Group 15:
Determining image authenticity using Artificial Neural Network

Objective: The objective of this group assignment was to develop a CNN model with a processing pipeline to prepare images in a dataset and train the model to determine whether a supplied image is real or fake.

The dataset: We used a subset of images from "Astronomy Picture of the Day" (APOD). Two different files containing training and validation images was provided in the assignment page. It contained images (size 256x256) categorised as ‘Fake’ and ‘Real’ into two folders.

The model: We built a convolutional neural network, with an input layer shape (256, 256, 3) for input image size is 256x256 pixels with 3 channels (RGB).

We applied a series of convolutional layers with a filter size of 3x3 and 32 filters in the first and second layers and 64 filters in the third and fourth layers, 128 filters in the fifth and sixth layers, and padding was set to "same" with ReLU (rectified linear unit) as the activation function.

We used max pooling layers to downsample the spatial dimensions of the image by taking the maximum value in a pooling window. This along with the dropout layers was done to reduce the number of parameters in the model and control overfitting.

We flattened the layer and converted the 3D tensor into a 1D tensor and put it through a series of dense layers with 512, 256, 128 neurons respectively using ReLU activation function.

Finally, the model had an output layer with 2 neurons and softmax activation function to produce probability distribution over 2 classes.

The model was then compiled with Adam optimizer which is an adaptive learning rate optimization algorithm that uses the gradient of the loss function to update the model's parameters. The learning rate was set to 0.001. The loss function used was 'sparse_categorical_crossentropy' for multi-class classification and the model was evaluated based on accuracy.

Challenges: We had to overcome the challenge posed by the amount of time required to run the model while iterating through different number of epochs, trying different learning rate, different activation and loss functions. The prediction from the model was stuck at predicting only 1 class of data at one point which was due to initial reduction of the images to 128x128 during the pre-processing step. This was addressed by keeping the image size to their original size.

The main hurdle was to increase the validation accuracy of the model. We tried:

Data augmentation by applying random transformations, Hyperparameter tuning with different learning rate, batch size, and number of filters and added Dropout layers.

We also tested different network architectures and number of layers to improve the validation accuracy.

Result and possible improvements: The model was overfitted to the training data despite our efforts on minimising it. The training accuracy was 96.5% whereas the validation accuracy reached 79%. We can try adding more layers and average pooling in combination with the max pooling layers. Also, also looked into ResNet and VGG-19 but the results were not significantly different.

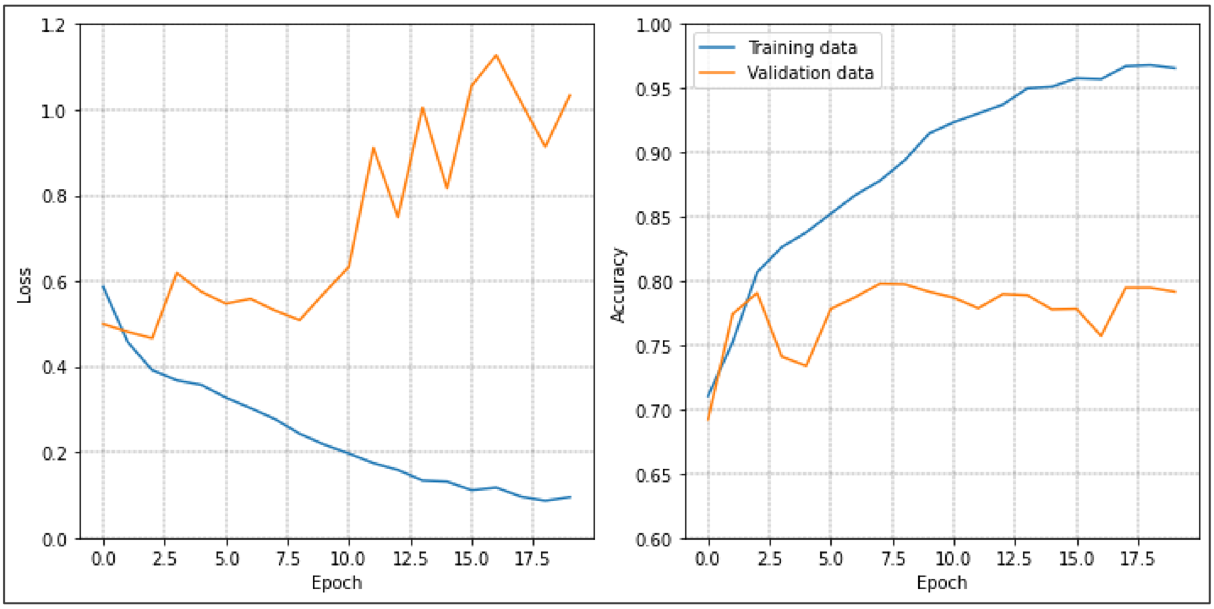

Fig 1: Plot of model performance.

References:

1. Lecture notes, tutorials on Neural Networks from Machine Learning and Neural Networks and Applied Data Science 2.
2. Charu C. Aggarwal, Neural Networks and Deep Learning, Springer International Publishing AG, 978-3-319-94463-0, Published: 25 August 2018.
3. https://apod.nasa.gov/apod/ap211109.html
4. Tianyi Wang, MingLiu, Wei Cao, Kam PuiChow, Deepfake noise investigation and detection Available at: https://www.sciencedirect.com/science/article/pii/S2666281722000762
5. https://www.kaggle.com/code/zohaib30/fake-vs-real-tensorflow-keras/notebook
6. Dr Chanda V Reddy, Anusha H, Dhanush N, Madhushree T P, Nischay P, Detection Of Real And Fake Image Using Deep Learning Algorithm, International Research Journal of Modernization in Engineering Technology and Science, Volume:03/Issue:07/July-2021 Available at: https://www.irjmets.com/uploadedfiles/paper/volume3/issue_7_july_2021/14249/1628083553.pdf