



ASSIGNMENT 1B

Joshua Paterson, Kaiyun Yu
N10193197, n9889663

Contribution Table

Person	Contribution
N10193197 – Joshua Paterson	Problem 1
N9889663 - Kaiyun Yu	Problem 2

Assignment 1B

Problem 1

CNN Model Design choices

For the first two parts (with and without data augmentation) of problem 1 used a convolution neural network made from scratch but the design is heavily influenced from the models used in the lectures and practicals. The layers of this model can be seen below in figure 1. The design of this model can be separated into 2 parts being made up of being your classic feedforward neural network and convolution/pooling parts. The convolution/pooling parts of the model are implemented directly after the first input layers (being of shape 32,32,3 meaning it is a 32,32-pixel image with 3 layers representing colour) and is repeated 3 times. The purpose of this layer is to compress the data down to a more manageable size and filter key features. Each of these 3 parts are made of the structure dot pointed below:

- 2x convolutional layers
- Normalisation layers
- Dropout layer
- Pooling layers

Each of these layers start with 2 convolutional layers with the purpose of extracting and filtering information from any sample. For the first pair of convolutional layers, it is design to produce 32 layers of dimensionality and this value is doubled per convolution/pooling parts. This is done in the hope that over each layer more combinations or patterns will be captured. A kernel size of (3,3) was chosen because the image itself is quite small being (32,32) so a large kernel size was not required.

After the 2x convolutional layers a layer dedicated to normalising the outputs of then is used. This layer is used to return values to a common scale after the data has been changed by the previous layers.

After a dropout layer is placed. This layer is used as removing some data at random may help to prevent overfitting to the training data.

The last part of each convolution/pooling parts is a pooling layer. Each of these layers have a pooling size of 2x2 each time the layer is used the dimension of the image is reduced by half. This is used to summarise features and reduce noise.

The final quarter of the model is made up of a feedforward section. To allow this, a layer is used to flatten the results of the previous convolution/pooling parts. This part of the model is made up of 5 layers where all but last layer uses the 'relu' activation function as it is a linear function and as I have no clue what the model will find a linear activation seemed like a reasonable place to start. The last layer has no activation function. The last layer was given no activation function as with trial and

error it was found that without one the model would produce better results. The first 3 layers are of 128 neurons wide. Through trial and error, it was found that increasing the number of 128-layers would produce better results however as explained latter 3 seemed like a good balance between training time and accuracy. The next layer is a layer containing 64 neuron and is used to reduce the number of neurons gradually before entering the final layer which is made up of 10 neurons as there are 10 classes.

Model: "cnn_model"		
Layer (type)	Output Shape	Param #
=====		
input_4 (InputLayer)	[(None, 32, 32, 3)]	0
conv2d_18 (Conv2D)	(None, 32, 32, 32)	896
conv2d_19 (Conv2D)	(None, 32, 32, 32)	9248
batch_normalization_9 (Batch Normalization)	(None, 32, 32, 32)	128
spatial_dropout2d_9 (Spatial Dropout)	(None, 32, 32, 32)	0
max_pooling2d_9 (MaxPooling2D)	(None, 16, 16, 32)	0
conv2d_20 (Conv2D)	(None, 16, 16, 64)	18496
conv2d_21 (Conv2D)	(None, 16, 16, 64)	36928
batch_normalization_10 (Batch Normalization)	(None, 16, 16, 64)	256
spatial_dropout2d_10 (Spatial Dropout)	(None, 16, 16, 64)	0
max_pooling2d_10 (MaxPooling2D)	(None, 8, 8, 64)	0
conv2d_22 (Conv2D)	(None, 8, 8, 128)	73856
conv2d_23 (Conv2D)	(None, 8, 8, 128)	147584
batch_normalization_11 (Batch Normalization)	(None, 8, 8, 128)	512
spatial_dropout2d_11 (Spatial Dropout)	(None, 8, 8, 128)	0
max_pooling2d_11 (MaxPooling2D)	(None, 4, 4, 128)	0
flatten_3 (Flatten)	(None, 2048)	0
dense_15 (Dense)	(None, 128)	262272
dense_16 (Dense)	(None, 128)	16512
dense_17 (Dense)	(None, 128)	16512
dense_18 (Dense)	(None, 64)	8256
dense_19 (Dense)	(None, 10)	650
=====		
Total params: 592,106		
Trainable params: 591,658		
Non-trainable params: 448		

Figure 1: CNN model layers

Loss Function

The loss function to be used for the models was the `sparse_categorical_crossentropy` loss function. This function was chosen as each sample will only belong to 1 of the classes where in similar functions samples may belong to multiple classes. This function was also chosen as labels came in the form of integers.

Dataset

The dataset for this problem consisted of 1000 labelled images for training the 10000 for testing. It should be noted as seen in figures 3 to 8 that both training and testing datasets do not have the same amount of training and testing data for all possible labels. The data seems to follow the trend that samples labelled with 2 will have 80% the number of samples that samples labelled with 1 will have this will continue as samples labelled with 3 will have 80% of samples when compared to samples labelled with 2. This is significant as this bias in training data could be translated into the models.

Data Augmentations

With the data augmentations used only a few parameters were chosen to change/alter images in the training space. This is because in each of the samples used for training and testing the number was always clearly in the centre of the image and other numbers could be present in a sample therefore the location of the number could not be changed to much. For simplicity 4 parameters were chosen to alter being zoom, height and small changes to rotation and shear_range as seen in table 1 below. Each of these parameters was chosen as they do not change the position (being the centre of image) of the labelled number except for height_shift_range. Height_shift_range was used as there was no images found in the training set with numbers above or below the labelled image as numbers are written left to right or horizontally.

Table 1: Data Augmentation used on Data

Data Augmentation	Range
rotation_range	10 degrees
zoom_range	80 to 120%
height_shift_range	10%
shear_range	15%

Computational Constraints

Due to computational constraints the model will be limited to a small model with less than 30 layers. Creating a large model would produce huge training times that would be infeasible to train due to time constraints on the project. However, a high level of accuracy has been achieved with the model detailed above as seen under the comparison heading with the model able to achieve above 80% accuracy on the testing set. It should be noted that with a more complex model (more layers) a higher level of accuracy should be able to be achieved.

Model description

Four models were used on the training and testing data provided. These being the CNN model detailed above both with and without data augmentations done the training data and a model developed for the CIFAR Dataset with and without data augmentations applied to the training samples.

When trained with no data argumentations a batch size of 40 and 50 epochs was chosen to train the data on the model. These numbers were selected by using trial and error by comparing both testing and training dataset accuracy however a batch size of 40 seemed reasonable as there were only a small amount of training data to use and 50 epochs was chosen as there is only a small amount of data a high value would expose the data too much to the model and could have caused overfitting.

With the model trained on the dataset with data augmentation applied to it the number of epochs was greatly increase to 250 as the data could produce more training data and was more likely to avoid overfitting because of this.

The CIFAR model is named 'vgg_2stage_CIFAR_small.h5 and was chosen because the input image shape and number of outputted classes where the same as the SHVN dataset. This allowed the model to be used for fine tuning on the SHVN dataset with no modification needed on the model itself. This model was also tested with and without data augmentations. The same batch size and epochs were used for training being 40 for batch size and 250 epochs when trained with data augmentations and 40 for batch size and 50 epochs when trained without data augmentations. This was for the same reasons as the purpose build CNN model detailed above.

```
Model: "simple_vgg"
```

Layer (type)	Output Shape	Param #
img (InputLayer)	[(None, 32, 32, 3)]	0
conv2d_40 (Conv2D)	(None, 32, 32, 8)	224
conv2d_41 (Conv2D)	(None, 32, 32, 8)	584
batch_normalization_34 (Batch Normalization)	(None, 32, 32, 8)	32
activation_34 (Activation)	(None, 32, 32, 8)	0
spatial_dropout2d_20 (Spatial Dropout)	(None, 32, 32, 8)	0
max_pooling2d_12 (Max Pooling)	(None, 16, 16, 8)	0
conv2d_42 (Conv2D)	(None, 16, 16, 16)	1168
conv2d_43 (Conv2D)	(None, 16, 16, 16)	2320
batch_normalization_35 (Batch Normalization)	(None, 16, 16, 16)	64
activation_35 (Activation)	(None, 16, 16, 16)	0
spatial_dropout2d_21 (Spatial Dropout)	(None, 16, 16, 16)	0
flatten_8 (Flatten)	(None, 4096)	0
dense_22 (Dense)	(None, 256)	1048832
batch_normalization_36 (Batch Normalization)	(None, 256)	1024
activation_36 (Activation)	(None, 256)	0
dropout_14 (Dropout)	(None, 256)	0
dense_23 (Dense)	(None, 10)	2570
Total params: 1,056,818		
Trainable params: 1,056,258		
Non-trainable params: 560		

Figure 2: CIFAR model Layers

As seen in figure 2 the CIFAR model is very similar to the model create for this problem above seen under the heading CNN Model Design choices. The difference these models have are that the CIFAR model has 2 less pooling layers and 1 less convolutional pair. It also has an activation layer added between the normalisation and dropout layers however the greatest difference between these models is that where the model created for this project is designed to increase the number of dimensions (filters) further through the layers where the CIFAR layers decrease the number of dimensions the further into the network. It should also be noted that after the layers are flattened in the CIFAR model the widths (number of neurons per layer) of the new model is twice as large as the

one created for this project and makes no attempt to decrease the layers gradually when close to the output layer.

CNN with no Data Augmentation Results

The results for the CNN model with no data augmentation used can be seen in figures 3 for the training data and figure 4 for the testing data. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified being 100% on the training images and 82.66% on the testing dataset.

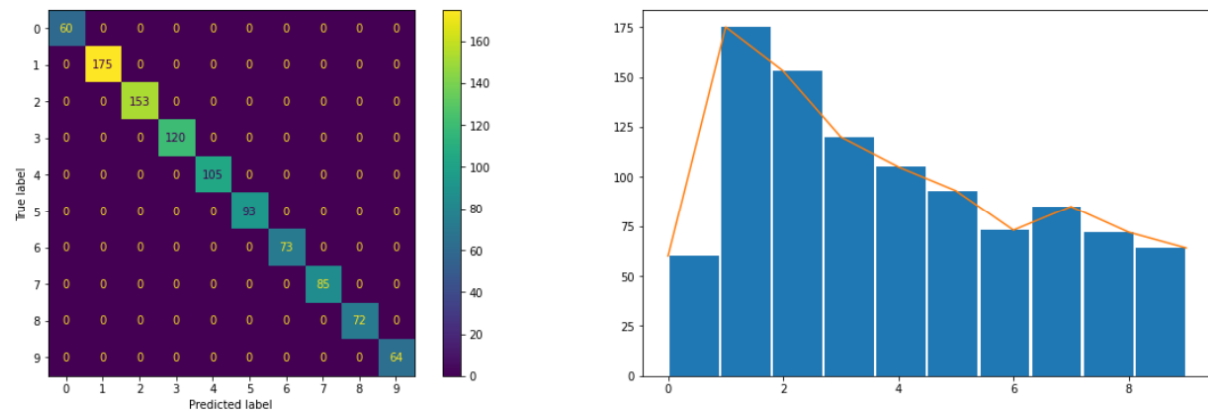


Figure 3: CNN with no Data Augmentation Training Dataset

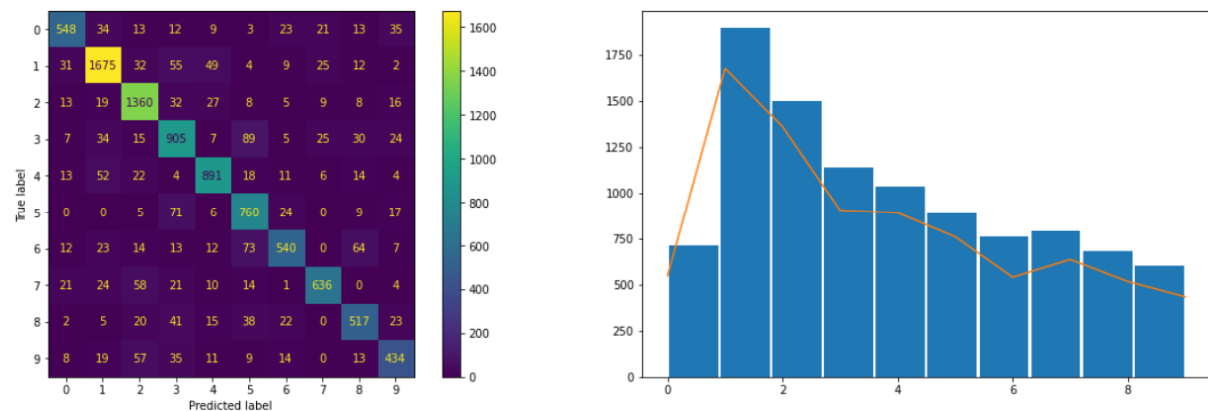


Figure 4: CNN with no Data Augmentation Testing Dataset

CNN Data Augmentation Results

The results for the CNN model with data augmentation used can be seen in figures 5 for the training data and figure 6 for the testing data. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified being 100% on the training images and 83.75% on the testing dataset.

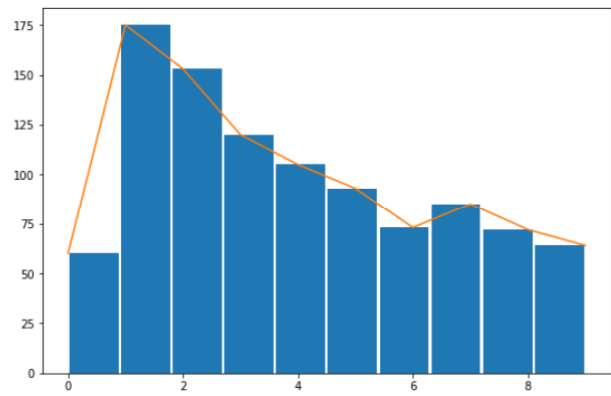
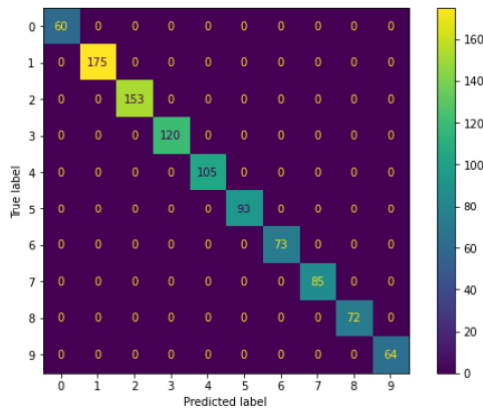


Figure 5: CNN with Data Augmentation Training Dataset

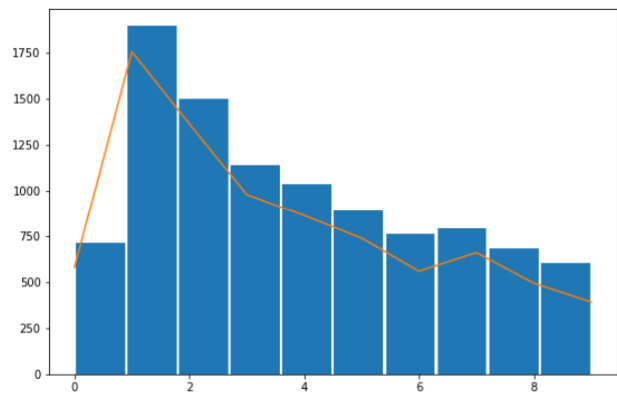
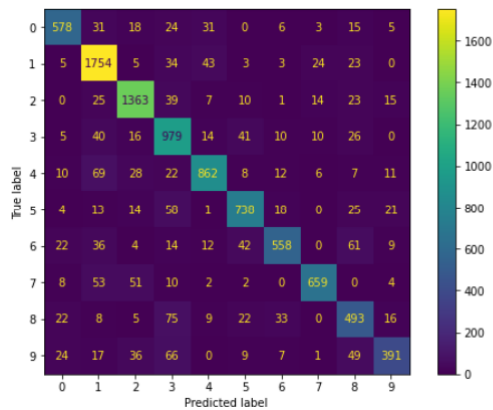


Figure 6: CNN with Data Augmentation Testing Dataset

CIFAR with Data Augmentation

The results for the CIFAR model with data augmentation used can be seen in figures 6 for the training data and figure 7 for the testing data. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified being 97% on the training images and 80.53% on the testing dataset.

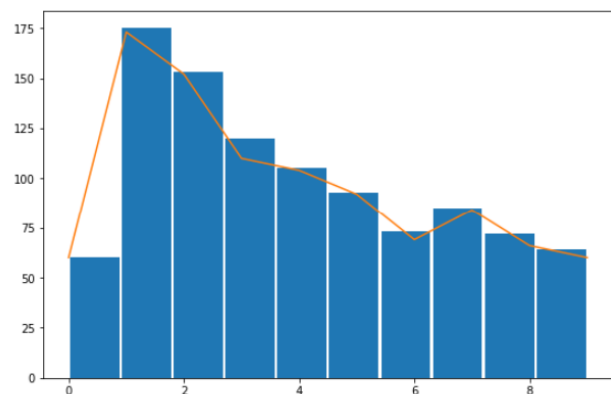
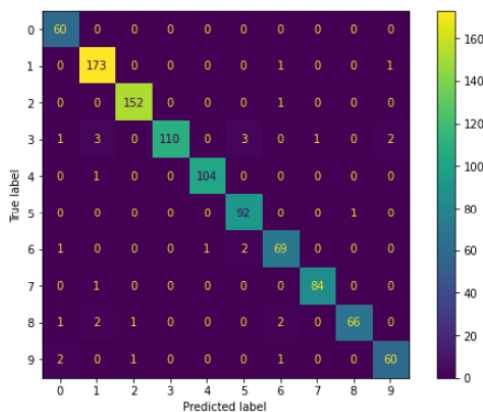


Figure 7: CIFAR with Data Augmentation Training Dataset

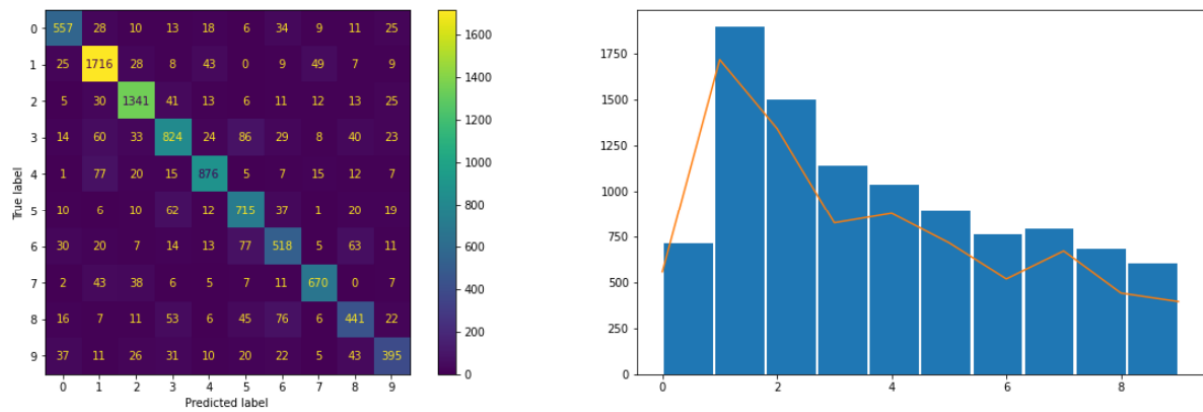


Figure 8: CIFAR with Data Augmentation Testing Dataset

CIFAR without Data Augmentation

The results for the CIFAR model without data augmentation used can be seen in figures 9 for the training data and figure 10 for the testing data. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified. The overall accuracy of the model can be seen below under model comparison on both the training and testing data given in table 2 which shows the percentage of correct samples classified being 62.8% on the training images and 46.7% on the testing dataset. Where unseen from the previous models the bias in the dataset has been shown within this model as the labels with more training data being samples labelled 1 and 2 have a better ratio of correctly predicted samples this can be seen in figures 9 and 10 left most plot as samples labelled 1 and 2 are the only labels to have a higher accuracy then around 50% in both training and testing data spaces.

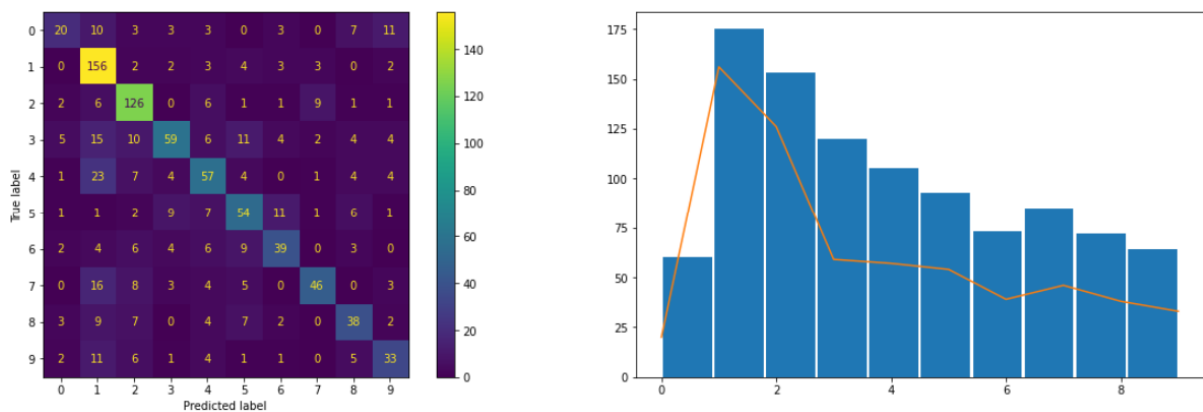


Figure 9: CIFAR without Data Augmentation Training Dataset

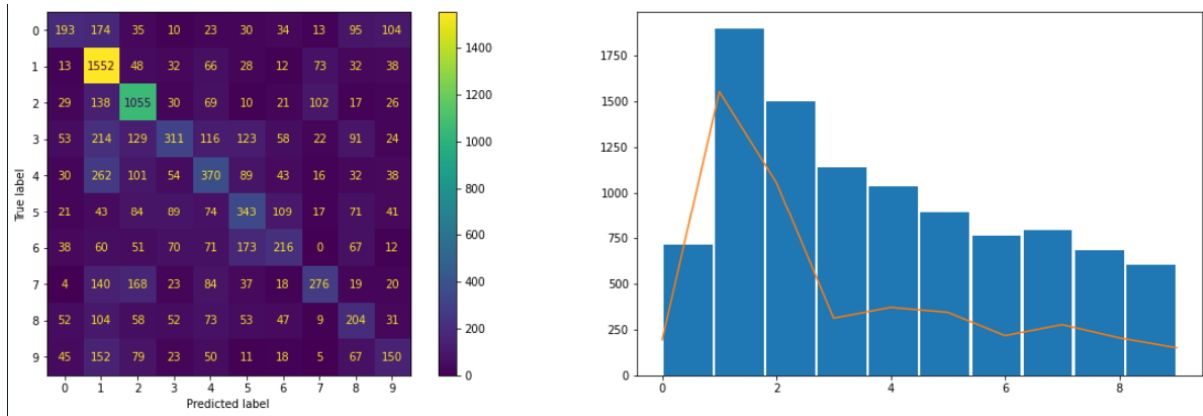


Figure 10: CIFAR without Data Augmentation Testing Dataset

Comparison of models

As seen in table 2 below all the tested models performed to a similar accuracy of around 80% on the testing samples and near perfect on the training samples except for the CIFAR model trained without data augmentations with an accuracy of 63% on the training samples and 47% on the testing samples.

Both model types being the purpose-built CNN model and CIFAR model where able to produce better results with data augmentations applied to the training data. It should be noted that the accuracy increase with the CNN model was small being of around 1.09% increase in accuracy on the testing samples where the CIFAR model was able to increase its accuracy by 33% on the testing samples. This was likely because the CNN model performed far better without data augmentations then the CIFAR showing there is demising returns the more accurate the model without data augmentations.

Both the purpose-built CNN models where able to produce the best result on this problem both being able to produce 100% accuracy on the data used for training and both being able to produce better results than the CIFAR models on the testing dataset where at worst there was a 2% increase in accuracy.

The CIFAR model was not able to produce very accurate result when data augmentations where not applied when used for fine tuning. This was likely due to the limit amount of data that the model could use for training (1000 samples). Due to both the increase in data due to fine tuning and the increased number of epoch used when training, the model was able to produce a accuracy on both training and testing that was comparable to the CNN models being around 2% less accurate on the testing set and 3 less accurate on the training set.

In conclusion all but the CIFAR model trained without data argumentations where able to achieve accuracy levels of around 80% on the testing set however this is still quite a poor performing model as it is still wrong 1 in 5 times. This low level of accuracy is likely due to both the small amount of data for training available as well as the self-imposed restrictions to model size of 30 layers. It is likely that a better result could be achieve with more data and a more complex model.

Table 2: Accuracy of Models on Datasets

Models	Training data Accuracy (%)	Testing data Accuracy (%)
CNN with no data augmentation	100.0	82.66
CNN with data augmentation	100.0	83.75
CIFAR_small model with data augmentation	97.0	80.53
CIFAR_small model without data augmentation	62.8	46.7

Problem 2

PCA and data extraction

Data is splinted to training set and testing set already. Data is saved as 5933 jpg images with the shape of 128x64. Pil.Image function has saved all Data in a 4D numpy array which size as (5933, 128,64,3) that keeps original size and information of training set and the data needs to be reshaped and resize in further.

```
load training data

[26] ▶ M4
train_path = 'Data/Q2/Q2/Training/'
train_imgs, train_labels = load_data(train_path)
print('Total Training Images : ', train_imgs.shape[0])
print('Training Image Shape : ', train_imgs[0].shape)

Total Training Images : 5933
Training Image Shape : (128, 64, 3)

load Gallery data

[27] ▶ M4
gallery_path = 'Data/Q2/Q2/Testing/Gallery/'
gallery_imgs, gallery_label = load_data(gallery_path)
print('Total Gallery Images : ', gallery_imgs.shape[0])
print('Gallery Image Shape : ', gallery_imgs[0].shape)

Total Gallery Images : 301
Gallery Image Shape : (128, 64, 3)

load Probe data

[28] ▶ M4
probe_path = 'Data/Q2/Q2/Testing/Probe/'
probe_imgs, probe_label = load_data(probe_path)
print('Total Probe Images : ', probe_imgs.shape[0])
print('Probe Image Shape : ', probe_imgs[0].shape)

Total Probe Images : 301
Probe Image Shape : (128, 64, 3)
```

Figure 11:Data loading

PCA is more suitable with unsupervised machine learning, PCA is mainly to find a better projection method from the angle of the covariance of the feature to select the direction of the sample point projection with the largest variance while LDA considers the classification label information more and seeks to size the data point distances between different categories after projection and minimize the data point distances of the same category. Which means choosing the direction with the best classification performance.

Reshape the data to 4 rows, 5933 columns matrix and use PCA to dimension the data for extracting feature information and calculated Euclidean Distance which is (301,301).

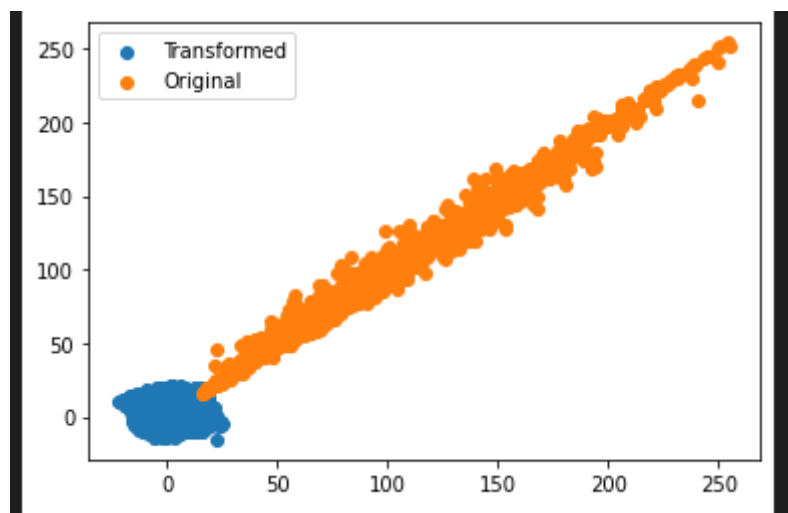


Figure 12: Data transformation

Hyperparameter selection

K as the only hyperparameter in the KNN algorithm, the selection of the K value will have an intuitive and important impact on the prediction results of the final algorithm. Because of complex and large size of Data k = 50 is chosen, too small value of k will easily cause overfit.

KNN method non deep learning method,

Use CMC Curve to get Top1, Top5 and Top10 Accuracy.

The CMC curve comprehensively reflects the performance of the classifier. Its evaluation indicators have the same meaning as the top1 err and top5 err evaluation indicators commonly used in deep learning. The difference is that the Rank on the abscissa represents the correct rate rather than the error rate.

Top1 accuracy is 19%, top 5 accuracy is 23% and top10 accuracy is 27%.

And use plot to show the CMC Curve.

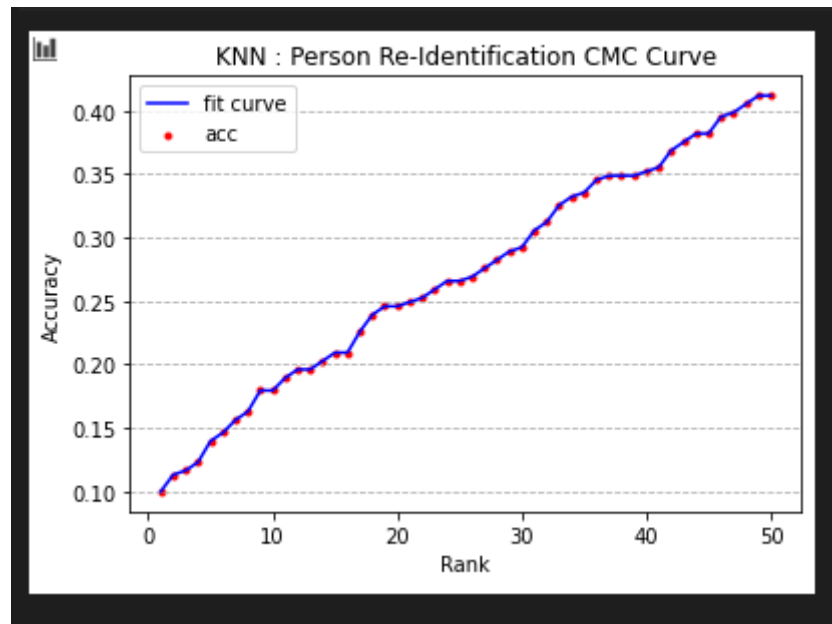


Figure 13: KNN Person Re-Identification CMC Curve

CNN deep learning method

Resnet compare with another CNN deep learning methods, Balduzzi found that even if the mode of the gradient stabilizes within the normal range after BN, the correlation of the gradient decays continuously as the number of layers increases. It has been proven that ResNet can effectively reduce the attenuation of this correlation. Resnet provide higher accuracy with more layers compare with “network”. (David Balduzzi, 2017)

Figure 14: CNN deep learning method layers printout

10 layers of Resnet achieve Top-1 accuracy is 31%, Top-5 accuracy is 52%, and Top-10 accuracy is 62%, 20 layers of Resnet is applicable, Top-1 accuracy is 46%, Top-5 accuracy has achieved 54% and Top-10 accuracy achieve 68%. The outcome has significant results, which matched in the most cases. Thus, compare with other CNN learning method, Resnet achieve significant results when number of layers has increased, other CNN learning method accuracy decrease when layers numbers too high.

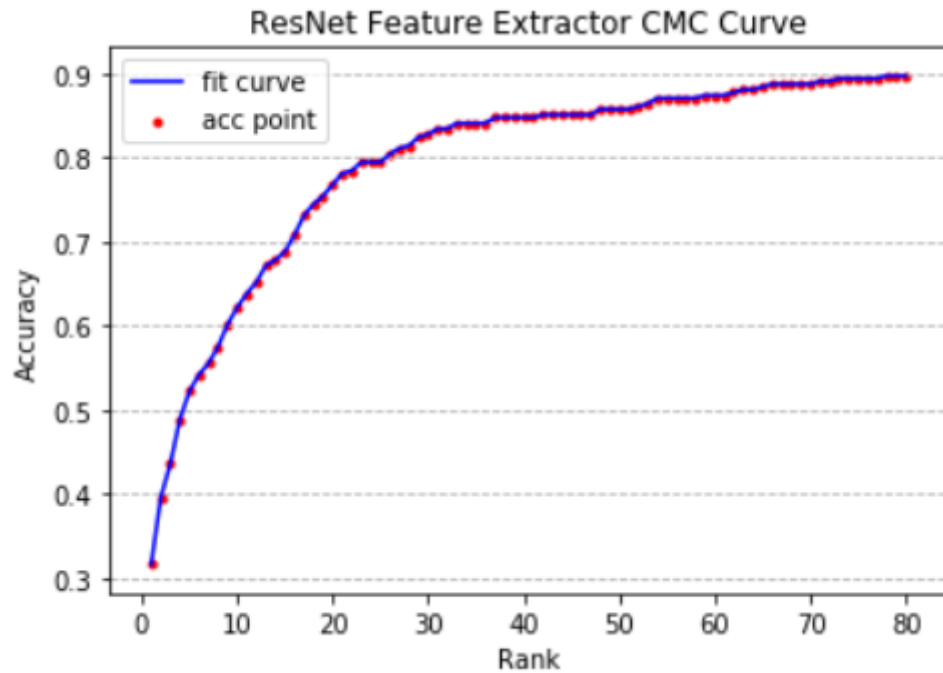


Figure 15: ResNet Feature Extractor CMC Curve

Comparison of deep and non-deep methods

Firstly, Deep learning method needs a lot of matrix calculation, thus deep learning method takes much more times compare with non-deep learning method also more relies on hardware performance.

Secondly, the accuracy of non-deep learning depends on the accuracy of feature processing. An excellent feature processor can significantly improve the accuracy of non-deep learning. However, making a feature processor relies on a lot of professional knowledge. When the data complexity increases, and the variables increase the production of feature processors will become very complicated. But deep learning attempts to obtain high-level features directly from data. This is the main difference between deep learning and traditional machine learning algorithms. Based on this, deep learning reduces the work of designing feature extractors for each problem.

Finally, when the amount of data is small, the performance of deep learning is not good, because deep learning algorithms require a large amount of data to understand the patterns contained therein. Thus, due to different problem-solving methods, deep learning and non-deep learning are suitable for different fields.

References

David Balduzzi, M. F.-D. (2017). The Shattered Gradients Problem: If resnets are the answer, then what is the question? *Proceedings of the 34th International Conference on Machine Learning* (pp. 70:342-35). Sydney, NSW, Australia: Proceedings of Machine Learning Research. Retrieved from <http://proceedings.mlr.press/v70/balduzzi17b.html>

Appendix Code