



Module 6

Generative Adversarial Network (GAN): Architecture

In Machine Learning, there are different ways by which it can predict output on the unseen dataset. Further, Deep Learning and Neural networks, a part of Machine Learning, are such powerful technologies that are capable of generating new human faces from scratch that did not even exist before but appear natural with the help of training data, and this is possible with the technology named GAN or Generative Adversarial Networks. **Generative adversarial networks (GANs)** are among the most popular and recent unsupervised machine learning innovations developed by **Ian J. Goodfellow** in 2014. GAN is a class of algorithmic machine learning framework having two neural networks that connect and can analyze, capture and copy the variations within a dataset. Further, both neural networks work against one another in GAN machine learning, hence called **adversarial networks**. It is most often used in various ML applications, such as image generation, video generation, and speech generation. In this topic, we are going to discuss Generative Machine Learning (GAN), applications of GAN in machine learning, how GANs work, components of GANs, steps for training and prediction via Generative Adversarial Networks (GANs), challenges faced by generative adversarial networks, types of GANs, etc. So, let's start with a quick introduction to Generative adversarial networks (GANs) in Machine Learning.

What are Generative Adversarial Networks (GANs) in Machine Learning?

A Generative Adversarial Network or GAN is defined as the technique of generative modeling used to generate new data sets based on training data sets. The newly generated data set appears similar to the training data sets.

GANs mainly contain two neural networks capable of capturing, copying, and analyzing the variations in a dataset. These two neural networks are known as generators and discriminators, and both of them compete with each other.

The term Generative Adversarial Network consists of three words, and each of them has its separate meaning, which is as follows:

- **Generative:** It is used to learn a generative model that visually explains how data is generated.
- **Adversarial:** As both neural networks compete with each other or are adversarial to one another, hence training of the model is done in an adversarial manner.
- **Networks:** It uses deep neural networks to train models, hence called networks.

Why need GANs?

With the advancement of technology, there are various possible ways by which ML algorithms and neural networks can be fooled into misclassifying data just by introducing some noise in the



Module 6

training datasets. But with the innovations in machine learning, various techniques are being developed that can prevent the chances of misclassifying the images. Hence, GANs were discovered to generate new data sets, which look like training data sets and hence can start visualizing new patterns like training data.

Applications of GANs

GANs are a much popular approach in machine learning and have various applications in real-world scenarios. Below are a few most famous applications of generative adversarial networks (GANs), which are as follows:

- Fashion, art, and advertising
- Science
- Video games
- Audio synthesis
- Transfer learning

Besides these applications, there are so many miscellaneous applications of GANs in machine learning, which are as follows:

- It is used to diagnose partial or total vision loss by detecting glaucomatous images.
- It is used to visualize the interior design, industrial design, shoes, bags, and clothing items by generating photorealistic images.
- It is used to reconstruct 3D models of objects from images and model motion patterns in the video.
- It is used to develop age face photographs that determine individuals' faces according to their age.
- It is used to denoise welding images by removing the random light reflection on the dynamic weld pool surface.
- It is being used in data augmentation.
- It is used to reconstruct individual faces after listening to their voice. It is known as **GAN Speech2Face technology**.
- It is used to visualize the effects of climate change on particular locations.
- It is used to develop intelligent games and animations by creating anime characters.
- GANs generate text, articles, songs, poems, etc.

As soon as research on GANs in machine learning is going at its peak, in the future, we will see GAN applications in producing high-quality video, audio, and images also. Further, Microsoft has already collaborated with OpenAI to work on GPT and explore the power of GAN at the next level.

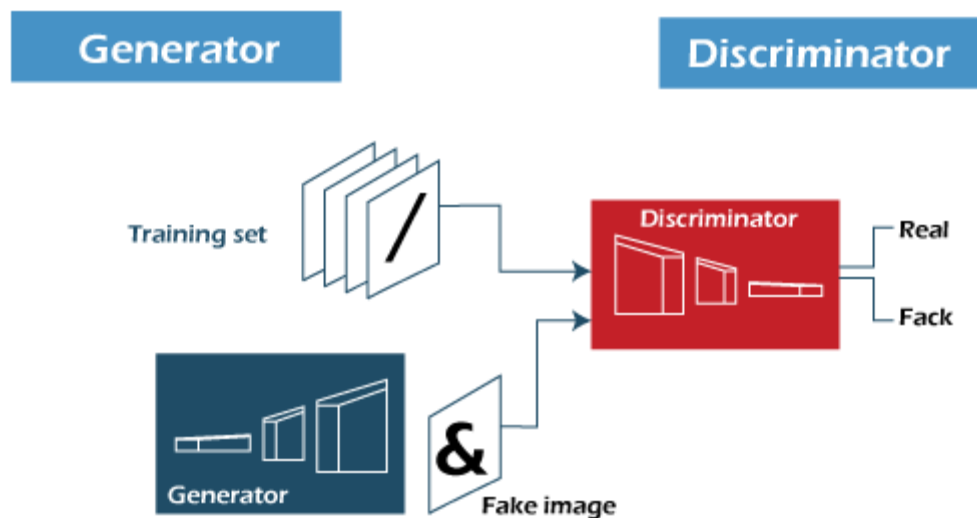
Components of Generative Adversarial Networks (GANs)

Generative adversarial networks are primarily made from two components, i.e., **generator** and **discriminator**. As the name suggests, the generator generates a fake output of unseen data based on training data sets and makes the discriminator fool to understand this fake data as accurate. Further, the discriminator acted as a cop and used to discriminate the training data and generated data, identify the abnormalities in the samples created by the generator and classify them as Fake or genuine. However, this entire process

Module 6

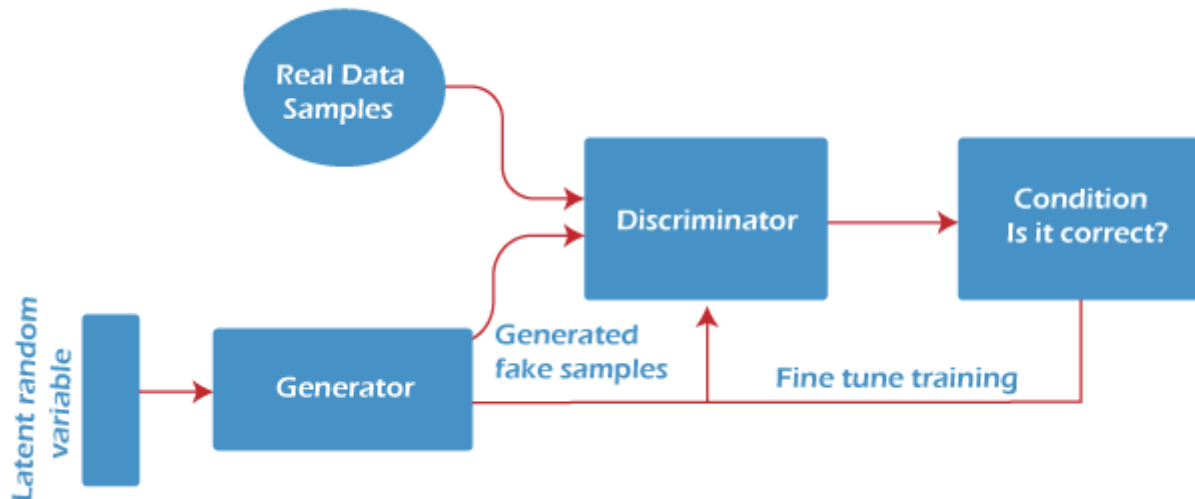
continues till the generator wins and ultimately makes a fool of the discriminator on fake data. Components of GANs are as follows:

Components of GAN



- **Discriminator:** It is used as a supervised machine learning approach in which a simple classifier is appointed to discriminate between real and fake data. Although, it is trained on actual training data sets and gives feedback to the generator.
- **Generator:** Unlike the discriminator, the generator is an unsupervised machine learning method used to generate fake samples based on actual training data sets. It is also a neural network with hidden layers, activation, and loss function. Further, the generator primarily focuses on generating fake data based on feedback given by the discriminator and makes the discriminator fool so that it cannot identify the difference between actual output and generated output by the generator.

Module 6



This process continues until the generator makes the discriminator fool, and once this is achieved generalized GAN model is created.

Training of Generative adversarial networks (GANs)

We have now discussed the basic concepts of generative adversarial networks (GANs) and their components. Now it's time to move further and learn about training and predictions of GANs in machine learning.

Here are a few essential steps to train GANs components individually. These are as follows:

Step-1: Identify the actual problems: This is essential in working on real-time projects. If you can identify the actual problems, you can only solve this efficiently. In GANs, whatever you are aiming for, you need to define that, which means What you want to create, like audio, poem, text, or image, is a type of problem.

Step-2: Choose appropriate GAN architecture: Although there are so many architectures of GANs exist, such as DCGAN, Conditional GAN, Unconditional GAN, Least Square GAN, Auxiliary Classifier GAN, Dual Video Discriminator, SRGAN, Cycle GAN, and Info GAN, we have to define which type of GAN architecture we are using in our project.

Step-3: Give training to discriminator on real data sets:

The discriminator is always given training on real data sets, and it only contains a forward path mechanism and does not follow backpropagation in n epochs. Further, it is only provided with actual data having zero noise or fake content. Further, for fake images, the discriminator uses instances created by the generator as negative output.

Some actions happen during the discriminator training process.



Module 6

Advertisement

- It discriminates both real and fake data in the process.
- It increases the model's overall performance and penalizes it when it fails to discriminate between both data.
- Discriminator loss is an essential part of the training process of discriminators, which helps in updating the weights of discriminators.

Step-4: Provide training to the generator: The training process of the generator starts with the introduction of some fake inputs. Initially, we give some fake input to the generator, but later it generates some fake output by adding some random noise. Further, whenever the generator gets trained, discriminators remain inactive, while the generator remains inactive when the discriminator gets trained. While providing training to generator training using any random noise as input, it aims to convert it into meaningful data to provide meaningful output, and the process takes time and runs under many epochs:

Below are a few simple steps to train the generator on fake input as follows:

- Provide fake input or noise and get random noise to produce output based on the noise sample.
- Predict generator output either real or fake using discriminator.
- Calculate discriminator loss and perform backpropagation.
- Calculate gradients to update the weights of the generator.

Step-5: Provide training to discriminators on fake inputs: In this step, we pass the samples to discriminators to predict whether the data is real or fake. Further, provide feedback received by decimators to generators again to do modifications in the samples.

How do GANs work?

As discussed above, GAN contains two neural networks, of which one is called Generator $G(x)$, and another one is called Discriminator $D(x)$. As the name suggests, both of these works in an Adversarial manner. The generator always tries to generate fake data similar to training data to fool the discriminator, i.e., it generates new data instances. Whereas the discriminator aims to identify the fake data from the actual data, i.e., it evaluates the authenticity of data. Both neural networks work simultaneously to learn from complex data, including images, audio, or video files.

Let's say we try to generate hand-written numerals similar to as MNIST dataset, which occurred in the real world; now, the discriminator aims to identify the instance of the accurate MNIST dataset as authentic. Meanwhile, the generator creates new synthetic images and passes them to the discriminator. The generator expects these images to be identified as accurate, even if they are fake. It generates as possible hand-written digits to fool the discriminator. The discriminator aims to identify images as fake coming from the generator.

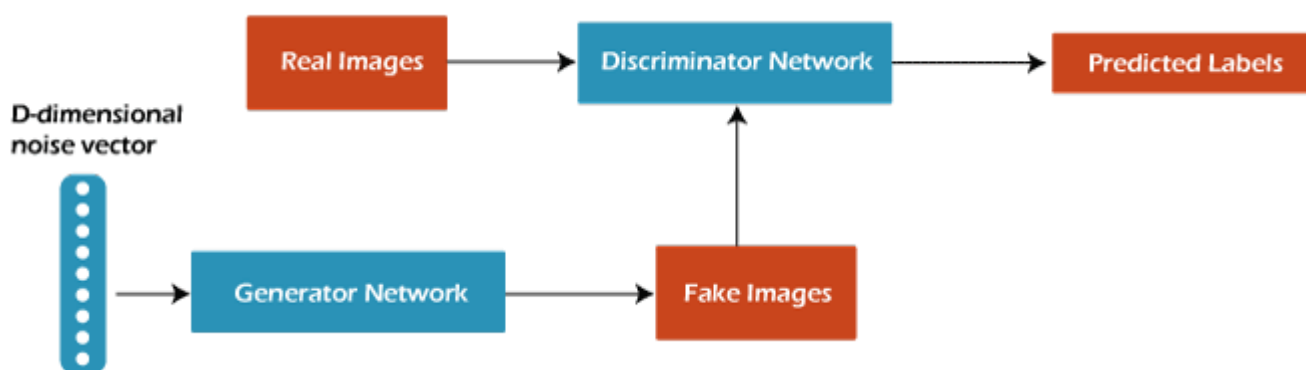
Advertisement

The working of GANs can be summarized in the below steps:



Module 6

- Firstly, the generator takes in any random number and generates an image.
- The generated image is inputted to the discriminator, and the authentic images are taken from the actual dataset.
- The discriminator contains both real and fake images, and now it aims to predict the labels with the identification of real and fake images. As an output, it returns probabilities of a number between 0 and 1, where 0 represents a prediction of fake and 1 represents authenticity. The working process of GAN is represented below image:



Advertisement

Different types of Generative Adversarial Networks (GAN)s

1. **DCGAN:** DCGAN or Deep Convolutional GAN is one of the most famous implementations of GAN. It makes use of ConvNets instead of Multi-layered perceptron. Contents use a convolutional stride and are built without max pooling. Further, layers in ConvNets are not entirely connected.
2. **Conditional and Unconditional GAN:** It is defined as a deep learning neural network having extra parameters. In conditional and unconditional GAN, labels are kept in such a way so that they can easily classify the input of the discriminator.
3. **Least Square GAN:** It is a particular type of generative adversarial network that uses the least-square loss function for the discriminator. Further, whenever the objective function of least square GAN is minimized, Pearson divergence also gets minimized automatically.
4. **Auxiliary Classifier GAN:** ACGAN or Auxiliary Classifier GAN is a similar but improved version of CGAN. Its discriminator not only classifies an image as real or fake but also gives information about the source of the input image.
5. **Dual Video Discriminator GAN:** It is the most helpful type of GAN for video generation built upon the BigGAN architecture. Further, it uses a spatial and temporal discriminator for generating videos.
6. **SRGAN: Super Resolution or SRGAN** is also known as domain transformation, primarily used to transform low-resolution images to high resolution.
7. **Cycle GAN:** It is used to perform image translation. E.g., we have trained it on a horse image dataset, and we can translate it into zebra images.
8. **Info GAN** is the latest and advanced version of generative adversarial networks used for unsupervised machine learning.



PARSHWANATH CHARITABLE TRUST'S
A.P. SHAH INSTITUTE OF TECHNOLOGY
Department of Computer Science and Engineering
Data Science



Module 6