EE 569 HOMEWORK VI

Royston Marian Mascarenhas

**Feedforward CNN Design**

**(a)**

**FF CNNs**

A Feed Forward Convolutional Neural Network (FF CNN) does not use back propagation to optimize the kernels of the convolutional layers. Therefore, it has less chance for error since the cost function of the output is not taken into consideration. Thus, the algorithm relies heavily on the information of the training data. In this rigorous data centric approach, the layer tries to extract not just spatial but spectral information too from the training data to gain a sharper insight into the features that connect that data point to a particular class. The network parameters are derived during the forward pass, from the statistics of the previous layer output.

Let’s start building the FF CNN from the ground up.

**Prerequisites**:

1. Neuron

The neuron is best explained by the following figure:

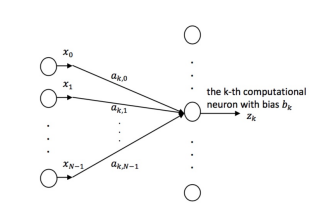
x

y = ax + b

add b

It can be divided into the affine component and the bias component. The input is a data point or a vector with N features or dimensions.

If N data points are taken into consideration, then we get the first layer of a neural network. It is visualized below:



Mathematically, it is expressed as



The output of this layer is fed to an activation function to enhance interpretability by introducing non linearity. ReLu output is expressed mathematically as the function which drops negative components and does nothing when it iterates over positive components.



1. Non-linear activation:

Non linear activation helps differentiate between two patterns of opposite polarity. This is know as the **sign confusion problem.** Without non linear activation, the output from the convolution will nullify the difference in polarity. Since the negative outputs will be stemmed by ReLu, non linear activation helps eliminate lack of ambiguity between foreground and background of similar but complementary images. Another technique employed to override the sign confusion problem is the SAAK transform which splits positive/negative correlations into two channels. Since the computational cost increases due to the presence of two channels, the SAAB transform is used instead.

1. Span of anchor vectors:

Anchor vectors are those vectors which are determined during training and remain unchanged during the testing process. They can be thought of as correlators. If the feature and the weight are highly correlated, then the response is small and vice versa. These extract patterns from the input by thresholding. The span of the anchor vectors can be thought of as output vectors which are projections of input vectors into the weight space. If the subspace can be determined by PCA, the anchor vectors can in turn be calculated. Note that this prerequisite assumes zero bias term.

**Feedforward design of convolutional layers:**

The CONV layer design includes the following essential concepts:

**Spatial Spectral Filtering:**

1. Just spatial filtering is not enough. In CNNs, as the layers go deeper, the receptive field focuses on a particular spatial section of the input but the resolution is lost. The solution to this is to find a spectral representation of the neighbourhood through PCA to extract dominant stroke patterns. These are called anchor vectors.
2. Image representations and transforms are distinguished with the help of spectral aided spatial representations

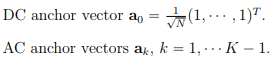
**Larger output:**

Neglecting the boundary effect, if each pixel is involved in filtering, then the output is larger than the input by a factor of K. While this might hinder faster run time, it provides a more diverse feature set.

**Saab Transform:**

The SAAB transform is a process of selection of anchor vectors, which comprise of AC and DC components.

**Selecting anchor vectors:**



The DC and AC components of the anchor vectors are configured as above. As a result, the input vector space is a sum of the subspaces of the two components.

The relation between the AC an the DC components is:



where



The anchor vectors are obtained by selecting the first (k-1) principal components of the result of PCA applied on input vectors belonging to the AC subspace.

**Bias Selection:**

The conditions for selecting bias are that all bias terms should be equal and they should be more than the maximum component of the input vector so when the bias is added, all the terms in the input vector are positive. This second constraint simplifies the design and computation.



**Spatial Pooling:**

This helps in

1. picking the best filter responses
2. reducing computation
3. optimizing storage
4. deviant visual patterns are supressed

Together, convolution and pooling can be thought as projecting the input into the space spanned by the anchor vectors. Together, spatial filtering, spectral interpretation and max pooling can capture similar but spatially translated patterns.

**Compound filters:**

The collection of features extracted by the convolutional layers are the outputs of compound filters. In feed forward CNNs, the target is a linear combination of orthogonal PCA filter responses, which correspond to receptive field extractions.

**Feed forward design of fully connected/dense layers.**

* In FF CNNs, each FC output is a linear LSR. As a result, we get a one hot encoded output of the dense layer as that is the output of a linear least square regressor.
* Due to the lack of labels, we use k-means and classify the output space into a number of clusters. Once we have the new label and the original label, we further classify each cluster into a set of clusters. This is done to accommodate the diversity of each class. This process is known as **pseudo label generation.**
* In the Le-Net 5, we do k-means clustering to obtain a 120 one hot encoded vector with 10 final classes and 12 clusters within main clusters.
* The LSR ensures that all samples are mapped to the unit target vector itself and not any other target vector (another class with its own pseudolabels).
* Leakage of information happens when similar features lead to mapping from one pseudo space to the other, leading to faulty classification.
* The densely connected layers take the inputs from the conv layers and align the feature spaces corresponding to input and output. This is carried out to reduce the cross entropy and introduce more variance in each feature, resulting in more discriminating power.

Now that we have explored the concepts, let us build the process.

**Network architecture:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Layer** | **Interpretation in FF CNN** | **Original LeNet output sizes and configurations** | **Modified Le-Net**  **configurations** |
| CONV | SAAB (AC and DC) coefficient convolution | 28 x 28 x 6 (5x 5 AC filters, totally 5 in number and 1 DC filter) | 5 x 5 x 3 |
| Max Pooling | Max Pooling | 14 x 14 x 6 | 32 |
| Bias addition | Bias addition | 14 x 14 x 6 |  |
| CONV | SAAB (AC and DC) coefficient convolution | 10 x 10 x 16 (5x 5 AC filters, totally 15 in number and 1 DC filter) | 5 x 5 x 32 |
| Max Pooling | Max Pooling of only AC responses | 5 x 5 x 15 | 64 |
| No Bias Addition | No need since the FC layers adopt a different approach. |  |  |
| First FC Layer | Least Square Regressor | One hot encoded output with 120 columns | One hot encoded output with 200 columns |
| Second FC Layer | Least Square Regressor | One hot encoded output with 84 columns | One hot encoded output with 100 columns |
| Output layer | Least Square Regressor | One hot encoded output with 10 columns | One hot encoded output with 10 columns |

**Flow Chart:**

**Differences**:

|  |  |
| --- | --- |
| **BP CNN** | **FF CNN** |
| **Background** | |
| Works on **optimization** of a cost function | Works on retrieving **data** statistics from previous layer to compute parameters of next layer |
| The mathematical core of BP CNN is **non convex optimization**. Once the cost function is computed, its gradient is plotted and an optimization algorithm is used to find the global minimum. Since this is non convex optimization, the update might get stuck at a local minimum and there might be a need to use momentum. | The mathematical flesh of an FF CNN relies heavily on **linear algebra and statistics**. The convolution is based on PCA and it aids discriminant analysis and reduction of the features. One advantage it has over the non convex optimization is that the vanishing gradient problem does not occur in this data centric approach. |
| **Structure and Perception** | |
| The BP CNN utilizes information from the input and the output. The input has an effect on the initial layers and the output decision space has an effect on the final layers. It is **end to end coupled**. | The FF CNN is split explicitly into two modules. The **data representation module** is formed by the PCA based convolutional layers. The **decision making module** is formed by the LSR densely connected layers. |
| BP CNNs **are hard to interpret** because of the mathematical density that develops with each layer. | FF CNNs are mathematically **clear and concise.** Therefore, they are easier to understand. |
| To ensure end to end connectivity and optimization, the BP design has a **constraint** on its layers. The FC layers have to be ANNs. | There is **no such constraint** in FF CNNs. The LSRs can be replaced by SVMs, random forests or another classifier. |
| **Complexity** | |
| The BP algorithm might have to run for several **epochs** for it to converge. With increase in data size or dimensionality, the **convergence might take a lot of time.** | The complexity can be mitigated in FF CNNs. The covariance might converge in a single epoch in some cases since the training image provides **several training patches**. Moreover, the **correlation** between the training images and the patches **can be statistically manipulated to further lower the complexity.** |
| **Versatility** | |
| For any task such as detection, tracking, segmentation, different CNNs will have to be designed because of differing cost functions. | Since this approach is data centric, the same CNN can be used for all tasks. The only part we might need to change is the setting for the FC layers. Information from different such techniques can be then combined to build one system rather than several networks. |
| **Performance** | |
| Optimization aids state of the art performance only if the network configurations are directly related to the problem statement at hand. | The performance can be boosted by ensemble learning since multiple classifiers can be constituted by several convolutional layers. |
| **Overfitting** | |
| The number of learning variables might lead to overfitting. However, there are several regularization methods such as dropout and early stopping which can help reduce overfitting. | In FF CNN, the degrees of freedom are not directly related to the model parameters. The weights in the deeper layers bank on those in the shallower layers. Since the weights of the CONV layers are determined by PCA of the input data to that layer, there is a direct correlation between the weights and the training data. Therefore, once the covariance matrices are identified, we can find the filter coefficients. i.e if the input of the first conv layer is 5 x 5 and the second conv layer is 5 x 5 x 6 the covariance matrices are of dimensions 25 x 25 and 150 x 150. For the FC layers, the dimensions of the LSR matrix is approximately the product between the input and the output dimensions. |
| **Discriminating power using signal analysis** | |
| Cross entropy is used to approximate the discriminating power of features. In BP CNN, the cross entropy of the first two CONV layers is much lower than that of the FF CNN. As the layers go deeper, the cross entropy decreases and the correlation in the information becomes more transparent. | The cross entropy for a FF CNN is higher than that of a BP CNN in the initial CNN layers but it decreases drastically in the FC layers. As a result, it has more orthogonality, less redundancy and wider information (broad band) flow. |

**Similarity:**

FF CNNs and BP CNNs are similar in their core structure. They use different implementations of a convolutional, max pooling and densely connected layer but the types of layers are the same. Both use the basic neuron structure and activation functions. FF CNN has no back propagation but it derives information from the forward pass. Both the BP and the FF CNN use the forward pass. Each CNN layer corresponds to a vector a matrix transformation in both cases. Although FF CNN is more statistic based, BP CNN is also data centric in the sense that it relies on vast amount of input features for best discrimination rather than just mathematical processes. In both types of CNNs, the spatial resolution reduces as the network goes deeper. In both CNNs, each dimension of the output refers to a class label. There are similar tunable parameters in either. Both have adjusted filter weights or learning parameters. Both are vulnerable to adversarial attacks when the model is fixed.

**(b)**

**Reconstruction using SAAB coefficients**

1. **Abstract and Motivation:**

The SAAB filters are used to obtain a statistical input to the CONV layer on the basis of its principal components and adjusted bias. The images, once feature encoded by SAAB can also be reversed.

1. **Approach and Procedures:**

*The approach followed here is:*

1. Load the number of layers and iterate from the deeper layer to the shallower layer
2. Obtain the kernel and the its inverse to resuscitate the transformed kernel. This is akin to the inverse PCA step.
3. If outermost layer, the samples have bias. Remove the bias by subtraction.
4. For both layers, revive the sample patches by reverse computation.
5. Subtract the feature expectation from the sample patches.
6. One last step is to perform dimension rearrangement to obtain the original patches.
7. Reshape to input image.
8. **Results:**

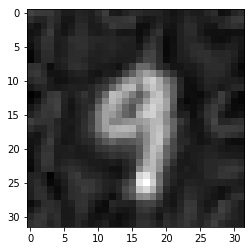
*Note that the dc component is discluded in the final number of filters.*

**PSNR values are given right below the image**

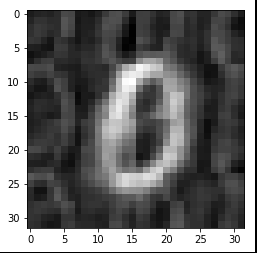
**Setting 1:**

**Number of filters in first layer: 5**

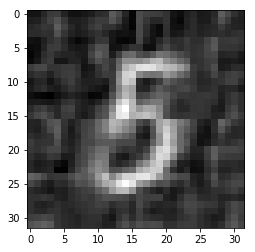
**Number of filters in second layer: 15**



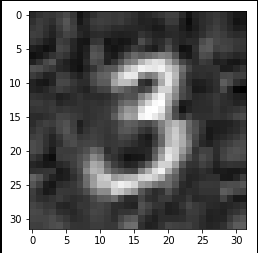
PSNR is 18.689149275274442 dB



PSNR is 16.63590590259514 dB



PSNR is 17.672289033793966 dB

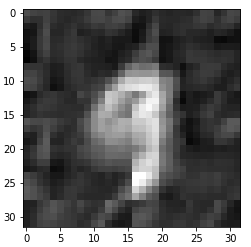


PSNR is 18.02334031191759 dB

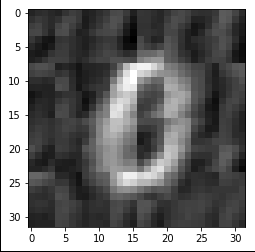
**Setting 2:**

**Number of filters in first layer: 5**

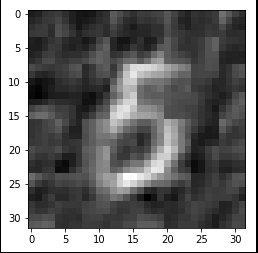
**Number of filters in second layer: 11**



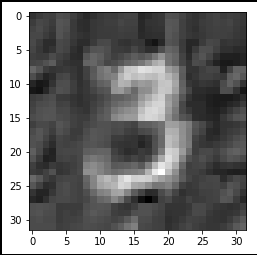
PSNR is 16.915136739446133 dB



PSNR is 15.856383840864002 dB



PSNR is 16.59938529803895 dB



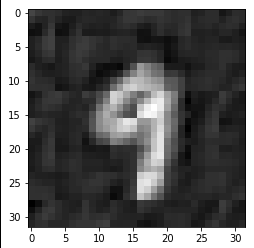
PSNR is 16.0894213600736 dB

**Setting 3:**

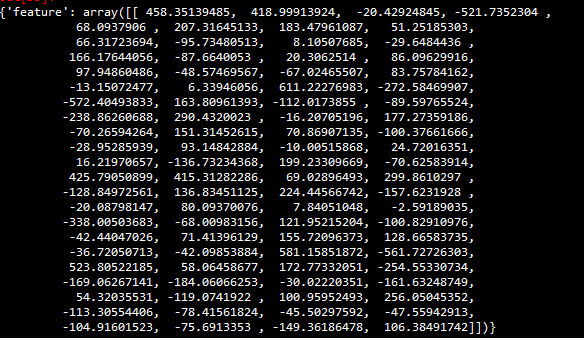
**Number of filters in first layer: 3**

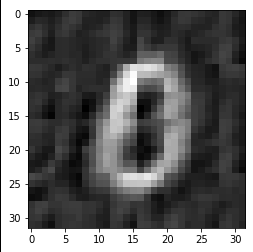
**Number of filters in second layer: 21**

Feat refers to SAAB coefficients. They are in the shape 2x2xsecond stage kernel number but they are displayed in the form 1x(2x2xsecond stage kernel number)

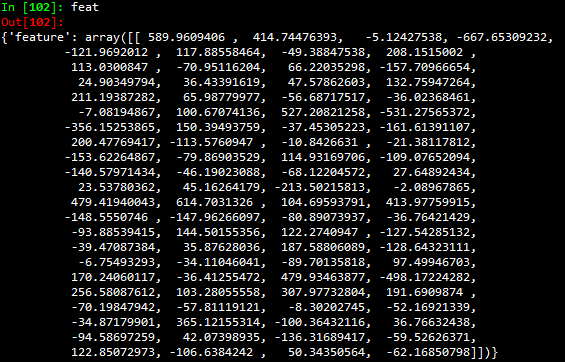


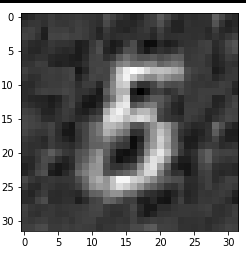
PSNR is 18.914979472919452 dB



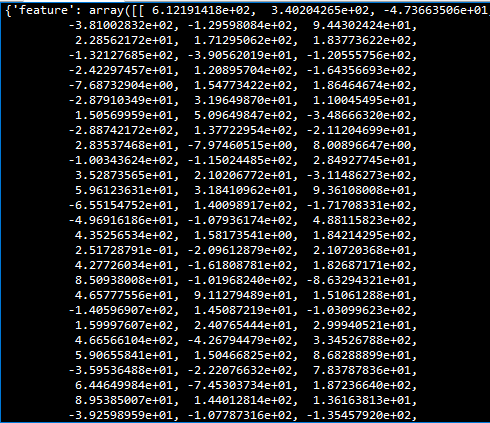


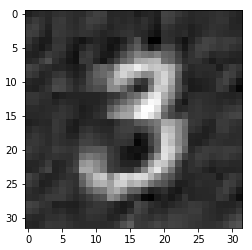
PSNR is 16.89226757315203 dB



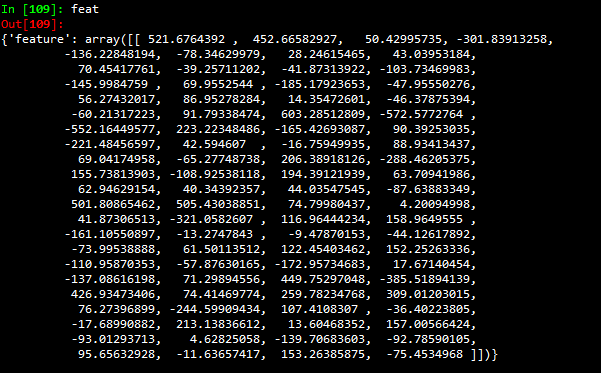


PSNR is 18.086554001146062 dB





PSNR is 17.763986201525718 dB

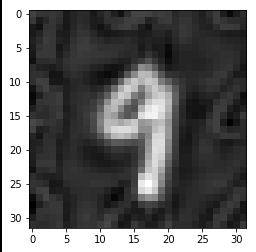


**Setting 4:**

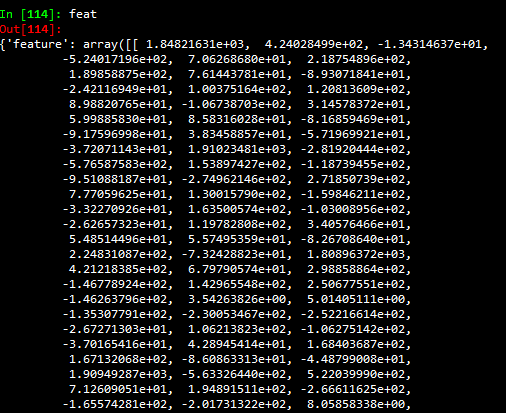
**Number of filters in first layer: 14**

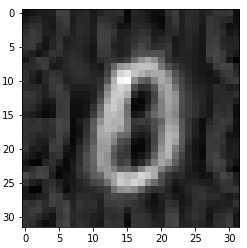
**Number of filters in second layer: 22**

Feat refers to SAAB coefficients. They are in the shape 2x2xsecond stage kernel number but they are displayed in the form 1x(2x2xsecond stage kernel number). Here, the numbers include the dc components of the filters.

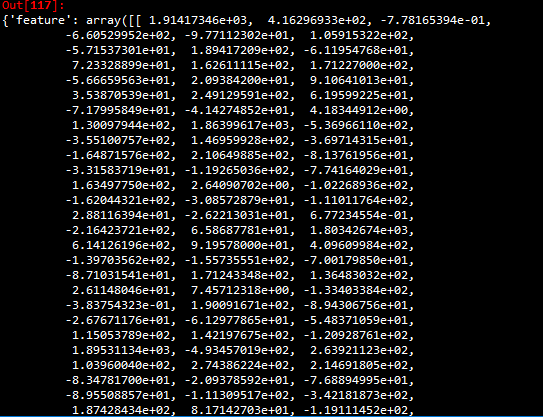


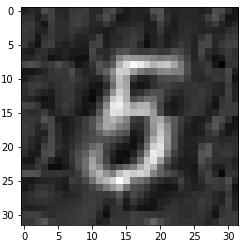
PSNR is 20.608254115070906 dB



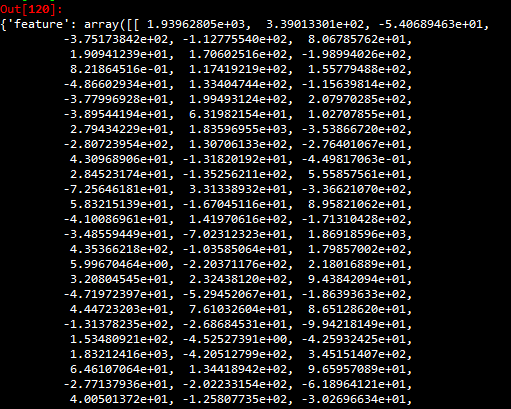


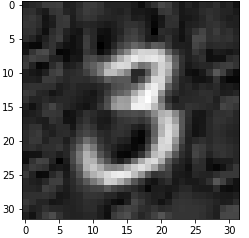
PSNR is 17.773702314861374 dB



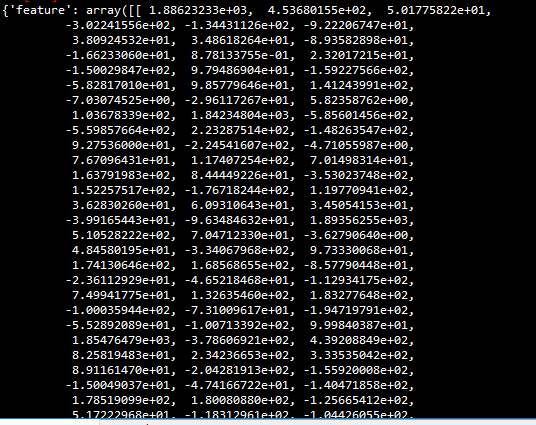


PSNR is 19.017636874705914 dB





PSNR is 19.389316286452946 dB



1. **Discussion:**

* Note that the reconstruction offers a good approximation to the original image.
* If the number of kernels filters are decreased in both the layers, then there is loss of information for sufficient statistics and therefore, there is a drop in the PSNR as can be observed from setting 2.
* In setting 1, the standard for the PSNR value is set. The other settings are compared to this setting.
* In setting 3, we can see that the number of second layer filters has been increased, which is supposed to increase the fine detail information encoded in the features because it is the deeper layer but the results are not very encouraging as the increase in second layer CONV filters is of not much use as the general features are not exploited by the first layer filters which are only 3 in number. As a result, we observe stagnant PSNR growth over this promising setting.
* In setting 4, the increase in filters in both the layers boosts the PSNR by about 2.5 dB as more information is extracted by the filters. As a result, the principle components are richer and the reconstructed images are more faithful to their original constitution.

**(c)**

**Ensembles of FF CNN Design**

1. **Abstract and Motivation:**

Since FF CNN is more data centric than optimization based, more statistics will help augment the accuracy of the system. Therefore, the ensemble model is used to include model diversity so that better predictions can be made.

1. **Approach:**

The algorithm used in this case is :

1. Run the FF CNN algorithm for different values of number of filters, kernel sizes and different law filters.
2. In each case, record the training accuracy and the testing accuracy.
3. Save the weights and features produced by the algorithm.
4. Once all ten settings are complete, merge all features horizontally so that a lot of discriminating power is created.
5. Use PCA to reduce the dimensionality of the data stack in order to speed up the system.
6. Feed the data and the features to a classification algorithm, in this case, SVM.
7. Note the output scores of the ensemble algorithm.
8. **Results:**

**Section 1 :Individual accuracies for training and testing:**

Settings adopted (The stride is taken 1 in all cases):

Note that the number of filters in each CONV layer as mentioned below ignores the (+1) filter (DC component). In actuality, in setting 1 for example, the number of filters in each layer are 6,16. In some cases, like the later settings, lower number of filters are taken because of strain on computational resources.

1. Kernel Size (layer 1, Layer2): 5 x 5, 5 x 5

Number of filters in CONV layer 1: 5

Number of filters in CONV layer 2: 15

1. Kernel Size: (layer 1, Layer2): 5 x 5, 5 x 5

Number of filters in CONV layer 1: 3

Number of filters in CONV layer 2: 13

1. Kernel Size: (layer 1, Layer2): 5 x 5, 5 x 5

Number of filters in CONV layer 1: 5

Number of filters in CONV layer 2: 11

1. Kernel Size: (layer 1, Layer2): 5 x 5, 3 x 3

Number of filters in CONV layer 1: 5

Number of filters in CONV layer 2: 15

1. Kernel Size: (layer 1, Layer2): 3 x 3, 3 x 3

Number of filters in CONV layer 1: 5

Number of filters in CONV layer 2: 15

1. Kernel Size: (layer 1, Layer2): 3 x 3, 5 x 5

Number of filters in CONV layer 1: 5

Number of filters in CONV layer 2: 15

1. Kernel Size: (layer 1, Layer2): 3 x 3, 3 x 3

Number of filters in CONV layer 1: 7

Number of filters in CONV layer 2: 17

1. Kernel Size: (layer 1, Layer2): 5 x 5, 5 x 5

Number of filters in CONV layer 1: 3

Number of filters in CONV layer 2: 11

**E5S5 Law filter application**

1. Kernel Size: (layer 1, Layer2): 5 x 5, 3 x 3

Number of filters in CONV layer 1: 3

Number of filters in CONV layer 2: 11

**Neighbourhood addition**

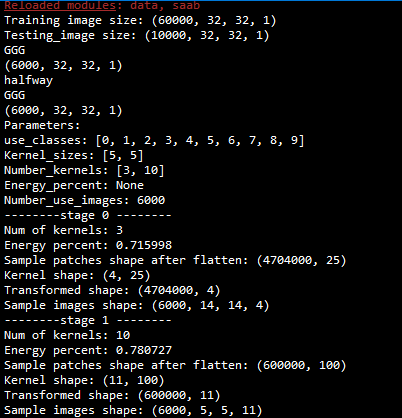
1. Kernel Size: (layer 1, Layer2): 5 x 5, 3 x 3

Number of filters in CONV layer 1: 3

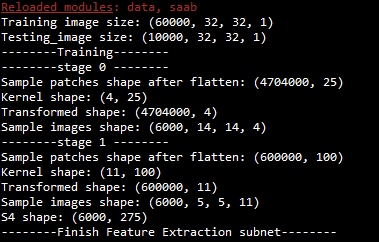
Number of filters in CONV layer 2: 10

**E5E5 Law filter application**

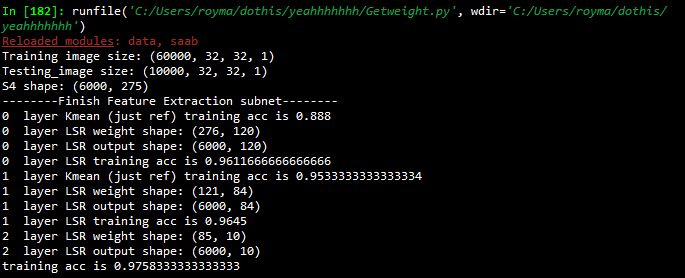
|  |  |  |
| --- | --- | --- |
| **Setting** | **Training Accuracy** | **Testing Accuracy** |
| 1 | 98.23 | 96.33 |
| 2 | 95.84 | 95.2 |
| 3 | 97.76 | 96.2 |
| 4 | 98.51 | 96.24 |
| 5 | 98.3 | 96.55 |
| 6 | 98.6 | 96.47 |
| 7 | 98.68 | 95.37 |
| 8 | 97.55 | 95.7 |
| 9 | 97.51 | 96.31 |
| 10 | 97.58 | 95.6 |



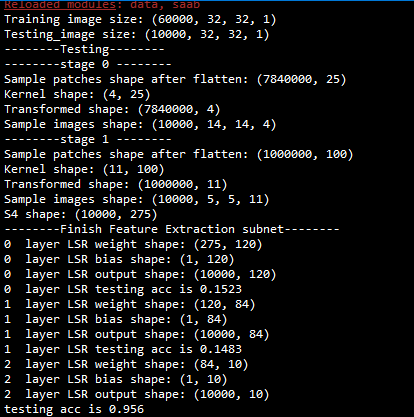
*Sample run of setting 10 in GetKernel*



*Sample run of setting 10 in GetFeature*



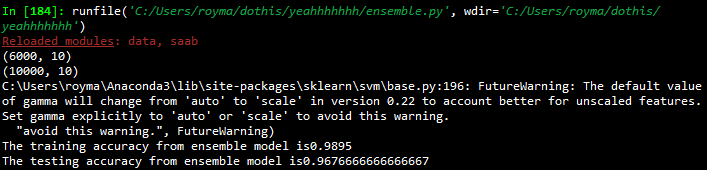
*Sample run of GetWeights*



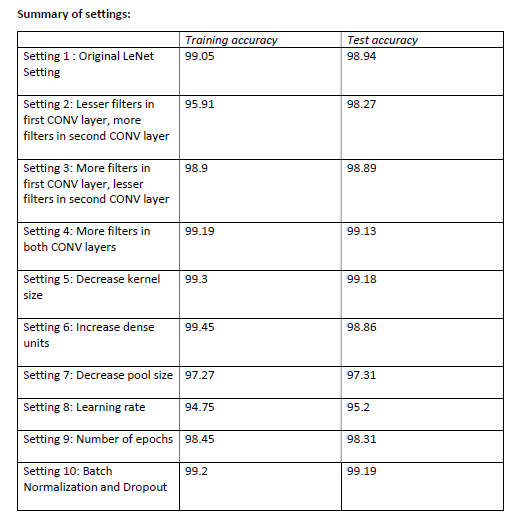
*Sample run of MNIST test*

**Section 2: Ensemble Results**

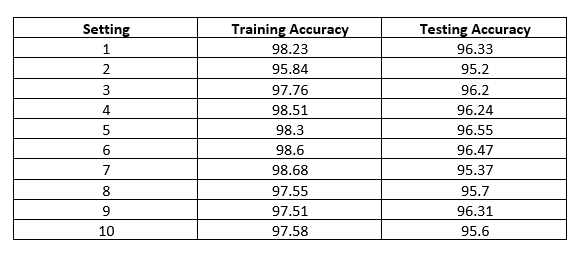
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Addition of different settings to ensemble model** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **Training accuracy** | 87.83 | 97.6 | 97.76 | 98.51 | 98.38 | 98.43 | 98.58 | 98.66 | 98.9 | 98.95 |
| **Testing accuracy** | 82.43 | 93.8 | 94.31 | 96.24 | 95.21 | 95.48 | 95.6 | 95.99 | 96.58 | 96.76 |



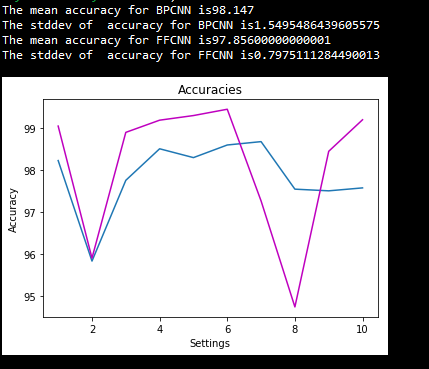
**Section 3: BP CNN and FF CNN performance:**



**Accuracies from BP CNN HW 5**



**Accuracies from FF CNN**



***The magenta line is BP CNN and the blue line is FF CNN***

**4.Discussion:**

1. Note that the complete set of 60000 images could not be handed in for training. Fewer images were input due to heavy strain on computational resources (the system crashed eleven times). Since FF CNN does not work on the basis of optimization and as is mentioned in the official paper, it is mentioned by experiment and proof that the convergence is much faster due to abundance of training patches and statistical correlation. Therefore, a very certain, direct line cannot be drawn between BP CNN executed in the past project since it had the luxury of several epochs and the complete dataset.
2. The accuracy for the FF CNN follows a similar pattern as it corresponded to BP CNN.
3. With increase in number of kernels, the accuracy increases.
4. With decrease in initial kernel filters and increase in final kernel filters, the accuracy varies depending on the task. If the generalizability is more, such as different types of animals, the initial number of kernels will not affect the accuracy as opposed to the case when the task is specific such as different types of cat. That is when the number of second layer kernel filters is more.
5. The ensemble model is used to boost the diversity of the model. Since FF CNNs rely heavily on statistics, more discriminability helps in increasing accuracy.
6. As the number of settings added increases, as can be noted from the table in the results section, the features added from the settings enhances the accuracy of the overall model.
7. Computation wise, the FF CNN requires fewer epochs to converge but the computations are on the large scale (huge matrix operations) as opposed to a multitude of small scale neuron level calculations in BP CNNs. With increase in the number of filters in both the CONV layers, the decrease in kernel size and stride, the algorithm becomes computationally more complex and therefore requires much more time to run.
8. As can be noted from the table of accuracies, setting 1 had optimal parameters, resulting in good accuracy.
9. Setting 2 had less number of filters, which had lesser run time, but costed information.
10. Similarly, the other settings correspond to the explanation above.
11. Laws filter application was used to enhance the diversity of the model. However, in the individual case, it did not result in the best accuracy, as opposed to the ensemble case, where it boosted the model.
12. Performance wise, we can see that BP CNN has a lot of constraints on its implementation whereas in this homework, I implemented FF CNN FC layers using Least Square Regressors and also SVM.
13. The accuracies were more for BP CNN since it had access to the complete dataset and is end to end optimized. The FF CNN has only used a certain set of statistical methods but if more were to be leveraged, it would reduce the run time and increase the efficiency.
14. The FF CNN is not task based since it depends on the statistics. The same model can be used for another problem. However, a different BP CNN will have to be designed.
15. The performance of the BP CNN, in the fine scale, depends on random initializations and the momentum of optimization, therefore, it has more standard deviation from an FF CNN since the statistics of the data helps center the accuracy.
16. **Improvements** that can be made to BP CNN include adding additional layers in between the traditional CONV and the FC layers which help select or boost the features more depending on the statistics of the dataset such as selective dropout based on performance of a neuron or batch normalization based on performance of the previous layer. Additions to the layer must be made optional depending on the efficiency of the previous layer.
17. **Improvements** that can be made to FF CNN include using more statistical techniques such as rejection sampling to monitor information gain, MCMC for statistical optimization in the forward pass since it is more data centric than non convex optimization.

**References:**

1. Interpretable convolutional neural networks via feedforward design. Journal of Visual Communication and Image Representation. C.C. Jay Kuo
2. Kuo, C. C. J. (2019). Ensembles of feedforward-designed convolutional neural networks.

**Thank you!**