Likewise, fake video detection focuses on both temporal and visual features. Temporal feature detection employs recurrent network models, while visual artifact detection scrutinizes individual video frames for irregularities [27]. Deepfakes have the potential to elevate current sources of disinformation and misinformation, becoming powerful tools in the hands of trolls, bots, conspiracy theorists, highly partisan media outlets, and foreign governments. In this sense, deepfakes could essentially serve as an upgraded version of fake news. On the positive side, deepfakes can also serve beneficial purposes, such as enabling realistic dubbing in foreign films [28] or bringing historical figures back to life for educational applications [29]. However, they can also be weaponized for harmful intents like creating fake adult videos to slander or extort someone [30], skewing electoral outcomes [31], inciting military conflicts [32], fomenting political or religious discord through fabricated speeches [33], destabilizing financial markets [34], or committing identity fraud [35]. It's evident that the negative uses of deepfakes substantially outweigh the positive ones. Recent advancements have not only enabled the creation of deepfakes with just a single image [26], but real-world instances of malicious use, such as an audio deepfake scamming a CEO out of $243,000, have also been reported [37]. Moreover, the risks extend to automated facial recognition systems (AFRS), which have been shown to have elevated error rates when faced with deepfakes and other face manipulations. For instance, studies have revealed that AFRS error rates can skyrocket to as high as 95% when confronted with deepfakes [38], with varying degrees of inaccuracy under other forms of manipulation [39-44]. Similarly, the accuracy of automated speaker verification systems can plummet from 98% to 40% under adversarial conditions [45]. In terms of detection, many methods exist for identifying deepfakes and face manipulations. However, most of these methods suffer from poor generalizability; their performance degrades significantly when exposed to new types of deepfakes or manipulations that were not part of the training data, as corroborated by multiple studies [46-50]. Previous research has largely treated deepfake detection as a reactive measure rather than a dynamic struggle between attackers and defenders [51-53]. This creates a noticeable disconnect between academic solutions and real- world needs, including issues like system robustness against adversarial attacks [54], decision explainability [55], and real-time mobile deepfake detection [56].

The exploration of diffusion models for the generation of realistic medical images, such as brain MRIs and chest X-rays, was conducted, demonstrating their utility in expanding medical datasets while ensuring patient privacy. The capability of these models to accurately depict oncological features within the generated images has been confirmed, paving the way for advancements in medical research and data protection [57]. The breast cancer immunohistochemical image generation challenge was initiated to advance research in generating IHC-stained images from H&E stained images, leveraging deep learning technologies to enhance treatment planning for invasive breast cancer. This challenge, providing paired H&E and IHC-stained images for model training, aimed to foster innovative solutions and discussions in the field, with a focus on analyzing the current limitations and predicting future developments in high-quality IHC image generation [58].

The field of deepfake generation and detection has garnered increasing attention in both the computer vision and machine learning communities. While existing review articles do cover the topic, they are generally academic in nature and often lack a practical perspective [59, 60]. They also tend to overlook the latest advancements in face manipulation methods and new deepfake generation and detection techniques [60, 61]. For this research, the deepfake techniques primarily leverage combined Generative Adversarial Networks (GANs), trained on realistic genomic and imaging data. Within the GAN architecture, the generator creates synthetic data, while the discriminator distinguishes between this synthetic data and real data. Feedback from the discriminator is used to refine the generator's output, in a cycle that continues until the discriminator can no longer differentiate between the two.

The contributions of this research are as follows:

1. Charting a pioneering path in radiogenomic analysis, harnessing the power of autoencoders and deep neural networks, and juxtaposed their prediction efficacy against that of linear regression.
2. Establishment of a foundational database for predictive targeting, thereby enabling researchers to better understand disease mechanisms.
3. Generation of genomic and imaging datasets for breast cancer, suitable for machine learning training.

4. Application of a deepfake methodology, harnessing robust deep learning algorithms to produce synthetic data nearly indistinguishable from real data, thereby enhancing breast cancer diagnostics.

Methodology

The primary focus of this study lies in the intersection of radiogenomics and deepfake technology. Radiogenomics combines genomic data with medical imaging, particularly in cancer research, to uncover correlations between genetic profiles and imaging features. The proposed approach leverages deepfake technology, a method known for producing high-quality manipulated images, to generate synthetic data in the radiogenomic domain.

Deepfake Technology in Radiogenomics

Deepfake technology, initially recognized for creating realistic videos and images, is now being repurposed for scientific applications. In this study, this technology is used to generate synthetic radiogenomic data. The goal is to produce data that closely mimics real-world scenarios, thus overcoming the limitations of data scarcity in this field. The parameters for the proposed neural networks were as follows:

- *Input Layer*: Matched to the dimensionality of the gene expression data.
- *Hidden Layers*: Three layers, each with 128, 64, and 32 neurons respectively.
- *Activation Function*: ReLU (Rectified Linear Unit) for hidden layers.
- *Output Layer*: Tailored to correlate with specific imaging features.
- *Learning Rate*: Initially set at 0.001, with an adaptive rate during training.
- *Loss Function*: Mean Squared Error (MSE), to measure the accuracy of the model.

Generative Adversarial Networks (GANs)

GANs, which consist of two parts is used in this work: a generator and a discriminator. The generator creates synthetic data, while the discriminator evaluates this data against real data. This process iteratively refines the synthetic data to a high degree of realism. For this research, the GANs are trained on realistic genomic and imaging data, facilitating the creation of synthetic data that is nearly indistinguishable from real data.

Data Generation and Evaluation

The generator part of the GAN architecture produces synthetic radiogenomic data. The discriminator then assesses the authenticity of this data against actual genomic and imaging datasets. Feedback from the discriminator is used to continuously improve the generator's output. This iterative process ensures that the synthetic data closely resembles the real data in both genomic and imaging aspects.

Deep Learning Algorithms

To enhance the generation process, advanced deep learning algorithms, such as autoencoders and Long Short- Term Memory (LSTM) models is used. These algorithms help in compressing and reducing the dimensionality of data, which is crucial for maintaining the integrity and relevance of the synthetic data.

The framework of this project includes three phases; in the first phase, data pre-processing method to prepare the selected dataset for the next phase is applied. In the second phase, harness deep neural network models to forge radiogenomic correlation maps that intertwine tumor gene expression profiles with their visual presentation in MR scans of breast cancer patients is employed. The third phase employs cutting-edge deep learning algorithms generating synthetic genetic and imaging data via GANs. Utilizing Python and scientific libraries such as PyTorch, the GANs models and its associated convolutional network layers is developed.

The algorithm was deployed on Amazon servers to ensure optimal performance regarding speed and accuracy.

Given the sensitive nature of medical data and the potential risks associated with deepfake technologies, various security measures have explored. This study includes an analysis of the detection methods for deepfakes and a discussion on the ethical implications of using such technologies in healthcare. This includes a consideration of the existing security measures in healthcare and the advancements needed to protect the integrity of medical data.

This work also delve into the use of deep learning algorithms for fraud detection in healthcare, especially with the increasing sophistication of manipulated multimedia content. Techniques for detecting fake images and videos, focusing on both neural networks and handcrafted methods, are explored. The study further examines the accuracy and generalizability of these detection methods against various types of deepfakes and manipulations.

Data Preprocessing Phase

Cancer Genome Atlas Dataset

This dataset incorporated ~ 530 patients with pristine, primary tumor samples sourced from The Cancer Genome Atlas (TCGA). The Broad Institute curated the gene expression profiles using Affymetrix microarrays. Level 3 data, fetched from the National Cancer Institute's Genomic Data Commons [66], underwent quantile normalization and background adjustment. Each profile was constituted by 12,042 genes, which were subsequently standardized.

Data Cleaning

The images were aligned to each patient's short spin-lattice relaxation time indicates as T1-WI+c, and linearly interpolated to 1 mm3. Region-of-interests (ROIs) underwent manual segmentation experts and garnered approval from board-credentialed neuroradiologists. ROIs epitomized three-dimensional volumes of two zones: contrast-enhancement sourced from T1W1+c and peritumoral edema ascertained from short spin- lattice relaxation time indicates as T2WI. A similar segmentation protocol via adept raters for some cases, as illustrated in Fig. 1 is emulated. Features were derived from the most expansive, contiguously segmented zone for each ROI using OpenCV and Python. Each one of the image features was normalized by its maximum value.

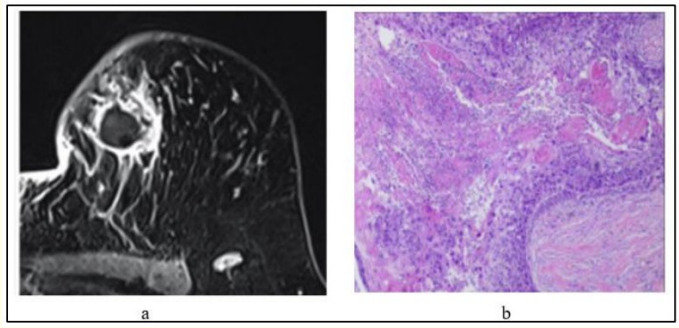

Figure 1: (a) Preoperative MRI of breast cell of T1WI+c node; (b) the posterior mass was confirmed to be invasive lobular carcinoma after surgery.

Radiogenomic Correlation Analysis and Prediction Phase

An autoencoder, a neural network variant, is conventionally employed to compact data into a more concise representation [22]. In this proposed approach, each gene expression profile served as an input. Both the ingress and egress layers boasted 1300 units. The

architecture housed five consecutive hidden layers, the model was subjected to training with the data from all gene expression profiles. For unearthing radiogenomic correlations, a deep neural network was trained on data from selected patients, all of whom had gene expression details and pre-operative MR studies. Fig. 2 shows the input, output, and hidden layers used in the DNN model. The first trio of hidden layers drew their initialization from the encoding layers of the previously trained. The network's weights and biases were further restricted to non-negative values to ensure the predictions followed suit. With a gene expression profile as the input, the deep neural network was tasked with the concurrent prediction of selected image features that corresponded to the tumor's morphology in the enhancing zone.

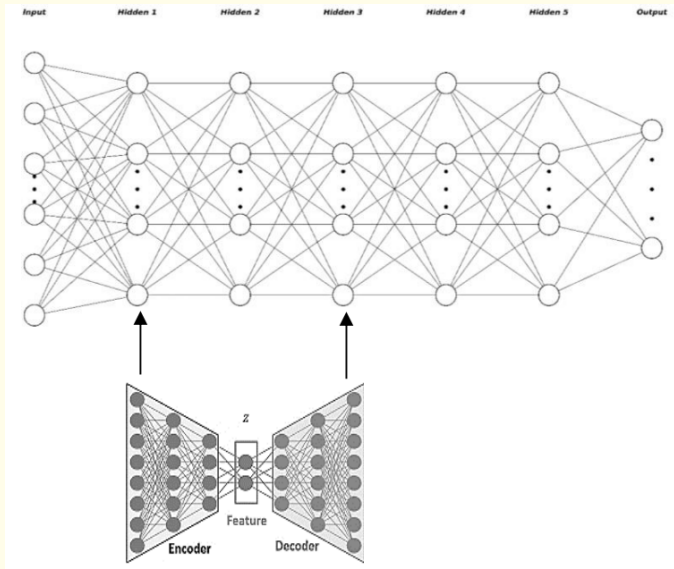

Figure 2: Deep Neural Network (DNN) Architecture with Input, Hidden, Output Layers, encoder, and decoder.

Radiogenomic Dataset Generation Phase

In this phase a Generative Adversarial Networks GANs are used to build a model to generate the radiogenomic dataset. GAN is a distinct subset of deep learning, falling under the umbrella of Convolutional Neural Networks (CNNs). GANs are engineered to generate new data that mirrors the data they've been trained on. For example, when trained on a dataset of images, a GAN can create new images that are visually convincing to human viewers. These artificially created images are commonly known as deepfakes. CNNs operate by taking an input image and allocating adjustable weights and biases to differentiate various features within the image. Within GANs, this framework is extended to include two neural networks: the Generator and the Discriminator. These networks cooperate to distinguish original data from generated data. The rise of deepfakes has posed societal challenges, particularly because they can be nearly indistinguishable from genuine images or videos. These fabricated media pieces have been exploited to create disinformation, including fake news and misleading visuals. Given the advancements in machine-generated imagery, distinguishing between authentic and machine-created content has become increasingly challenging.

Examples include deepfake videos of Barack Obama making derogatory remarks about Donald Trump and Mark Zuckerberg claiming to control stolen data, among others. An AI company called Deeptrace reported that as of September 2019, there were 15,000 deepfake videos online, almost double the number from nine months prior. Technological advancements have also enabled individuals

with limited technical expertise to create various types of deepfakes, contributing to an already complicated landscape. Deepfake technology can create fictional, albeit convincing, images from scratch, as well as "voice skins" or "voice clones" for celebrities and public figures. Deepfake technology has been used in scams involving manipulated voice messages on platforms like WhatsApp, YouTube, and Facebook. Researchers have highlighted the potential risks, particularly in the realms of special effects and image manipulation. To create deepfakes, specific AI algorithms known as encoders and decoders are utilized.

The encoder compresses the features of multiple faces, while the decoder reconstructs these features, often swapping them with other faces. The computational demands are significant, often requiring high-end computing resources or cloud-based solutions. The legal consequences of creating and disseminating deepfakes can vary and could include copyright infringement, data protection violations, and even defamation. Unauthorized sharing of images could lead to criminal charges and potential jail time. In the realm of deepfakes, GANs are often used. A typical GAN network consists of a Generator, denoted as G(x), and a Discriminator, denoted as D(x). The Generator fabricates synthetic images that closely resemble the training set, while the Discriminator aims to differentiate real images from these synthetic creations. Both the Generator and Discriminator are trained simultaneously on different kinds of data, such as video, audio, and images. During the training phase, a dataset X is used, containing a multitude of real images x under a distribution Pdata. The Generator G strives to create images G(z) that mimic the real images x, where z is a noise variable under a distribution Pz. The Discriminator D aims to discern between generated and real images. The process is described as a two-player minimax game, which can be formalized by a specific value function shown in equation 1 below.

$$\mathrm{Min_G}\ \mathrm{max_D}\ V(D,G) = E_{X\sim P_{data}(X)}[\log D(X)] + E_{Z\sim P_z(Z)}[\log(1 - D(G(Z)))] \quad (1)$$

After adequate training, the Generator should be capable of producing highly realistic images, while the Discriminator should improve its ability to distinguish between real and artificial images.

A GAN that has architectural topological constraints applied to it to provide training stability is called Deep Convolution GAN DCGAN [63]. The DCGAN consists of CNNs with different layers for both the generator and the discriminator. DCGANs are used for style transfer; for instance, the network will generate a set of handbags that has the same style as an inputted set of shoes. In this work, two DCGAN generators and two discriminators are used as shown in Fig. 3.

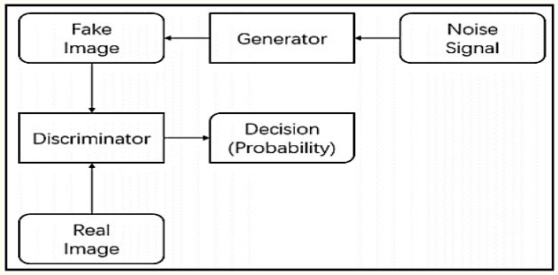

Figure 3: A block diagram of GAN [62].

In this phase, two sets of images as input for each DCGAN inspired by [64, 65] are used. The objective of each discriminator is to distinguish genuine images from the synthesized ones, generated by their respective generators. the block diagram, as depicted in Fig. 4, initiates by accepting two distinct sets of images, denoted as X and Y. During processing, regions of interest within these images are identified, cropped, and aligned.

The training phase focuses on generating fake images from set X that resemble images in domain Y and vice versa. The architecture for both the generator and discriminator networks consists of eight layers. Within each layer, batch normalization and Leaky ReLU are applied, followed by a tanh activation function, these networks are unified into a single model for training.

Loss metrics are calculated for both generators and discriminators to ensure the generated images closely map to their input counterparts. The losses for the generators and discriminators are aggregated to obtain a composite loss for the entire network are shown in questions 2 and 3 respectively.

$$L_{GAN} = E_{x\sim P_{data}(x)}[(1 - D_Y(G(x)))^2] + E_{y\sim P_{data}(y)}[(1 - D_X(G(y)))^2] \quad (2)$$

$$\begin{aligned} L_D = {} & E_{x\sim P_{data}(x)}[D_Y(G(x))^2] \\ & + E_{y\sim P_{data}(y)}[D_X(F(y))^2] \\ & + E_{x\sim P_{data}(x)}[1 - D_X(x))^2] \\ & + E_{y\sim P_{data}(y)}[1 - D_Y(y))^2] \end{aligned} \quad (3)$$

Where X and Y are two domains,
x, and y are different sets of input images,
G is the generator of images in domain X.
F is the generator of images in domain Y.
D is the discriminator of the GAN.

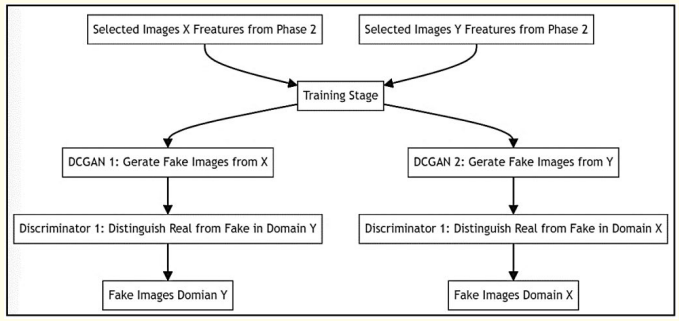

Figure 4: The diagram of the proposed method.

The generated images are saved, and new dataset shows the progression of this work is created from random noise to increasingly real images.

Results and Discussions

The research in the field of deepfake generation and detection, particularly within radiogenomics, represents a significant stride forward. Leveraging combined Generative Adversarial Networks (GANs) trained on realistic genomic and imaging data, synthetic data that is nearly indistinguishable from real data successfully generated. In the GAN architecture, the generator created synthetic data, while the discriminator's role was to distinguish between synthetic and real data. The iterative feedback process refined the generator's output, leading to increasingly accurate synthetic data generation. The deepfake algorithm has been fine-tuned using a carefully chosen dataset from TCGA [65] radio genomics. This data is annotated to establish a baseline for evaluating the predictions of the pro-

posed model against actual outcomes. This study leverages data from the Cancer Genome Atlas (TCGA), a resource that has generated a massive data across various omics disciplines, already contributing to advances in cancer diagnosis, treatment, and prevention. Fig. 5 displays a portion of this TCGA dataset, while Fig. 6 illustrates variations in tumor positions within samples of breast cancer from the same dataset.

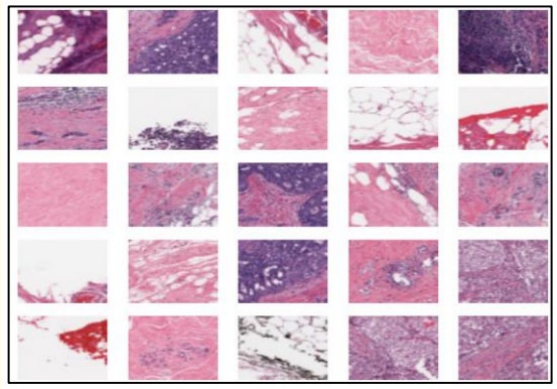

Figure 5: A snapshot of the TCGA dataset.

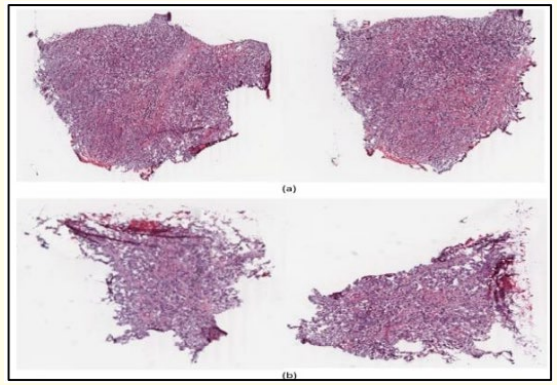

Figure 6: Variants of breast tumor positions in the TCGA dataset. (a) The upper part of the breast containing 92% tumor nuclei. (b) The lower part of the breast containing 80% tumor nuclei.

An array of hyperparameters, including learning rate, decay, momentum, loss function type, activation function type, and dropout are fine-tuned, the hyperparameters are show in table 1. The models' mettle was tested using 10-fold cross-validation, repeated for hyperparameter selection when diverse values were considered. The hyperparameters yielding the lowest average validation loss were cherry-picked. Performance errors were computed as the discrepancy between the reference value of an image feature, y^i (e.g., actual volume of edema) and the model's prediction, y^i (e.g., estimated volume of edema) across the 10 validation folds. Error was averaged over all N patients using mean absolute error (MAE) and mean absolute percent error (MAPE). The training specifications and environment details are listed in table 2.

Hyperparameter	*Value*
Learning Rate	0.001
Decay	1e-6
Momentum	0.5
MSE	0.105
MSA	0.105
Activation Function	ReLU
Dropout	0.1

Table 1: The hyperparameters used in the proposed approach.

Parameter	*Value*
Batch Size	1.0
Epoch Number	200
Optimization Method	Stochastic Gradient Descent
Libraries Used	Keras, Tensorflow
Hardware	Nvidia GRID K520 GPU
Cloud Service	Amazon Web Services

Table 2: Training Specifications and Environment Details.

The proposed model, with its hyperparameters of 0.2 learning rate, 1e−5 decay, and the hyperbolic tangent activation function, clocked in a 0.013 loss (mean squared error) post retraining. The deep neural network, when primed with pre-training and dropout, was optimized at a learning rate of 0.3 and a decay of 5e−5, epoch of 200, yielding mean training and validation losses (mean absolute error) of 0.105 and 0.134 respectively, as visualized in Fig. 7. In comparing the proposed approach with existing state-of-the-art methods, this work shows that the dual GAN architecture and deep learning models offer a more robust and comprehensive analysis. This is reflected in a 1.8% improvement in mean absolute percent error over traditional linear regression models. The comparison of the proposed method in this work with state of art methods is shown in table 3. The proposed method outperforms the previous state-of-the-art method, CNN- RNN, by 0.9% AUC (Area under the ROC Curve) on Hybrid Model of CNN, by 1.8% AUC on LSTM, by 1.3% AUC on DNN, by 1.6.

No	*Method*	*AUC*
[23]	CNN-RNN	85.4
[53]	Hybrid Model of CNN	84.5
[54]	LSTM	85
[56]	DNN	84.7
Proposed Method	Combined DCGAN	86.3

Table 3: The comparison of the proposed method with state of art methods.

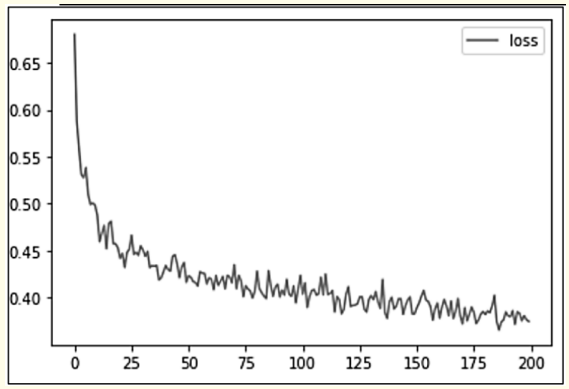

Figure 7: The proposed model learning curves from 10-fold cross-validation using selected hyperparameters.

Conclusion

Current machine learning techniques have the capability to identify cancer from a wide array of medical imagery. However, the scarcity of such images can hinder the performance and predictive accuracy of machine learning models. In this study, a pioneering path in radiogenomic analysis is charted, harnessing the power of autoencoders and deep neural networks, and juxtaposed their prediction efficacy against that of linear regression. On the whole, neural networks displayed superior precision than linear regression in forecasting the morphology of enhancing and peritumoral edema in pre-surgical MR images. After the radiogenomic analysis phase is done, deep GANs to construct a deepfake model for generating a synthetic dataset of breast cancer images for use in machine learning-based cancer detection is employed. The findings underscored the proficiency of neural networks in discerning the relative magnitude of an image feature. It also indicate that the deepfake-generated medical images were indistinguishable from the original ones.

While the results of this work are promising, certain limitations in this study is acknowledged. Firstly, the reliance on synthetic data, despite its high fidelity, may not fully capture the nuances of naturally occurring radiogenomic variances. Additionally, this study focused on a specific cancer type (glioblastoma), which might limit the generalizability of the findings. Future research directions include expanding the methodology to other cancer types and further refining the GAN architecture to enhance the accuracy and realism of the synthetic data generated. Moreover, the aim is to explore the integration of the used synthetic data with larger, more diverse datasets to validate and potentially improve its diagnostic utility.

In conclusion, this research represents a significant advancement in the field of radiogenomics, offering a novel approach to generating and analyzing synthetic radiogenomic data. The implications of this study are far-reaching, potentially transforming the landscape of cancer diagnostics and treatment planning. The findings highlight the efficacy of deep learning models in medical research, opening new avenues for exploration and development in this rapidly evolving field.

Acknowledgments

We thank University of Arkansas/AHPCC center for providing a Pinnacle account which significantly improves the current work.

Funding

This work was supported by the Arkansas National Science Foundation NSF EPSCoR Track 1 award number OIA-1946391. Funding of the DART Seed Grant Program, the Board of Directions of the Arkansas Economic Development Commission's Division of Science &

Technology in Resolution 21-3, dated May 7, 2021.

References

1. Lambin P., et al. "Radiomics: extracting more information from medical images using advanced feature analysis". Eur J Cancer 48.4 (2012): 441-446.
2. Sala E., et al. "Unravelling tumour heterogeneity using next-generation imaging: radiomics, radiogenomics, and habitat imaging". Clin Radiol 72.1 (2017): 3-10.
3. Kumar V., et al. "Radiomics: the process and the challenges". Magn Reson Imaging 30.9 (2012): 1234-1248.
4. Mazurowski MA. "Radiogenomics: what it is and why it is important". J Am Coll Radiol: JACR 12.8 (2015): 862-866.
5. Kuo MD and Jamshidi N. "Behind the numbers: decoding molecular phenotypes with radiogenomics-guiding principles and technical considerations". Radiology 270.2 (2014): 320-325.
6. Bigos KL and Weinberger DR. "Imaging genetics--days of future past". Neuroimage 53.3 (2010): 804-809.
7. Stoyanova R., et al. "Association of multiparametric MRI quantitative imaging features with prostate cancer gene expression in MRI- targeted prostate biopsies". Oncotarget 7.33 (2016): 53362-53376.
8. Renard-Penna R., et al. "Multiparametric magnetic resonance imaging predicts postoperative pathology but misses aggressive prostate cancers as assessed by cell cycle progression score". J Urol 194.6 (2015): 1617-1623.
9. Mehta S., et al. "Predictive and prognostic molecular markers for cancer medicine". Ther Adv Med Oncol 2.2 (2010): 125-148.
10. Punnappurath A and Brown MS. "Learning raw image reconstruction-aware deep image compressors". IEEE 12 Transactions on Pattern Analysis and Machine Intelligence (2020).
11. Cheng Z., et al. "Energy compaction-based image compression using convolutional autoencoder". IEEE Transactions on Multimedia (2019).
12. Chorowski J., et al. "Unsupervised speech representation learning using wavenet autoencoders". IEEE/ACM Transactions on Audio, Speech, and Language Processing 27.12 (2019): 2041-2053.
13. T Karras, S Laine and T Aila. "A style-based generator architecture for generative adversarial networks". in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2019): 4401-4410.
14. T Karras., et al. "Analyzing and improving the image quality of STYLEGAN". in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2020): 8110-8119.
15. X Zhang, S Karaman and S Chang. "Detecting and simulating artifacts in GAN fake images". in 2019 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE (2019): 1-6.
16. L Guarnera, O Giudice and S Battiato. "Deepfake detection by analyzing convolutional traces". in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (2020): 666-667.
17. L Guarnera, O Giudice and S Battiato. "Fighting deepfake by exposing the convolutional traces on images". IEEE 8 (2020): 165085-165098.
18. Jun-Yan Zhu., et al. "Unpaired image-to-image translation using cycle-consistent adversarial networks". arXiv preprint (2017): arXiv:1703.10593.
19. Masood M., et al. "Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward". Applied Intelligence (2022).
20. Shen T., et al. "Evaluation of an audio-video multimodal deepfake dataset using Unimodal and multimodal detectors". "Deep Fakes" Using Generative Adversarial Networks (GAN) (2018).
21. Khalid H., et al. "Evaluation of an audio-video multimodal deepfake dataset using Unimodal and multimodal detectors". Proceedings of the 1st Workshop on Synthetic Multimedia - Audiovisual Deepfake Generation and Detection (2021).
22. Guera and EJ Delp. "Deepfake video detection using recurrent neural networks". 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (2018).
23. Pu J., et al. "Deepfake Videos in the Wild: Analysis and Detection". arXiv (2021): (arXiv:2103.04263).

24. Westerlund M. "The Emergence of Deepfake Technology: A Review". Technology Innovation Management Review 9.11 (2019): 40-53.
25. N Mangaokar., et al. "Jekyll: Attacking Medical Image Diagnostics using Deep Generative Models". 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genoa, Italy (2020): 139-157.
26. Thambawita V., et al. "DeepFake electrocardiograms using generative adversarial networks are the beginning of the end for privacy issues in medicine". Sci Rep 11.1 (2021): 21896.
27. SP and S Sk. "DeepFake Creation and Detection:A Survey". 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India (2021): 584-588.
28. Roettgers J. How AI Tech Is Changing Dubbing, Making Stars Like David Beckham Multilingual (2019).
29. Lee D. "Deepfake Salvador Dali Takes Selfies with Museum Visitors". The Verge (2019).
30. Güera D and Delp EJ. "Deepfake Video Detection Using Recurrent Neural Networks". In Proceedings of the 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand (2018): 1-6.
31. Diakopoulos N and Johnson D. "Anticipating and addressing the ethical implications of deepfakes in the context of elections". New Media Soc 23 (2021): 2072-2098.
32. Pantserev K. "The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability". In Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity; Springer: Cham, Switzerland (2020): 37-55.
33. Oliveira L. "The current state of fake news". Procedia Comput. Sci 121 (2017): 817-825.
34. Zhou X and Zafarani R. "A survey of fake news: Fundamental theories, detection methods, and opportunities". ACM Comput. Surv. (CSUR) 53 (2020): 1-40.
35. Kietzmann J., et al. "Deepfakes: Trick or treat?". Bus. Horiz 63 (2020): 135-146.
36. Zakharov E., et al. "Few-Shot Adversarial Learning of Realistic Neural Talking Head Models". In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, Republic of Korea (2019): 9458-9467.
37. Damiani J. A Voice Deepfake Was Used to Scam a CEO Out of $243,000 (2019).
38. Korshunov P and Marcel S. "Vulnerability assessment and detection of Deepfake videos". In Proceedings of the International Conference on Biometrics (ICB), Crete, Greece (2019): 1-6.
39. Scherhag U., et al. "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting". In Proceedings of the International Conference of the Biometrics Special Interest Group, Darmstadt, Germany (2017): 1-7.
40. Rathgeb C, Drozdowski P and Busch C. "Detection of Makeup Presentation Attacks based on Deep Face Representations". In Proceedings of the 25th International Conference on Pattern Recognition (ICPR), Virtual Event (2021): 3443-3450.
41. Majumdar P., et al. "Evading Face Recognition via Partial Tampering of Faces". In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Long Beach, CA, USA (2019): 11-20.
42. Ferrara M., et al. "On the impact of alterations on face photo recognition accuracy". In Proceedings of the International Conference on Image Analysis and Processing, Naples, Italy (2013): 743-751.
43. Yang L, Song Q and Wu Y. "Attacks on state-of-the-art face recognition using attentional adversarial attack generative network. Multimed". Tools Appl 80 (2021): 855-875.
44. Colbois L, Pereira T and Marcel S. "On the use of automatically generated synthetic image datasets for benchmarking face recognition". arXiv (2021): arXiv:2106.04215.
45. Huang C-Y., et al. "Defending Your Voice: Adversarial Attack on Voice Conversion". In Proceedings of the IEEE Spoken Language Technology Workshop (SLT), Virtual (2021): 552-559.
46. Akhtar Z, Mouree MR and Dasgupta D. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection". In Proceedings of the IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), Irvine, CA, USA (2020): 55-60.
47. Akhtar Z and Dasgupta D. "A Comparative Evaluation of Local Feature Descriptors for DeepFakes Detection". In Proceedings of the IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, WA, USA (2019): 1-5.

48. Bekci B, Akhtar Z and Ekenel HK. "Cross-Dataset Face Manipulation Detection". In Proceedings of the 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Türkiye (2020): 1-4.
49. Khodabakhsh A and Akhtar Z. "Unknown presentation attack detection against rational attackers". IET Biom 10 (2021): 1-20.
50. Yavuzkilic S., et al. "Spotting DeepFakes and Face Manipulations by Fusing Features from Multi-Stream CNNs Models". Symmetry 13 (2021): 1352.
51. Wang T., et al. "Deep convolutional pooling transformer for deepfake detection". arXiv (2022): arXiv:2209.05299.
52. Kaddar B., et al. "HCiT: Deepfake Video Detection Using a Hybrid Model of CNN features and Vision Transformer". In Proceedings of the 2021 IEEE Visual Communications and Image Processing (VCIP), Munich, Germany (2021): 1-5.
53. Yavuzkiliç S., et al. "DeepFake Face Video Detection using Hybrid Deep Residual Networks and LSTM Architecture". In AI and Deep Learning in Biometric Security: Trends, Potential and Challenges; CRC Press: Boca Raton, FL, USA (2021): 81-104.
54. Hussain S., et al. "Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples". In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, Virtual (2021): 3348-3357.
55. Lim S-Y, Chae D-K and Lee S-C. "Detecting Deepfake Voice Using Explainable Deep Learning Techniques". Appl. Sci 12 (2022): 3926.
56. Kidder BL. "Advanced image generation for cancer using diffusion models". bioRxiv (Cold Spring Harbor Laboratory) (2023).
57. Zhu C. "Breast Cancer Immunohistochemical Image Generation: a Benchmark Dataset and Challenge Review". arXiv.org (2023).
58. Mehta V., et al. "FakeBuster: A DeepFakes detection tool for video conferencing scenarios". In Proceedings of the International Conference on Intelligent User Interfaces-Companion, College Station, TX, USA (2021): 61-63.
59. Juefei-Xu F., et al. "Countering Malicious DeepFakes: Survey, Battleground, and Horizon". Int. J. Comput. Vis 130 (2022): 1678-1734.
60. Lu Z., et al. "Recent progress of face image synthesis". In Proceedings of the 4th IAPR Asian Conference on Pattern Recognition (ACPR), Nanjing, China (2017): 7-12.
61. Zhang T. "Deepfake generation and detection, a survey". Multimed. Tools Appl 81 (2022): 6259- 6276.
62. Mustak M., et al. "Deepfakes: Deceptions, mitigations, and opportunities". J. Bus. Res 154 (2023): 113368.
63. Ian Goodfellow., et al. "Generative adversarial nets". In Advances in neural information processing systems (2014): 2672-2680.
64. Alec Radford, Luke Metz, and Soumith Chintala. "Unsuper. Demonstration of results for transferring Ukiyo-e to photos". Revised representation learning with deep convolutional generative adversarial networks. arXiv preprint (2015): arXiv:1511.06434.
65. (https://portal.gdc.cancer.gov/).

Volume 6 Issue 3 March 2024