Ensembles and Cascading of Embedded Prototype Subspace Classifiers

Anders Hast and Mats Lind
Department of Information Technology
Uppsala University
SE-751 05 Uppsala, Sweden
anders.hast@it.uu.se; mats.lind@it.uu.se

ABSTRACT
Deep learning approaches suffer from the so called interpretability problem and can therefore be very hard to visualise. Embedded Prototype Subspace Classifiers is one attempt in the field of explainable AI, which is both fast and efficient since it does not require repeated learning epochs and has no hidden layers. In this paper we investigate how ensembles and cascades of ensembles perform on some popular datasets. The focus is on handwritten data such as digits, letters and signs. It is shown how cascading can be efficiently implemented in order to both increase accuracy as well as speed up the classification.

Keywords
Subspaces, Ensembles, Cascading, Embedded Prototypes, Neural Networks, Deep Learning.

1 INTRODUCTION
Recently, deep learning based methods [Sha18], have shown tremendous performance in the area of handwritten text recognition [KDJ18, DKMJ18, SF16]. Nevertheless, there are a few problems and challenges that still need to be addressed. First of all these methods usually require powerful GPU resources in the training process, not at least because of the back propagation in numerous epochs, which makes them very time consuming. Secondly, the learning process of a deep neural network can be regarded as a black-box [CPC19]. Furthermore, the learning mechanism is not easy to comprehend nor to visualise, because of the many hidden layers. This is know as the interpretability problem [Kri19, CPC19] and in order to find a solution the field of explainable AI (XAI)[ADRS19, GSC19, CPC19] has emerged.

A new kind of learning process together with a well researched classification method [KLR77] was recently proposed [HLV19] called Embedded Prototype Subspace Classification (EPSC), which go beyond the black-box deep neural network. It is a mathematically well-defined neural net based on subspaces (or manifolds) aimed at classification of handwritten letters, which is both easy to interpret, explain and visualise. This method is an especially interesting alternative when speed is crucial since it is not based on back propagation and therefore does not require an iterative training procedure. Even if it not always beats the state of the art, it comes close enough to be an interesting alternative due to its interpretability and compactness, having just one input layer and one output layer with no hidden layers.

In this paper we present how ensembles of EPSC can be set up in such a way that classification can be done in an efficient manner. Cascading is used to progressively exclude nodes in the resulting neural network that cannot contribute to the correct classification. The idea is to make classification faster without compromising accuracy.

2 BACKGROUND
The first application of subspaces in pattern recognition was proposed by Watanabe et al. [WP73] in 1967, and later further developed [WLK67], by Kohonen and others [KLR77, KO76, KRMV76, OK88]. The idea of the later approaches of subspace learning was to choose some group of prototypes for the construction of each subspace. This was done by searching for the k nearest neighbors in feature space, which is a rather time consuming process. In the following subsections a more efficient and accurate procedure is explained.
2.1 Embedded Prototype Subspace Classification

The idea of EPSC [HLV19] was to use t-distributed stochastic neighbour embedding (t-SNE) [MH08] to find representative clusters in 2D image space by applying kernel density estimation (KDE) [CHTT96] and a so called inverse watershed transform (IWS) [RM00, VS91], which is simply the watershed transform on an inverse image. Therefore, *valleys* between mountain tops are found in the image rather than the *drainage divide* that separates adjacent drainage basins, also known as watersheds.

The t-SNE is a machine learning technique that reduces the number of dimensions of high dimensional data to 2 or 3 dimensions. Clusters are formed since it strives to maintain a representation of similarities among features, so that similar features are represented as points closer to each other and dissimilar points further away from each other.

PCA [WEG87] is used both as an intelligent start guess for t-SNE in order to make the process deterministic, but also for generating each subspace [Laa07]. By computing the norm of the projected feature vector to be classified into each subspace, the process can be regarded as a two layer neural network [OK88, Laa07], where the weights are mathematically defined through PCA. Another important advantage is that the learning process can easily be visualised, which makes it easy to understand, interpret and explain compared to most state of the art deep learning approaches.

2.2 Clustering

The main idea behind clustering, or cluster analysis, is to group data that are in some sense similar into separate clusters. Usually some kind of distance function is used to group similar data points together [JMF99]. Clustering is a common technique for exploratory data mining and analysis, and is used in many fields, including machine learning, pattern recognition, image analysis, machine vision and its applications [JMF99].

The selection of an appropriate clustering approach is indispensable for the performance of a machine vision task [XW05]. Clustering can be done in many ways, and a variety clustering algorithms have been proposed in literature, such as k-means [HW79] and DBSCAN [EKSSX96]. These algorithms require the user to set the number of clusters to be found, while others, like Mean-Shift [CM02, FH75] finds the number of clusters depending on the size of the Gaussian Kernel chosen. Just as in [HLV19], it was chosen to perform clustering in image space in order to easily be able to visualise it as the learning process proceeds. Nonetheless, the method used is producing a similar result as Mean-Shift.

2.3 Kernel Density Estimation

Kernel Density Estimation (KDE) [CHTT96] can be performed by splatting Guassian discs onto an image, for each point in the dataset. The size $d$ of each disc can be set in a similar way as the kernel size for Mean-Shift. However, since KDE and IWS work in image space, the result can easily be visualised. It was chosen in [HLV19] to use the Silverman’s rule of thumb as the base level for computing the bandwidth $h$ of the clustering,

$$h = \left( \frac{4\sigma^5}{3n} \right)^{1/5}$$

where $\sigma$ is the standard deviation of $n$ samples.

The KDE surface can be used in a visualisation as a visual aid to identify clusters, but is also used as the basis for the IWS. By multiplying $h$ by a scale factor, it is possible to vary the number of clusters.

![Visualisation of a subset using one character from the Kuzushiji-MNIST dataset. (a) Visualisation using low resolution. (b) Heatmaps from each cluster. (b) Visualisation using high resolution. (c) Heatmaps from each cluster. The number above the heatmaps tells how many images are superimposed to make the heatmap. Figure best viewed in color.

Figure 1 shows the result of clustering using the character $R$ from the Kuzushiji-MNIST dataset. In Figure 1a) a rather large scale factor $h = 3.0$ is chosen and three main clusters appears representing the three main ways of writing the character $R$. By decreasing the scale factor to $h = 1.0$ more clusters are found as shown in Figure 1c) and the heat maps in Figure 1d) reveal more variation among the individual characters. In Figure 2 all characters from four different clusters are depicted. Each cluster contains rather similar ways
By projecting the vector \(\hat{x}\), using all vectors in the subspace through

\[
\hat{x} = \sum_{i=1}^{n} (x^T u_i) u_i
\]  

(4)

\[
= \sum_{i=1}^{n} \rho_i u_i
\]  

(5)

\[
= U^T U x^T
\]  

(6)

Since all the vectors in \(U\) are normalised, the norm of the projected vector can be simplified as

\[
||x||^2 = (U x^T) \cdot (U x^T)
\]  

(7)

\[
= (U x^T)^2
\]  

(8)

\[
= \sum_{i=1}^{n} \rho_i^2
\]  

(9)

Therefore, the feature vector \(x\), which is most similar to the feature vectors that were used to construct the subspace in question \(\mathcal{L}_{U_i}\) will subsequently also have the largest norm \(||x||^2\).

3. CASCADING AND ENSEMBLES

Cascading [GB00], first introduced by Viola and Jones for face detection [VJ01] can be regarded as a special case of ensemble learning [OM99, Rok10]. It is based on the concatenation of several classifiers rather than combining the result of multiple classifiers in order to obtain a better result. The idea is that further processing is done only on tentative classes and non-relevant classes are progressively excluded. By implementing cascading for a neural network, the overall workload will not only decrease, but in some sense the network will mimic what humans do. When being presented to a classification problem a person often instantly see the correct answer, i.e. when being sure enough, no further examination is necessary and therefore we sometimes naturally make use of what is known as early termination. However, sometimes a person have to take a closer look and choose from two or more tentative answers by scrutinising the images further, e.g. “is the number a 5 or a 6?”. Hence, the decision has already been made that it cannot be any other number. Such closer examination helps in making a more accurate classification and therefore humans also deploy the strategy of cascading in such cases.

3.1 Ensembles

Ensembles can be setup in several ways, and here was chosen to use four EPSC networks working on the very same test data images but using four different variants of features that are extracted from the images. Hence, the t-SNE will create a bit different looking clusters depending on what kind of image features the different features extractors are focusing on.
3.2 Features

The features used herein are handcrafted in order to be faster than learned features from CNN’s. They were made from different combinations of HoG [DT05] and combinations of some of the most significant elements of the magnitude of the FFT (subsequently referred to as mFFT), i.e. low pass filters, [MHWS17] of different parts of the image and also in combination with down scaled versions of the image itself. These were made ad hoc through experiments in order to find good features yielding both high accuracy used alone, but also used together in an ensemble. In the paper introducing EPSC [HLV19] a similar approach, using a combination of HoG and a down scaled version of the image, achieved an accuracy of 99.2%, i.e. error of 0.8%. As shown in table 1 using mFFT helped lowering the error below that error for all features.

Feature 1 was setup by combining two HoG features with different cell size and five mFFT features from five different partitions of the image. The second Feature is a combination of one HoG and eleven mFFT of eleven different partitions. The third feature is a combination of one HoG, five mFFT and the image itself down scaled to a quarter of its size. The fourth feature is a combination of one HoG and five mFFT.

3.3 Cascading

The cascading was setup in six stages as visualised in Figure 3. In the first stage a rough estimation on feature 1 is done by using a rather large scale parameter $h = 2.5$ for clustering, which will produce a quite small neural net that produces good enough results to distinguish with a high probability the (obvious) false positives from the tentative true positives.

In the second stage, one net (still using the same feature) evaluates only the top five candidates in a more accurate but larger net that was produced by using a smaller scale parameter $h = 0.5$ in order to get smaller clusters. Hence, only the parts of the larger net that corresponds to these five candidates need to be evaluated. The lowest ranking candidate is then excluded from further processing. The advantage here is that only one step of t-SNE is used for this particular feature, used in the first two stages, while two different KDE’s are produced. The latter is many times faster than the t-SNE so the overhead is small.

In the third stage, the nets corresponding to the four candidates, evaluates the second and third features. These are summed together in the fourth stage, together with the output of the second stage, and a new ranking is done based on the accumulated results from these three finer nets. The two lowest score candidates are then discarded and in the fifth stage the remaining two candidates are evaluated using the fourth feature and their corresponding nets. Finally, a total accumulated score from all four stages is used to finally determine the class.

The whole procedure is visualised for two examples of non trivial images in Figure 3. Note how the pipeline eventually comes up with the correct answer even if the top candidate is wrong in the beginning of the pipeline.

3.4 Early Termination

If the difference in score between the top candidates at stage 2 or 4 exceeds a certain threshold $\theta$, it can in most cases be safely concluded that the top candidate is already found, since the uncertainty is considered low. If the difference in score on the other hand is low, it means that the nets cannot easily tell which class it is, i.e. the uncertainty is high, and further processing is necessary. Experimentally it was found that a threshold of $\theta = 0.03$ in both stages worked well. However, since stage 4 is the sum of three scores it means that the values compared are higher and the difference generally is higher, which in its turn means that the threshold is in fact set more tight in this stage.

4 METHOD AND DATASETS

This section describes the method used in the experiments and the individual datasets.
Three important questions needed to be addressed. First of all, how much would an ensemble of EPSC improve the classification results? The second is, how much would cascading improve speed and how close to the accuracy of the ensemble could be achieved? Finally, how much would an early termination mechanism affect both speed and accuracy?

First different variants of features where run on MNIST to find good candidates. A combination of HoG and mFFT on the whole image (or partitions of the image) turned out to give better results than just using HoG and a down scaled version of the image. As explained earlier they were made ad hoc in a trial and error process. This means that other features might do better for other types of input data, and we propose this for future research.

Next combinations of four features where run in an ensemble to find what four features actually give the most different classifications in order to diminish the total error in the ensemble.

Finally, the experiments where repeated on the other data sets without changing any parameters or features. This was done in order to determine whether the cascading and ensembles still improves on these datasets.

### 4.1 Datasets

The proposed EPSC framework has been tested on the images from the following datasets:

- The MNIST database of handwritten digits [LCB10], which is the standard benchmark dataset within the machine learning community. It consists of a training set of 60,000 examples, and a test set of 10,000 examples.
- The E-MNIST (MNIST) dataset has the same example and test set sizes as MNIST [CATvS17], but the conversion process tried to optimise the size of each digit.
- L-EMNIST has the same example and test set sizes as MNIST and contains letters (26 in total).
- B-MNIST has the same example and test set sizes as MNIST and contains both letters and digits (47 different in total).
- The Kuzushiji-MNIST (K-MNIST) dataset has the same example and test set sizes as MNIST [CBK18] and contains 10 different Japanese Hentaigana, where each character may possess rather different forms. The letters present in the dataset are あきすつなはまやれを.
- The Fashion MNIST (F-MNIST) [XRV17] dataset has the same example and test set sizes as MNIST and contains miniature images of clothes and bags.

These were chosen for several reasons. First of all most of them contain handwritten numbers and letters, which is of our main interest, except for the F-MNIST dataset that contains miniature images of clothes and bags. Secondly, they all have similar format, making them easy to evaluate for algorithms that have already been tested on the MNIST dataset, which is very well researched for machine learning. Nevertheless, it is a good starting point for understanding how well classification of handwritten text can perform.

### 5 RESULTS

Table 1 shows the classification errors on the datasets using different approaches and features. In all cases the four features used on ordinary EPSC (denoted \(F_1, F_2, F_3\) and \(F_4\)) perform a little better than using the feature for EPSC reported in [HLV19].

More importantly, cascading on all features (C-ESCP) as well as a full ensemble without cascading (E-EPSC) perform much better than any of the single networks using any of the features. One can also note that cascading performs almost as well as the full ensemble, but being much faster. Furthermore, the cascading on just one feature (C-F1), which corresponds to the first stage in Figure 3 also works very well. It is, not surprisingly, the fastest of all methods as can be seen in Table 3, but is of course not the most accurate since it does not make use of all the features and the full cascading pipeline.

The result of using C-EPSC compared to what was presented in different papers introducing each of the datasets are shown in Table 2. Certainly, better accuracy have been achieved by much more complicated deep learning architectures since the datasets where introduced. However, the point here is not to beat the state of the art by using the C-EPSC, but rather to show that it is possible to come very close to a much lesser cost, both for learning but also for the classification.

The cascading with early termination, denoted \(C_\theta\), comes close to what the cascading does when it comes to accuracy, but is quite a lot faster. In fact, it comes close to what cascading using only one feature (C-F1) does. The reason is that the whole cascading is seldom necessary for an accurate classification. Table 4 shows the percentage of classifications that goes on beyond stage 2 and 4. Hence, the lower percentage, the more cases can be terminated early.

It can be seen in Table 4 that the percentage vary quite a lot among the datasets and one reason is probably the fact that the same threshold of \(\theta = 0.03\) for both stages were used for all datasets. This implies that this is one parameter that could be learned for an implementation of word classification.
Table 1: Prediction error (%) using different features, cascading (C), with early termination (C$_{et}$) and the full ensemble (E).

<table>
<thead>
<tr>
<th>Dataset</th>
<th>EPSC</th>
<th>E-EPSC</th>
<th>C-EPSC</th>
<th>C$_{et}$-EPSC</th>
<th>C-F1</th>
<th>F1</th>
<th>F2</th>
<th>F3</th>
<th>F4</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>0.80</td>
<td>0.56</td>
<td>0.56</td>
<td>0.56</td>
<td>0.69</td>
<td>0.69</td>
<td>0.75</td>
<td>0.70</td>
<td>0.74</td>
</tr>
<tr>
<td>E-MNIST</td>
<td>0.78</td>
<td>0.58</td>
<td>0.59</td>
<td>0.60</td>
<td>0.66</td>
<td>0.65</td>
<td>0.63</td>
<td>0.66</td>
<td>0.61</td>
</tr>
<tr>
<td>L-MNIST</td>
<td>7.60</td>
<td>6.38</td>
<td>6.43</td>
<td>6.43</td>
<td>6.90</td>
<td>6.89</td>
<td>6.97</td>
<td>6.84</td>
<td>6.98</td>
</tr>
<tr>
<td>K-MNIST</td>
<td>3.08</td>
<td>2.17</td>
<td>2.20</td>
<td>2.19</td>
<td>2.52</td>
<td>2.51</td>
<td>2.15</td>
<td>2.35</td>
<td>2.58</td>
</tr>
<tr>
<td>F-MNIST</td>
<td>11.88</td>
<td>8.73</td>
<td>8.73</td>
<td>8.73</td>
<td>10.11</td>
<td>10.11</td>
<td>10.05</td>
<td>9.82</td>
<td>10.30</td>
</tr>
</tbody>
</table>

Table 2: Classification accuracy (%) for some popular datasets and comparison with other learning methods. Note that we have taken the results from each paper proposing these methods and therefore the table is not covering the use of all methods on all datasets.

<table>
<thead>
<tr>
<th>Learning method</th>
<th>MNIST</th>
<th>E-MNIST</th>
<th>L-MNIST</th>
<th>B-MNIST</th>
<th>K-MNIST</th>
<th>F-MNIST</th>
</tr>
</thead>
<tbody>
<tr>
<td># classes</td>
<td>10</td>
<td>10</td>
<td>26</td>
<td>47</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>C-EPSC</td>
<td>94.44</td>
<td>94.41</td>
<td>93.57</td>
<td>87.35</td>
<td>97.80</td>
<td>91.23</td>
</tr>
<tr>
<td>EPSC [HLV19]</td>
<td>99.20</td>
<td>99.22</td>
<td>92.40</td>
<td>85.87</td>
<td>96.92</td>
<td>88.12</td>
</tr>
<tr>
<td>OPIUM [CATvS17]</td>
<td>-</td>
<td>96.22</td>
<td>85.15</td>
<td>78.02</td>
<td>-</td>
<td>87.1</td>
</tr>
<tr>
<td>MLP [XRV17]</td>
<td>97.20</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>95.12</td>
</tr>
<tr>
<td>Keras CNN [CBK’18]</td>
<td>99.56</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>97.82</td>
<td>-</td>
</tr>
<tr>
<td>PreActResNet-18 [CBK’18]</td>
<td>99.54</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>98.83</td>
<td>-</td>
</tr>
<tr>
<td>PreActResNet-18 + Manifold Mixup [CBK’18]</td>
<td>99.54</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>98.83</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 3: Wall clock time of classification in seconds of using different features, cascading (C), with early termination (C$_{et}$) and the full ensemble (E).

<table>
<thead>
<tr>
<th>Dataset</th>
<th>E-EPSC</th>
<th>C-EPSC</th>
<th>C$_{et}$-EPSC</th>
<th>C-F1</th>
<th>F1</th>
<th>F2</th>
<th>F3</th>
<th>F4</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>825</td>
<td>381</td>
<td>192</td>
<td>187</td>
<td>250</td>
<td>247</td>
<td>178</td>
<td>157</td>
</tr>
<tr>
<td>E-MNIST</td>
<td>797</td>
<td>379</td>
<td>193</td>
<td>194</td>
<td>248</td>
<td>228</td>
<td>177</td>
<td>153</td>
</tr>
<tr>
<td>L-MNIST</td>
<td>3667</td>
<td>834</td>
<td>592</td>
<td>509</td>
<td>1088</td>
<td>1050</td>
<td>736</td>
<td>696</td>
</tr>
<tr>
<td>B-MNIST</td>
<td>4296</td>
<td>691</td>
<td>565</td>
<td>478</td>
<td>1321</td>
<td>1198</td>
<td>888</td>
<td>786</td>
</tr>
<tr>
<td>K-MNIST</td>
<td>614</td>
<td>306</td>
<td>172</td>
<td>159</td>
<td>186</td>
<td>183</td>
<td>131</td>
<td>118</td>
</tr>
<tr>
<td>F-MNIST</td>
<td>684</td>
<td>326</td>
<td>257</td>
<td>164</td>
<td>202</td>
<td>202</td>
<td>147</td>
<td>134</td>
</tr>
</tbody>
</table>

Table 4: Percentage of how many are not terminated early in step 2 and 4 respectively, but passes to the next step in the cascading with respect to the total amount of images to be classified.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>ET-2</th>
<th>ET-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>6.32%</td>
<td>1.04%</td>
</tr>
<tr>
<td>K-MNIST</td>
<td>11.52%</td>
<td>2.75%</td>
</tr>
<tr>
<td>F-MNIST</td>
<td>63.20%</td>
<td>33.73%</td>
</tr>
<tr>
<td>E-MNIST</td>
<td>4.01%</td>
<td>0.77%</td>
</tr>
<tr>
<td>L-MNIST</td>
<td>45.30%</td>
<td>21.22%</td>
</tr>
<tr>
<td>B-MNIST</td>
<td>30.20%</td>
<td>12.15%</td>
</tr>
</tbody>
</table>

6 CONCLUSION

Deep learning architectures and the learning and classification process are not easy to visualise, nor to explain. The EPSC on the other hand is based on clustering of embedded features. Both the clusters and corresponding images as well as the resulting neural nets can easily be visualised and comprehended. Therefore, EPSC is an interesting alternative in the domain of XAI. It was experimentally shown that both ensembles and cascading can improve the speed and accuracy. Furthermore, early termination bring down the cost of classification quite a lot, without compromising the accuracy.

For future work we propose to use EPSC for word images rather on individual letters. Moreover, it is necessary to find some plausible explanation why HoG and
features based on the magnitude of FFT works so well together.

7 REFERENCES


