Annotating handwritten characters with minimal human involvement in a semi-supervised learning strategy

Jan Richarz, Szilárd Vajda and Gernot A. Fink
Faculty of Computer Science XII, TU Dortmund, Germany
{jan.richarz, szilard.vajda, gernot.fink}@udo.edu

Abstract

One obstacle in the automatic analysis of handwritten documents is the huge amount of labeled data typically needed for classifier training. This is especially true when the document scans are of bad quality and different writers and writing styles have to be covered. Consequently, the considerable human effort required in the process currently prohibits the automatic transcription of large document collections. In this paper, two semi-supervised multiview learning approaches are presented, reducing the manual burden by robustly deriving a large number of labels from relatively few manual annotations. The first is based on cluster-level annotation followed by a majority decision, whereas the second casts the labeling process as a retrieval task and derives labels by voting among ranked lists. Both methods are thoroughly evaluated in a handwritten character recognition scenario using realistic document data.

1 Introduction

Training pattern recognizers typically requires large amounts of manually annotated samples in order to capture the characteristics of the data. In offline handwriting recognition, where characters may exhibit large variations in appearance due to different writers and writing styles, and no temporal information is available to aid the task, this problem is especially severe.

In museums and archives, large collections of handwritten documents exist that are of great potential interest for historians and scientists. Thus, there has been considerable effort to digitize them. However, ideally, the scanned document images should be fully transcribed in order to enable fast searching, browsing, efficient storage, and complete automatic analysis. Today, the transcription is still mostly done manually, which is a very laborious and tiresome task, and only insignificant numbers of documents can be processed this way. Nevertheless, the lack of sufficiently reliable general offline handwriting recognizers and the amount of effort that has to be spent in training them currently prohibits fully automatic processing of such collections.

The focus of this paper is thus not primarily to investigate features or techniques for handwritten character recognition, but to develop methods that help in annotating large amounts of data efficiently. Suppose it is possible to label large databases with sufficiently small manual effort, say, a few hundred manual operations to label several thousand samples. Then, even the repeated training of classifiers specialized on some specific writer or script may become feasible. It can be expected that such a specifically trained recognizer will perform better than a general one, that has to cover the variations of largely differing writing styles.

Therefore, two methods are presented that greatly reduce the required manual effort in labeling by adopting approaches from the field of semi-supervised and multiview learning (cf. e.g. [18]), utilizing a voting scheme over different feature representations of the data in order to increase reliability. The first method is based on clustering, annotating the clusters and performing a majority vote. The second casts the labeling problem as an interactive retrieval task. The applicability of both is demonstrated on a set of handwritten documents.

2 Problem statement

In offline handwriting recognition, the large variability of character appearances over different writers and styles poses a challenging problem. Consequently, the error rates obtained in multi-writer recognition scenarios are typically high (cf. e.g. [8]). Existing recognizers thus are often restrained to a single writer (cf. e.g. [2, 17]). While there exist successful approaches for automatic keyword indexing in document collections (cf. e.g. [9, 11]), the automatic transcription of handwritten
documents still remains an open problem. Generally, recognizers can only perform reliably on data similar to the training data, and have to be adapted or re-trained when applied to a new data domain. Consequently, the amount of human effort required to collect sufficient ground truth data for training becomes prohibitive for applications outside the academic field.

Thus, it is worthwhile to develop methods that reduce this labeling effort, making the training of specialized – and, thus, more reliable – classifiers feasible for large and diverse collections. We seek to contribute in this field by presenting approaches for efficient labeling of large data sets, adopting ideas from semi-supervised learning to alleviate the required manual effort.

The general idea of semi-supervised learning (cf. e.g. [18]) is to operate on both labeled and unlabeled data. Specifically, semi-supervised classification is the problem of training a classifier when only a small part of the data is annotated and the (typically) vast majority of data labels is unknown. Consequently, known labels must be robustly propagated to the unknown data by using unsupervised techniques. In order to achieve this, we adopt the concept of multiview learning. Here, an ensemble of learners is trained, each having a different view on the data (for an overview of ensemble methods, cf. e.g. [6]). Decisions are then obtained by combining the outputs of the different learners, e.g. by majority voting. Some concepts used in this work are also related to active learning (cf. e.g. [13]), where the learner actively selects the data that should get annotated based on its current knowledge in a feedback loop.

The problem of propagating labels to large corpora from just a few annotated instances has been studied extensively in the field of semantic image retrieval (cf. e.g. [3, 14]). In [1], it is shown that the recognition rate of a handwriting recognizer can be improved using a self-learning strategy on unlabeled adaptation data. In [12], character annotations are derived from word-level ground truth by optimizing segmentation hypotheses in an unsupervised manner. However, the initial set of word annotations must be provided manually.

3 Proposed methods

In the following, we outline the proposed semi-supervised multiview methods for efficient labeling in a general manner. Concrete realizations and parametrizations will be presented in section 4.

3.1 Clustering-based annotation (CBA)

In our previous work [16], a multiview labeling method requiring minimal human effort was proposed. We slightly enhance this method in the following, and provide a more thorough evaluation. The idea behind the method is simple: Label as few samples as possible and infer the labels for other samples automatically.

The labeling process consists of three major steps. First, an ensemble of data representations is created, providing alternative views of the data by using different types of features. Then, each representation is clustered into $k_j$ clusters, where $k_j$ may differ for each representation. Further diversification is achieved by applying different clustering algorithms. The result is a set of $r$ different data setups $R_{j, r = 1..r}$, i.e. alternative combinations of features and clustering algorithms.

Given a set of clusters, only the centroids are labeled manually, and the rest of the samples in the cluster inherit the label. This implies $\sum_{j} k_j$ manual operations, and yields $r$ independent labels for each sample.

Inheriting labels from cluster centroids will result in some incorrectly labeled samples, since, generally, the clusters are not pure. Thus, the final step of the procedure is to determine which labels are reliable. Assume that the labels are given as $d$-dimensional binary vectors $[l_{i, 1}, \ldots, l_{i, d}]^T \in \{0, 1\}^d$, $i = 1, \ldots, r$, where $l_{i, j} = 1$ if a sample $p$ is assigned to class $\omega_j$ in setup $R_i$, and 0 otherwise. Applying a majority voting procedure results in an ensemble decision for a specific class label $\omega_{k}^{\text{max}}$. A threshold $\kappa_e$ on the ensemble decision is used to select only those samples where the class membership is determined with high agreement:

$$\omega_{k}^{\text{max}} = \max_{k} \sum_{i=1}^{r} l_{i, k} \geq \kappa_e. \quad (1)$$

In the following, we only retain samples for which all votes agree on the same label (unanimity vote), i.e. $\kappa_e = r$. Finally, the subset of samples and assigned labels retained from the above procedure is used to train a classifier. This classifier can then be used to either re-evaluate the training data (inductive learning) or classify a test set of unknown data (transductive learning).

3.2 Retrieval-based annotation (RBA)

The second proposed method is based on interactive retrieval, and is related to pool-based active learning with relevance feedback (cf. e.g. [15]). However, it differs in a few important aspects from this paradigm. Most importantly, we want to retrieve labels for all possible classes (quasi-) simultaneously. Additionally, selecting relevant samples manually counteracts the goal of lessening the burden for the annotator. Consequently, the manual relevance feedback step is replaced by a simple automatic selection rule on the
Unlabeled samples

Select query

Manual annotation

Feature rep. 1

Feature rep. 2

Feature rep. r

Retrieval lists

labeled samples

Termination criterion met?

Majority vote

N

N

Partially labeled sample set

Figure 1. Overview of the proposed retrieval-based annotation process.

retrieval list, propagating the annotation to unlabeled samples. Since incorrectly assigned labels will occur in this stage a multiview voting concept taking into account several retrieval runs is integrated. The intuition behind is that, if multiple runs for the same query in several data representations agree on a subset of samples, then those belong to the query class with high confidence. Figure 1 gives an overview of the procedure.

Let \( \mathcal{X} = \{ X_i, i = 1...n \} \) be a pool of \( n \) unlabeled data samples, \( X_i = \{ x_{ij}, u_i, v_i, n_i, j = 1...r \} \), where \( x_{ij} \) is the \( i \)-th data sample’s \( j \)-th feature representation, \( u_i \) is a variable-length vector of class labels (empty on initialization), \( v_i \) is a vector of confidence scores associated with each label in \( u_i \), and \( n_i \) is the number of times the sample has been considered. Also, let \( \mathcal{T} = \{ X_k, y_k, k = 1...m \} \) be an initially empty pool of trusted samples, with the \( k \)-th sample’s final label \( y_k \).

First, a sample \( X_s \) is selected from \( \mathcal{X} \). Since no information is available in the first iteration, this selection is random. In further iterations, only the subset \( \mathcal{X} \) of samples with minimum value of \( n_i \) is considered, i.e.

\[
\mathcal{X} = \{ X_i : n_i = \min_i(n_i) \},
\]

and \( X_s \) is selected randomly from this subset. The rationale behind is that those samples should be selected that have not been considered (often) before, thus exploring the data set. Then, a class annotation \( \omega_s \) for \( X_s \) is requested from the annotator, which can also be a rejection label. This manual assignment is trusted, hence \( X_s \) is removed from \( \mathcal{X} \) and appended to \( \mathcal{T} \), with \( y_s = \omega_s \). Note that, in “real” active learning, the sample selection would be based on the current state of some classifier. In omitting this, we are able to start with a completely unlabeled data set and avoid frequent re-training with potentially unreliable ground truth.

Afterwards, \( r \) retrieval tasks are carried out on the remaining set \( \mathcal{X} \setminus X_s \) using the \( r \) different feature representations \( x_{ij} \) as queries. This results in \( r \) retrieval lists \( L_j \), ranked according to some distance \( d(x_{ij}, x_{ik}) \), and thresholded with a common threshold \( \kappa_d \) on the distances. In the following, the cosine distance is used for \( d(...) \). Assume that a sample \( X_p \) is present in \( N_p \) of the \( r \) thresholded lists. Then, the confidence \( \gamma_{ps} \) of \( X_p \) belonging to the query class \( \omega_s \) is given by \( \gamma_{ps} = \frac{N_p}{r} \). If \( \gamma_{ps} \) is 1, i.e. if \( X_p \) appears in all thresholded lists, then \( \mathcal{X} = \mathcal{X} \setminus X_p, y_p = \omega_s, \mathcal{T} = \mathcal{T} \cup \{ X_p, y_p \} \).

Otherwise, \( u_p = u_p \cup \omega_s, v_p = v_p \cup \gamma_{ps}, n_p = n_p + 1 \). The sample remains in \( \mathcal{X} \) in this case, and may be considered again in further iterations. Samples with \( d(...) > \kappa_d \) in all retrieval lists remain unchanged.

This interactive procedure is repeated until a termination criterion is met. In practice, we simply abort after a fixed number \( I_m \) of manual operations. Each remaining sample \( X_i \in \mathcal{X} : n_i > 0 \) now has a list \( u_i = \{ u_{it}, t = 1...n_i \} \) of assigned labels with associated confidences \( v_i = \{ v_{it} \} \). Furthermore, the set of available classes \( \Omega = \{ \omega_k, k = 1...c \} \) has evolved based on the manual annotations provided in the process. For each \( X_i \), the accumulated class confidences

\[
\sigma_i(\omega_k) = \sum_{t} \sum_{k} v_{it} \delta(u_{it} = \omega_k)
\] (3)

are calculated and then normalized to \([0, 1]\) by dividing by the maximum possible accumulated confidence:

\[
\hat{\sigma}_i(\omega_k) = \frac{\sigma_i(\omega_k)}{(r - 1) \cdot n_i}.
\] (4)

Finally, the final class label \( y_i \) of \( X_i \) is determined as \( y_i = \arg\max_k(\hat{\sigma}_i(\omega_k)) \). If the associated maximum confidence \( \hat{\sigma}_i(\omega_k) \) is above a threshold \( \kappa_v \), the sample is added to the set of trusted samples \( \mathcal{T} \). Otherwise, the sample is rejected because the assigned label would be too unreliable. The classifier is then trained on \( \mathcal{T} \).

Compared to CBA presented in the previous section, the above procedure offers several advantages. No prior knowledge or assumption about the number of classes is required because they will evolve implicitly based on the labels assigned by the annotator. Also, it is possible to manually reject "bad" samples, and the required manual effort does not depend on the number of different representations \( r \) since they are evaluated simultaneously. On the other hand, the impact of errors in the manual annotation can be expected to be higher. Additionally, values for the parameters \( \kappa_d, \kappa_v \) and \( I_m \) have to be selected heuristically. Suitable values will be determined experimentally in section 4.4.
4 Experiments

In order to assess the performance of the proposed methods, we first derive suitable parameters on the MNIST handwritten digit dataset [7]. Afterwards, a realistic transductive recognition experiment is conducted on a set of historical documents.

4.1 Data description and experimental setup

Our data set consists of historical official weather reports, kindly provided by the German Weather Service ("Deutscher Wetterdienst", DWD). Detailed characteristics of the data are given in [10]. For the experiments reported here, a set of 106 document images was provided, scanned at approximately 200 dpi. The entire collection comprises several 10,000 pages, but only a small subset is currently available in digitized form.

In total, the data contains 13,331 samples (5,140 characters, 8,191 digits) in 17 classes. Ground truth labels are available for all samples. The data set is unbalanced, and several classes occur very rarely. We assume that knowledge about the type of each sample (character or digit) is known from a document template (cf. [10]). This information will be used in the retrieval and classification to limit the set of candidates. Documents are subdivided in a 3-fold cross-validation setup.

In each validation set, approximately 2/3 of the documents constitute the training set and the remaining the test set. Thus, training and test set are disjunct, but overall, all documents are considered once for testing.

4.2 Features

The proposed labeling methods rely on a multiview approach using different feature representations. In principle, the methodology is independent of the types of features used. Obviously, the better the discriminative power of the features, the better the results will be. Especially for the retrieval-based approach, compact features are desirable in order to keep the process efficient and avoid latencies in the interactive loop.

In the following, we focus on a set of features that yielded good performance in our previous work. Specifically, we consider the raw image of a character (RAW), normalized to size $28 \times 28$ pixels, its PCA representation using the first 80 PC [10], and higher-level structural features based on contour chain codes (CC), skeletons (SKEL) and character reservoirs (RES) [5]. The latter were modified by considering 5 types of reservoirs (top, bottom, left, right, loop) and using just a soft assignment of the positions of their gravity centers to image cells. All features are calculated in a $4 \times 4$ regular grid on the normalized character image. Feature dimensionalities range from 36 (SKEL) to 80 (PCA).

4.3 Parametrization of CBA

Even though using all features might provide a better discrimination for the different clusters, selection of a subset is advisable for efficiency reasons. In order to select the best setup (features/clustering methods), an exhaustive search was performed. All different features extracted from the MNIST training material were clustered using k-means, SOM (Self Organizing Map) and GNG (Growing Neural Gas) [4]. The cluster centers were then manually annotated by an expert.

As quality criteria, the sample recall $R$ (percentage of retained trusted samples after voting) and label precision $P$ (percentage of correctly labeled retained samples) obtained on MNIST were used. Ranking the different combinations, the best setup was: RAW/GNG, CC/GNG, and CC/k-means. In general, GNG and k-means outperform SOM clustering. With this setup and 54 cluster centers [16] for each combination, unanimity vote occurred in $R = 76.15\%$ of the cases with $P = 96.10\%$. Thus, 45,690 annotations were inferred using only 162 manual labeling operations (0.35%). Compared to [16], the substantial increase in sample recall (approx. 21%) while retaining the same labeling accuracy shows the benefit of using diversified feature representations and different clustering methods.

4.4 Parametrization of RBA

In order to find suitable values for the parameters $\kappa_d$ and $\kappa_v$, a number of experiments was conducted on the MNIST data set, performing $I_m = 500$ labeling operations and averaging over 10 runs with identical parametrization in order to smooth the effects of the random selection. The manual labeling was simulated by assigning the respective ground truth label to the query example, i.e. error-free annotation is assumed. The goal is to find a range of parameters offering a good balance between sample recall and label precision. Numerous combinations of the different features were investigated, excluding RAW for efficiency reasons. Due to space restrictions, we will not provide details on all experiments, but just report results for the best feature combination (CC + PCA + RES, i.e. $r = 3$).

As can be seen in Fig. 2, the labeling precision is generally high, except for small values of $\kappa_v$. It also degrades for small values of $\kappa_d$, because then only few samples will be considered in each retrieval run, and the small overall number of votes leads to an unreliable majority decision. In terms of sample recall, the method...
is more restrictive than CBA retaining large fractions of the data only for small values of $\kappa_v$.

In order to determine a suitable parametrization, we calculate the F3 score $F_3 = \frac{10Pv}{85P + 15\kappa_v}$, reflecting the assumption that it is more desirable to have correctly labeled samples than retaining large portions of the original data. The maximum was $F_3 = 91.54\%$ ($R = 82.72\%$, $P = 92.63\%$) for parameter values $\kappa_d = 0.25$, $\kappa_v = 0.20$. However, from Fig. 2, it becomes obvious that the quality in terms of $F_3$ is comparable for a range of parameter values around this optimum, meaning that the method is not too sensitive against the concrete choice of values. In the following, again favoring high precision, we will use more restrictive parameter values of $\kappa_d = 0.2$, $\kappa_v = 0.30$, yielding $P = 97.15\%$, $R = 59.02\%$, $F_3 = 91.26\%$ for the above experiment.

### 4.5 Recognition experiments

The setups derived above are evaluated in a transduction classification experiment on the MNIST and DWD data, demonstrating that the methods perform reliably on different datasets and that tuning the parameters to specific data – which is not possible in real applications – is not necessary. We perform a realistic experiment, where the training sets are first labeled by an expert annotator using the proposed methods. Then, the resulting classifiers are evaluated on the disjunct test sets. For comparison, we present results of oracle experiments, using all ground truth labels for training. These constitute an upper limit of the achievable performance.

In order to make the results comparable, an identical number of manual annotations (162) is used for both CBA and RBA. Statistics on MNIST for CBA using this setting were given in Sec. 4.3. For RBA, a recall of $R = 57.91\%$ and precision of $P = 90.02\%$ were obtained.

For the 3-fold cross-validation on the DWD data, also 162 labeling operations were performed for each validation set. With CBA, on average $R = 92.00\%$ of the training material was retained, yielding an average label precision of $P = 92.18\%$. With RBA, $R = 87.74\%$ of samples were retained with $P = 95.64\%$.

As discussed in [10], a drawback of CBA is that it tends to discard rare classes in the case of highly unbalanced data. While this did not occur for the balanced MNIST set, only 14 out of 17 classes were recovered on average on the DWD data. With RBA, all 17 classes were retained. This shows a major advantage of the RBA approach: Because of the steered sample selection, rare classes are less likely to be discarded.

Character recognition rates, obtained with a linear SVM in a 1-vs-1 multiclass setup, are given in Table 1. Applying the proposed labeling schemes to the MNIST data results in a substantial loss in recognition performance. Both methods rely on discovering clusters of similar samples, i.e. from the same writer or written in the same style. Since the MNIST data is very diverse and contains hundreds of writers, this assumption is violated, resulting in a loss of accuracy. RBA performs worse than CBA because propagating the labels based on the retrieval lists proceeds considerably slower than labeling the large portions of data contained within a cluster. As shown in Fig. 3, the performance of RBA keeps increasing until approximately 400–500 manual annotations were performed (still less than 1%).

However, for the DWD data, which is much more homogeneous in terms of writing style, the results obtained with both CBA and RBA are close to the reference oracle experiment. This clearly shows the potential of both methods, provided that large portions of the data show similar characteristics. Only very little manual effort was required (performing the 162 labeling operations was a matter of a few minutes) to obtain competitive recognition rates, making the proposed methods especially promising for large single-writer collections.
5 Conclusion

Two semi-supervised methods for annotating data with minimum human effort were proposed. Both build on ideas from multiview learning in order to propagate labels reliably, incorporating a voting procedure over different feature representations. It was demonstrated that thousands of training labels can be inferred from very few manual annotations with high accuracy, facilitating the annotation of large data sets within minutes. Using these labels a recognizer was trained that achieved good performance in a handwritten character recognition experiment on two different databases. Since both approaches rely on finding large clusters of similar data samples they are especially promising for collections containing large portions of data from the same writer(s). In this case, the recognition performance is close to the reference oracle experiment.

Acknowledgments

This work is supported by the German Federal Ministry of Economics and Technology on a basis of a decision by the German Bundestag within project KF2442004LF0.

References