The Application of Artificial Intelligence in Generating Fake Photos

Zixuan Wang – University of California, Los Angeles

Abstract

With the rapid development of artificial intelligence, people are able to do much work under the help of artificial intelligence. This report will focus on the application of artificial intelligence in generating fake photos. It will mainly introduce a research conducted by a company called Nvidia and evaluate the algorithm behind this technique. The report will also talk about what benefits the technique can bring to people and what concerns the technique may have.

1. Introduction

In recent years, scientists and researchers all over the world are dedicated to a new application of artificial intelligence – a technique that can generate convincing images and even can change the already existed images in a very convincing way.

www.nytimes.com/interactive/2018/01/02/technology/ai -generated-

Let us firstly look at these two pictures. It is hard for us to figure out which one is generated by the computer. In fact, both of them are generated by artificial intelligence. At present, A.I. does very well in generating celebrity photos that look real to people. It is important to learn how A.I. could produce such realistic photos.

2. Research

A group of researchers of Nvidia is now working on a project that is aimed at applying artificial intelligence in creating realistic images, at a lab in Finland. They have successfully built a system that can generate believable celebrity photos. The system began with a total of 30000 low-resolution images and produced over 10 million revisions during the 18 days of training.

www.nytimes.com/interactive/2018/01/02/technology/ai-generated-photos.html

The above series of images clearly gives the output of this system. We can see that it generated the low-resolution images at the beginning and gradually generated higher-resolution images. It shows that A.I. is a powerful tool to build up photos.

3. Basic procedure

To generate realistic photos, there are three basic steps to do this:

Firstly, we need to make A.I. analyze a large number of snapshots for the data sample, which is common in artificial intelligence. Then A.I. would recognize common patterns from the data sample for generating. At last, A.I. would try to produce data sample that is closed to the collected data. After these three steps. A.I. can generate photos that look real to people.

4. The algorithm behind the technique

4.1. Neural Network

To understand the way A.I. is working, it is essential to take a look at the neural network, which is the critical computing system for machine learning. The neural network is inspired by biological neural network and there are mainly four key elements of neural network:

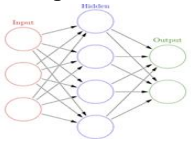
Artificial neurons: A neural network is basically a collection of artificial neurons and they are the elementary units of the neural network.

Adaptive weights: There are adaptive weights on the path connecting neurons. Adaptive weight is a kind of tunable parameter of the neural network.

Learning algorithm: The learning algorithm is used to tune the adaptive weights and it is a way to learn from the data observed. The learning algorithm is aimed to improve the whole model used by the neural network.

Cost Function: It is necessary to select an appropriate cost function to decide the best values of all the tunable parameter so that the learning algorithm is able to work properly. A cost function is the key of optimization.

Basically, neural network works to find out a solution to a specific problem and tries to optimize the solution, as close as possible to be optimal.



www.kdnuggets.com/2016/10/artificial-intelligence-deep-learning-neural-networks-explained.html

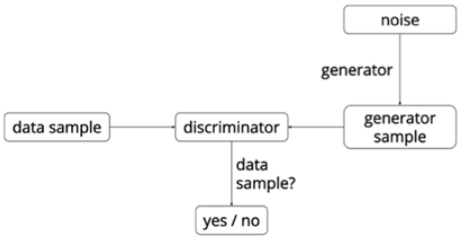
The above chart is a simple model of neural network. It contains an input layer, a hidden layer, and an output layer. There are neurons in each layer and paths connecting them. In addition, to improve the performance of the neural network, we can add more and more hidden layers to make the neural network more complex.

4.2. Generative Adversarial Network

The system to generate realistic images used the algorithm called generative adversarial network. It is of great significance for generating images and also the most popular algorithm for unsupervised machine learning. From its name, it is clear that it has two main characteristics, generative and adversarial:

A generative model: This model is able to learn the joint probability distribution of the labels and the input data. It can also derive the conditional probability using Bayes' theorem, which describes a fundamental formula in probability and also used in machine learning. There is another model in probability, discriminative model. The discriminative model can only learn the conditional probability. Therefore, the generative model is more advanced that the discriminative model in some way because the generative model learns the labels and the input data at the same time. The simultaneity may allow the generative adversarial network to figure out the underlying structure of the input data without labels but the discriminative model cannot do this.

Two competing neural networks: The system applies two neural networks, a generator and a discriminator.



http://blog.aylien.com/introduction-generative-adversarial-networks-code-tensorflow/

The above diagram explains how the two neural networks work: The generator is trying its best to produce realistic images and the discriminator is trying its best to distinguish the generated images from the images in the provided library of the data sample. Therefore, A.I. is playing a "cat-and-mouse game" against itself. As this competitive "game" goes on, A.I. is supposed to generate photos that look close to the data sample in the library provided.

5. Application

The technique is very powerful and can bring many benefits to the society. Traditionally, designers are working hard to build up images using Photoshop or other tools, which is very time-consuming. However, with this technique, it takes much less time to produce realistic images. Hence, it is very convenient and can be applied in various fields such as: computer interfaces, games, movies, advertising, fashion and so on. It can also be used for image reconstruction, which is consequential for scientists and researchers. Although there are still limits on this technique, (for example, it can only generate celebrity photos.) the researchers are confident that in the future, it can be applied in 3D images, videos and virtual reality.

6. Concerns

The progress of this technique also raises many concerns. The rapid speed to generating fake photos makes it easier for people to build up images that are not true. Hence, this may cause a rise of fake news on social media. It would become harder for the public to discern truth from untruth. The social concerns are considered by a number of researchers. But the step to studying artificial intelligence will not stop. Technology is not a fault itself. It depends on how people use it.

7. References

[1] Cade Metz and Keith Collins. "How an A.I. 'Cat-and-Mouse Game' Generates Believable Fake Photos". www.nytimes.com/interactive/2018/01/02/technology/ai-generated-photos.html.

[2] Alex Castrounis. "Artificial intelligence, Deep Learning, and Neural Networks, Explained". www.kdnuggets.com/2016/10/artificial-intelligence-deep-learning-neural-networks-explained.html.

[3] John Glover. "An introduction to Generative Adversarial Networks (with code in TensorFlow)" http://blog.aylien.com/introduction-generative-adversarial-networks-code-tensorflow/.

[4] Generative model. In Wikipedia. https://en.wikipedia.org/wiki/Generative_model.

[5] Stephanie Mlot. "Nvidia AI Generates Fake Faces Based On Real Celebs". www.geek.com/tech/nvidia-ai-generates-fake-faces-based-on-real-celebs-1721216/.