VLG Open Project
Generative AI

REPORT

By Arjun Angirishi
20112023
arjun_a@ee.iitr.ac.in

Github link :
https://github.com/Arjun-Angirishi/AI-Image-Detection-VLG

Problem Statement

With the advent of generative AI, it has become easily difficult to separate real data from AI-Generated.In a world where most services are available online, identity verification is crucial to ensure that only real individuals can access and use these services. However, with the rise of generative AI, fake identities can be easily created using sophisticated algorithms. This has led to an increase in identity fraud, as fake identities can be used to gain access to online services and commit fraudulent activities.
The goal is to develop a model that can identify a fake photo created by AI.

Dataset Used

https://bitgrit.net/competition/18#

Dataset contains mainly two csv files, a test data and a train data. Data is mainly 20 * 20 *3 images(RGB channels). The data is all preprocessed and cannot be turned back into images. Train contains about 5250 data points and the test contains 2250 data points.From the test data , F1 score is calculated which is the accepted competition metric.

Approach and Explanations

Earlier I tried using a simple convolutional neural network (CNN) with multiple convolution layers , max pooling layers with ReLu as an activation function and 3 layers of MLP along with batch normalization and dropout . That yielded maximum 87% val accuracy but was poor on the f1 score metric. As it turned out, the dataset was already fully processed and needed no more processing. Hence attention was turned to using simple ANN

which yielded much better results with above 75% f1 score. That also reinforced the hypothesis that the data provided was enough processed. ML based algorithms were also tried, with KNN giving high accuracy and high F1 score (93%) when used with SelectKBest. Hence this proves that the simple machine learning based models can also successfully classify this data and in some ways provide better performance than the deep learning counterparts.
A possible reason for this can be the amount of data provided was too less for deep learning based techniques to learn properly and hence machine learning based algorithms can prove to be a great alternative on this data set.

Result and Submissions

The github is provided with two submissions. One which is deep learning based (ANN) and other which is machine learning based (KNN). Both achieved f1 score over 0.7 with KNN based solution reaching 0.9335 and the other reaching 0.77. Code of both is provided along with the solution csv file.

Acknowledgement

I want to thank VLG for giving me this wonderful opportunity to work on this project. These projects led me to learn many new things especially in the fascinating avenues of deep learning which were earlier unexplored by me.