Deepfakes on Retinal Images using GAN

Yalamanchili Salini
School of Computer Science & Engineering
VIT-AP University, Amaravati
Andhra Pradesh, India

Dr J HariKiran
School of Computer Science & Engineering
VIT-AP University, Amaravati
Andhra Pradesh, India

Abstract—In Deep Learning (DL), Generative Adversarial Networks (GAN) are a popular technique for generating synthetic images, which require extensive and balanced datasets to train. These Artificial Intelligence systems can produce synthetic images that seem authentic, known as Deep Fakes. At present, data-driven approaches to classifying medical images are prevalent. However, most medical data is inaccessible to general researchers due to standard consent forms that restrict research to medical journals or education. Our study focuses on GANs, which can create artificial fundus images that can be indistinguishable from actual fundus images. Before using these fake images, it is essential to investigate privacy concerns and hallucinations thoroughly. As well as, reviewing the current applications and limitations of GANs is very important. In this work, we present the Cycle-GAN framework, a new GAN network for medical imaging that focuses on the generation and segmentation of retinal fundus images. DRIVE retinal fundus image dataset is used to evaluate the proposed model's performance and achieved an accuracy of 98.19%.

Keywords—DeepFakes; deep learning; retinal fundus image synthesis; segmentation; generative adversarial network (GAN); variational autoencoder (VAE)

I. INTRODUCTION

An eye’s retina is a sensitive membrane responsible for vision. As shown in Figure 1, three primary anatomical components are the Optic Disc, Macula, and Blood Vessels.

Fig. 1. Picture of the Retina on the Left; The Segmented Image on the Right.

To categorize the GAN’s working capability, we divided them into seven categories: synthesis, segmentation, reconstruction, detection, de-noising, registration, and classification. The use of GANs has been studied across many different imaging modalities, including MRI (magnetic resonance imaging), CT (computed tomography), OCT (optical coherence tomography), chest X-rays, dermoscopy, ultrasound, PET, and microscopy.

A classic area of study in computer vision is image classification. A large, well-balanced dataset is frequently needed for training deep neural networks. However, because of the unbalanced dataset, most networks' performance will suffer while classifying medical images. Moreover, collecting pathological instances takes time in the domain of medical images. The ideal option is to create new, high-quality, diverse photographs of minority classes.

Artificial intelligence (AI) has gained popularity in recent years for use in medical imaging jobs. However, even while medical data sets are more widely available, most of them only apply to certain medical diseases, and collecting data for machine learning methods is still tricky. Some initiatives have focused on adding to the existing data to get beyond this obstacle. Numerous techniques for data augmentation have been proposed in this regard. Despite this, only minor adjustments, such as overfitting in learning processes or geometric modifications, have been made to meet the urgent requirement to provide data sets more meaningful. However, considerable improvement has been accomplished by introducing synthetic data augmentation to extend training sets. For example, synthetic data can present novel photos to existing data sets. It might contribute to increased diversity within a dataset and, eventually, to more robust machine learning algorithms if such a strategy is adopted.

To achieve the mentioned improvements: 1) GANs exploit density ratio estimation in an indirect manner of supervision to maximize probability density over the data-generating distribution; 2) By discovering the latent distribution of high-dimensional data, GANs have improved the performance of visual feature extraction.

For all these Deepfakes comes into picture because Deepfakes have gained public attention for their sinister uses, but they have also investigated in several medical fields. As ophthalmology has been at the forefront of the DL revolution, synthetic images can be used for various purposes, including fundus images and OCT. Several potential uses of GANs in ophthalmology have yet to be investigated, including how they can be applied to DL development and medical education and the implications of their use for privacy regulations. This study had two goals:

- A GAN applied to synthetic images generated by using DRIVE database was tested to determine whether the machine could identify the authentic fundus images.
- In addition, GANs are being examined for their uses in ophthalmology, as well as their limitations.

The remaining portions of this paper take place in multiple sections—first, the related work regarding Image translation and Image synthesis is discussed in Section II. Then, Sections III goes on with Materials & Methods for retinal image
generation. Next, the proposed network and its importance will discuss in Section IV. Next, the experimentation findings take part in Section V where the segmentation’s performance and execution time are concerned with existing techniques. Later on, concluding with a discussion in Section VI. Finally, Section VII contains a conclusion.

II. RELATED WORK

Deep learning-based computer systems that assist in medical diagnostics are greatly interested. But because of restrictions on data access due to proprietary and privacy issues, these systems’ development and improvement cannot be sped up by contributions from the general public [14]. For example, without the patient’s consent, it might be challenging for medical personnel to publish most medical pictures [15]. Furthermore, the publicly accessible datasets frequently have an insufficient size and expert annotations, making them unsuitable for training data-hungry neural networks. As a result, only academics with access to private data can create these systems, which restricts the development and potential of this area of study.

A. GAN & VAE

In addition to GAN, Variational Autoencoder (VAE) is another family of deep generative models that should investigate for medical imaging tasks. Latent (random) vectors are the input for GAN. However, one must carefully modify the GAN output to create synthetic images with the required characteristics. To deal with this issue, VAE had introduced. An encoder and a decoder are the two components of a VAE. Utilizing multilayer convolutional neural networks, the encoder turns input images into latent vectors of random variables with corresponding mean and standard deviations.

VAE, unlike GAN, starts with samples selected from the latent vector associated with the input and then sends them to the decoder for reconstruction. Thus, we can manipulate VAE directly to create specific synthetic output images for clear input photos. However, due to the loss function of the mean square error, the output of the VAE could appear hazy. Combining the advantages of VAE and GAN creates an adversarial network for similarity measures to address this problem. The application of VAE in medical imaging is quite innovative [16,17] and needs further investigation to process retinal images.

B. Image-to-Image Translation

In picture-to-image translation, an altered version of an existing image is created synthetically. Therefore, a sizable dataset of matched instances is often needed when training a model for image-to-image translation. For which a paired sample dataset is traditionally required to prepare an image-to-image translation model. In other words, a sizable dataset with several examples of modified versions of the input image X that can be utilised as the intended output image Y. These datasets, particularly in the medical field, are time-consuming, expensive, and sometimes impossible to compile. The image-to-image translation framework can be applied to a variety of computer vision problems, including image super-resolution [18], image inpainting [19], and style transfer [20]. It is possible to employ both supervised and unsupervised methods [21,22,23].

C. Retinal Image Synthesis

Surgical simulations using an anatomic model of the eye and surrounding face were one of the first applications of retinal image synthesis. Nevertheless, the segmentation module’s performance heavily influences the quality of the generated images. To reduce the requirement for annotated samples and to improve the representativeness (for example, the variability) of synthesized images [24], a generative adversarial approach is used in conjunction with a style transfer algorithm. Recent implementations like the retinal background and fovea have been modelled using a dictionary of small images without vessels [25]. In addition, it’s an idea that training a segmentation network with authentic retinal images combined with synthesized ones leads to better segmentation results.

D. GAN’s on Retinal Image Synthesis: Present Status

GANs have shown the ability to produce impressively realistic synthetic medical images. This section describes existing work on GANs for synthesising coloured retinal fundus images [26,27,28,29,30,31]. (Table I)

III. MATERIALS & METHODS

A. Dataset

The DRIVE dataset initially consisted of 40 photos, but we expanded it to 120 images, using 125 for training, 55 for validation, and 20 for testing. This image used with a field view of 45 degrees and a dimension of 565 x 584 pixels. It has 540 pixels in diameter and a FOV of 540 pixels. As seen in Fig 2, each image in the DRIVE dataset has a mask to aid in identifying the field of view (FOV) region.

Fig. 2. DRIVE Database Sample (a) Original Image. (b) Mask Image.

B. Image Preparation

A black-and-white retinal vasculature map was created for each image using a U-Net trained on 154 photos from the DRIVE database [32]. The unaided eye cannot detect pigmentation and choroidal blood vessel patterns on vessel maps, so information about them is removed. In addition, a circular mask with black background was placed on all retinal images with suitable vascular maps to create photos of the synthetic retinal fundus images.
TABLE I. LIST OF ARTICLES ON THE CREATION OF COLOURED RETINAL IMAGES

<table>
<thead>
<tr>
<th>References</th>
<th>DataSets</th>
<th>Methods</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>i-ROP</td>
<td>PGANs</td>
<td>Segmentation and Latent space expression</td>
</tr>
<tr>
<td>27</td>
<td>Messidor</td>
<td>cGAN(Pix2Pix)</td>
<td>ISC,Qv</td>
</tr>
<tr>
<td>28</td>
<td>Messidor</td>
<td>AAE and cGAN(Pix2Pix)</td>
<td>Segmentation and ISC</td>
</tr>
<tr>
<td>29</td>
<td>Messidor</td>
<td>cGAN(Pix2Pix)</td>
<td>Segmentation and SSIM</td>
</tr>
<tr>
<td>30</td>
<td>Drive, Stare and Style references</td>
<td>cGAN(Pix2Pix) and Style transfer</td>
<td>Segmentation</td>
</tr>
<tr>
<td>31</td>
<td>Drive, Stare, HRF and Style references</td>
<td>cGAN(Pix2Pix) and Style transfer</td>
<td>Segmentation and SSIM</td>
</tr>
</tbody>
</table>

C. Why GANs?

GANs are deployed and used for artificial data augmentation. GANs work through the creation of synthetic pictures while simultaneously learning to distinguish between them as actual pictures see Fig 3. In addition to their use in ophthalmology, GANs are helpful in molecular oncology imaging and generated positron emission tomography (PET) pictures [33]. Even though present radiology applications attempt to aid in the diagnosis, human perception has not yet been used in this situation to assess the quality of GAN created synthetic data. In several instances, using GAN improves medical imaging by creating fresh retinal pictures from data consisting of pairs of retinal vascular trees [34]. Generator loss function and Discriminator classification information about generated images are depicted as well as Convolutional neural networks (CNNs) are standard tools for categorizing images and returning a scalar to represent the realness of the input pictures.

![Fig. 3. Generative Adversarial Network Training, pix2pix.](image)

D. U-Net

In order to generate a wider range of realistic images, we developed a pipeline instead of CNN based on this we trained a U-Net segmentation network with our synthetic data to generate a segmentation mask from a photorealistic medical image to assess the credibility of the data. The u-net design, explicitly created for biomedical images, is descended from the auto encoder architecture, which uses unsupervised learning for dimensionality reduction. The u-net is particularly helpful for biomedical applications because it lacks completely connected layers, has no restrictions on the size of input images and permits a substantially higher number of feature channels than a conventional CNN [35]. The decoding procedure also concatenates the receptive fields before and after convolution. By doing this, the network can use both the up-convolutional and initial properties. To determine the accuracy of the GAN, 4282 image pairs were trained for 200 epochs. Following this, synthetic retinal fundus images were created using all the retinal vascular maps from the test data. It is one of the key advantages of GANs that they can produce much larger datasets than the initial ones see Fig 4.

![Fig. 4. U-Net Segmentation Network](image)

E. Segmentation

Machine learning involves segmenting images into appropriate sections. Fundus pictures with low contrast, complicated, and compound characteristics must be meticulously segmented to separate retinal vessels from one another. Deep learning systems are capable of identifying vessels against backgrounds accurately. This method, however, did not factor in ambiguous vessels, resulting in inaccurate estimates of vascular calibre biomarkers, such as tortuosity, length-to-diameter ratios, branching angles, and fractal dimensions. The proposed architecture uses long and short skip connections along with U-Net to address the abovementioned problem. Segmenting retinal vessels and looking for anomalies in the retinal subspace requires an exact technique. In recent years, several supervised and unsupervised algorithms have been proposed to segment retinal vessels. However, manual feature extraction is necessary for training with supervised approaches for different applications [36], [37]. In below we can see the workflow of supervised and unsupervised algorithms.

- A minimization function is used over the tuning process to determine which separation between the vascular and background classes is the most effective. Fig 5 displays a typical unsupervised learning algorithm workflow.
In supervised approaches, the segmentation algorithm must learn the vessel segmentation rule by studying the images manually labelled by professionals. Fig 6 depicts the workflow of a typical supervised technique.

![Fig. 6. Supervised Learning Algorithm Workflow.](image)

For getting segmented image initially in the first set, 577,649 pixels (12.7 percent) are marked as vessels, while 556,532 pixels (12.3 percent) are marked as vessels in the testing set, which is segmented twice from the training set [38]. See Fig 7 and Fig 8 for detailed view of DRIVE dataset segmentation and masking. Our results are comparable to those achieved by state-of-the-art methods using U-Net implementation to Cycle-GAN Network.

![Fig. 7. A Sample from the DRIVE Dataset. (a) Training Image, (b) Vessel Segmented of the Training Image, and (c) Mask of the Image.](image)

![Fig. 8. (a) A Sample Test Image from the DRIVE Dataset. (b) The First Segmentation (c) The Second Segmentation (d) The Mask Image.](image)

**F. PreProcessing**

During this stage, the retinal image quality is enhanced by separating vessels from the backdrop for achieving segmentation of vessels accuracy. The recommended network ensures that the retinal vascular tree can be segmented more effectively. Therefore, the trained model of the suggested network serves as the foundation for our method for retinal vascular segmentation, and its processing pipeline, as shown in Fig 9.

![Fig. 9. Forward cycle consistency loss for Cycle-GAN Network.](image)

It should note that using the DL network to segment a complete image may produce unreliable results. For the suggested neural network to focus, it is necessary to crop photos into patches. We will repeat this process in testing to produce segmented patches using the trained model. The segmented vessel tree is then produced by merging the segmented patches during the post-processing stage as shown in Fig 9.

**IV. PROPOSED WORK**

**A. Cycle-GAN: General Pipeline**

Any model should be able to identify the underlying relationship between the two domains and extract distinctive features from each field for image transformation between them. Cycle-GAN is nominated to offer these guidelines[39]. The finding in (1) briefs a mapping between domain X and domain Y, and vice versa, the system essentially merges two GANs. A generator G: X Y trained by discriminator DY and a generator F: Y X trained by discriminator DX create a structure shown in Fig 10.

\[
\min_{D, G} = \mathbb{E}_{x \sim P_{data}}[\log D(x)] + \mathbb{E}_{x \sim P_{y}}[1 - D(G(y))] 
\]

(1)

**B. Loss Function**

No paired data is available for CycleGAN training, so the input X and the target Y pair are not guaranteed to be meaningful. Thus, we propose the Cycle Consistency loss to ensure the network learns the correct mapping. Both discriminator loss and generator loss are similar to those used in pix2pix.

A cycle consistency refers to a close match between the input and the output. For Example, when we talk about NLP translations, the resulting sentence should be the same as the original sentence when translating from English to Telugu and then back to English. As a result of cycle consistency loss as specified in (2) and (3):

- X image information is passed to generator G, which produces image Y1.
- A cycled image Y1 is generated by passing generated image F through generator X1.
- Between X and X1, we calculate the mean absolute error. In the Figure 11, generator G is responsible for converting image X into image Y. If you feed image Y to generator G, and the output would be the image Y itself or something close.

\[
\text{Forward cycle loss: } X \rightarrow G(X) \rightarrow F(G(X)) \rightarrow X1 \tag{2}
\]

\[
\text{Backward cycle loss: } Y \rightarrow F(Y) \rightarrow G(F(Y)) \rightarrow Y1 \tag{3}
\]

**C. Image Generation**

The validation dataset examined images created from retinal vessel maps manually after training the GAN for 100 epochs on 120 pairs of images. Using all vessel maps, produced a synthetic retinal fundus image from the test dataset, see Fig 12 how the synthetic image looks by using proposed network.
D. PostProcessing

A segmented blood vessel image is created by merging all segmented patches. As a result, the offered patches are gathered and reduced in size for cropping. These patches are then replicated in the appropriate order, depending on the image size for cropping[40]. To remove the white pixels surrounding the retina, the mask of the used picture is placed on the combined image. Then, noise is removed using the morphological transformation "erosion" utilising an ellipse structural element of size 2*2.

V. EXPERIMENTS AND ANALYSIS

In this section, it is explained about the Parameter Settings in Section A. Later on, the evaluation principle is described in Section B, where the method is configured and put into practice. Then, using a retinal image dataset, Image classification is provided in Section C. Finally, we will see execution time measures in Section D.

A. Parameter Setting

Segmentation performance is achieved by training the suggested network with parameters selected experimentally or by consulting recent works. Experimentally, we determine the learning rate, the optimizer algorithm, the weight initialization method, and the epoch number [41]. First, we train one model without changing the parameters. Next, we pick the value with the highest segmentation rate.

B. Evaluation Principle and Metrics

We advise comparing the segmentation findings with manual segmentation by a skilled medical professional. Each pixel is defined as True Positives (TP), True Negatives (TN), False Positives (FP), or False Negatives for the evaluation (FN). Pixels correctly identified as background or vessels are expressed as TP and TN, respectively. As opposed, FP and FN represent pixels incorrectly identified as background or boats. A segmentation performance measure consists of Accuracy, Sensitivity, Specificity, and F1-Score. These metrics are the ones that are used most often to evaluate segmentation results. To classify
pixels as vessels. Accuracy performance is calculated, while Sensitivity and Specificity represent the ability to categorize pixels as vessels and backgrounds. The Precision parameter specifies the percentage of correctly classified background and vessel pixels among all correctly classified background and vessel pixels. As shown in Table II, the suggested method employs the following performance metrics.

Table III provides the performance metrics on DRIVE dataset where our method achieves 98.19% accuracy in detecting segmented images. The obtained ROC curves and plots representation for the performance metrics is shown in below Figure 13, Figure 14.

**Table II. Performance Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Elucidation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>$\frac{T_P + T_N}{T_P + F_P + T_N + F_N}$</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>$\frac{T_P}{T_P + F_N}$</td>
</tr>
<tr>
<td>Specificity</td>
<td>$\frac{T_N}{T_N + F_P}$</td>
</tr>
<tr>
<td>F1-Score</td>
<td>$\frac{T_P}{T_P + F_P}$</td>
</tr>
</tbody>
</table>

**C. Image Classification**

Using the high dimensional space, we can calculate the conditional probability, $P(ai|aj)$, representing the similarity between two samples is shown in (4).

$$P(ai|aj) = \frac{\exp \left( -\frac{||ai-aj||^2}{2 \sigma^2} \right)}{\sum_k \#1 \exp \left( -\frac{||ak-al||^2}{2 \sigma^2} \right)}$$  \hspace{1cm} (4)

50 actual and 50 synthetic photos with the same stage and illness distribution as the original dataset were uploaded, and runned ML programs to judge whether the photographs were natural or artificial. According to Figure 15 findings, most machine programs significantly distinguish between actual and artificial photographs.

**D. Execution Time Measures**

The proposed method is examined in this section for its processing performance. As shown in Table IV, we propose calculating each image’s execution period from the DRIVE dataset, respectively. Our analysis shows that despite the size of the image used, the computation values are too low for preprocessing, segmentation, and postprocessing. Then, we proposed evaluating the accuracy of the execution time compared to existing methods. Timing data is used in the evaluation for training the data. Because DRIVE is the most frequently used database, where values are provided in Table V, both metrics correspond to that database.

**VI. DISCUSSION**

In medical imaging, variations in illumination, noise, patterns, etc., result in a nonconvincing image produced by a GAN. A poorly defined vessel tree structure and dark spots show that the GAN can’t distinguish complex systems. As a result, it can only identify colour, shape, and lighting features. There are many intricacies in medical images that must be accurately portrayed for the data to be useful for medical imaging. This lack of detail is unacceptable for medical image generation, as medical images contain many intricacies. By breaking down the complex task of generating medical ideas into hierarchical processes, our Cycle-GAN architecture improves the quality of synthetic images by using the below rules:

- In the first step of generating Images, GAN focuses on developing segmentation metrics by ignoring the realism of photos.
- Using this technique, in the second step, GAN concentrates only on generating the colour of an image, brightness of image, and texture of image based on the dimensions provided.

In addition, our proposed network generates more diverse photos than original dataset. With Fig 12, GAN is able to produce synthetic images by keeping general statistical classification of the real dataset.

The method of retinal image synthesis currently used for rebuilding the optic disc and fovea is quite adequate, but duplicate lesions with high fidelity is a challenge that requires further research. In addition, for quality validation, experts and ophthalmologists must assess the level of realism of generated images. As a result of this study, we were able to demonstrate the below points:

- That vessel maps of original retinal images obtained by ROP screening can yield realistic-appearing synthetic fundus images and
TABLE III. PERFORMANCE MEASURE VALIDATIONS ON DRIVE DATASET.

<table>
<thead>
<tr>
<th>Database</th>
<th>No. of Epochs</th>
<th>Accuracy</th>
<th>Sensitivity</th>
<th>Specificity</th>
<th>F1-Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRIVE</td>
<td>25</td>
<td>82.83%</td>
<td>47.43%</td>
<td>89.45%</td>
<td>46.52%</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>89.77%</td>
<td>66.84%</td>
<td>93.11%</td>
<td>62.45%</td>
</tr>
<tr>
<td></td>
<td>75</td>
<td>98.19%</td>
<td>85.88%</td>
<td>99%</td>
<td>60.1%</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>97.5%</td>
<td>73.18%</td>
<td>99.46%</td>
<td>89.17%</td>
</tr>
</tbody>
</table>

TABLE IV. DURATION PERIOD ON DRIVE DATASET IMAGES.

<table>
<thead>
<tr>
<th>Metric</th>
<th>DRIVE Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preprocessing</td>
<td>0.026(s)</td>
</tr>
<tr>
<td>Segmentation</td>
<td>0.67(Time taken per patch)</td>
</tr>
<tr>
<td>Postprocessing</td>
<td>0.00347(s)</td>
</tr>
<tr>
<td>Time duration for each Image</td>
<td>0.7341(s)</td>
</tr>
</tbody>
</table>

TABLE V. COMPARISON TABLE OF TIME DURATION AND ACCURACY ON DRIVE DATASET.

<table>
<thead>
<tr>
<th>References</th>
<th>Publication Year</th>
<th>Time Duration in(s)</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>2008</td>
<td>0.193</td>
<td>0.198</td>
</tr>
<tr>
<td>35</td>
<td>2012</td>
<td>6.8</td>
<td>0.916</td>
</tr>
<tr>
<td>36</td>
<td>2018</td>
<td>0.421</td>
<td>0.943</td>
</tr>
<tr>
<td>37</td>
<td>2019</td>
<td>0.037</td>
<td>0.938</td>
</tr>
<tr>
<td>Our Method</td>
<td>2022</td>
<td>0.69</td>
<td>0.9819</td>
</tr>
</tbody>
</table>

- That most of machine programs can distinguish natural from synthetic retinal images. Annotated data can be used to create innovative methods for analyzing retinal images or to enrich information in existing databases to create synthetic images that look as authentic as possible. Additionally, due to GAN’s adaptability, they can be used to synthesize medical images using approaches used for retinal synthesis.

VII. CONCLUSION

The synthesis of retinal pictures using GANs has recently attracted more interest, and GANs have significantly developed in recent years. These tools can overcome restrictions like the scarcity of sizable annotated datasets and overcome the expense of collecting high-quality medical data. However, the findings of GAN applications in the realm of medical imaging are still far from being practically applicable. The unique anatomy of a colour retinal fundus image must also be taken into consideration when generating synthetic retinal images in order to learn about a patient’s health.

In this study, we present the Cycle-GAN framework, a new generative adversarial network for medical imaging that focuses on the generation and segmentation of retinal artery images. As a result, these artificial visuals appear realistic. DRIVE retinal fundus image dataset is used to evaluate the proposed model’s performance and achieved an accuracy of 98.19%. We must focus on investigating datasets of various biomedical images for interaction, domain adaptation tasks, and segmentation of medical images in the future.

ACKNOWLEDGMENT

We would like to thank VIT-AP university for facilitating the resources required for conducting this research.

REFERENCES


