Self-Training of Handwritten Word Recognition for Synthetic-to-Real Adaptation

Fabian Wolf
Department of Computer Science
TU Dortmund University
44227 Dortmund, Germany
fabian.wolf@cs.tu-dortmund.de

Gernot A. Fink
Department of Computer Science
TU Dortmund University
44227 Dortmund, Germany
gernot.fink@cs.tu-dortmund.de

Abstract—Performances of Handwritten Text Recognition (HTR) models are largely determined by the availability of labeled and representative training samples. However, in many application scenarios, labeled samples are scarce or costly to obtain. In this work, we propose a self-training approach to train a HTR model solely on synthetic samples and unlabeled data. The proposed training scheme uses an initial model trained on synthetic data to make predictions for the unlabeled target dataset. Starting from this initial model with rather poor performance, we show that a considerable adaptation is possible by training against the iteratively predicted pseudo-labels. Therefore, the investigated self-training method does not require any manually annotated training samples. We evaluate the proposed method on four benchmark datasets and show its effectiveness on reducing the gap to a model trained in a fully-supervised manner.

I. INTRODUCTION

Handwritten Text Recognition (HTR) constitutes a complex pattern recognition problem, due to the high variability in its data. A single word, even when written by the same writer, does never share the exact same appearance. Machine learning models and especially neural networks have become the approach of choice for this recognition task. During the last decades, the field has seen an evolution of approaches from Hidden Markov Models [1]–[3] to recurrent neural networks trained with Connectionist Temporal Classification (CTC) [4]–[7]. Recently, sequence-to-sequence methods relying on attention based decoders got increasingly popular, pushing the performance of HTR models further on several benchmarks [8]–[10]. Nonetheless, the use of increasingly complex models comes at the cost of requiring huge annotated training sets. While datasets such as ImageNet [11] contain millions of samples, handwriting data is still usually quite limited and academic benchmarks rarely surpass 100,000 word images. The limited number of samples is especially challenging, when confronted with document collections that have a distinctive style. Considering, for example, historic documents, the appearance is often too specific to simply employ a HTR system trained on modern handwriting [12]. Collection specific annotations need to be created, which often can only be done by experts making it a costly approach.

While the visual appearance of different handwritten text collection may diverge heavily, the underlying structure is still well defined by character and language constraints. This motivates the idea to pursue methods that allow to adapt a general model to a specific writing style. Writer adaptation is a concept studied in the literature already before the field was taken over by neural networks [13]. A common strategy for domain adaptation in the general computer vision and object recognition communities is the use of adversarial learning, which has been also investigated to adapt a HTR model [14]. This approach relies on minimizing the differences of the domains in the feature space to improve the generalization capability of the decoder.

Beside the use of unlabeled samples, a common approach to alleviate the data requirements especially in document analysis is to synthesize samples [15]–[18]. Due to the limited variability of the synthesized data which often relies on true type fonts, performances of models purely trained on synthetic data are usually poor. Nonetheless, bootstrapping and pre-training on synthetic samples has been shown to leverage the data problem.

In this work, we propose a self-training method that only relies on synthetically generated handwriting samples and unlabeled in-domain data to train a handwritten word recognizer. At the core of our approach, we use a sequence-to-sequence recognition model, that has already been investigated in the context of writer adaptation [9], [14]. First, we train the model on purely synthetic samples, giving an initial model with rather poor performance. In order to adapt from synthetic data to a document collection, the model predicts pseudo-labels for...
previously unlabeled samples. Training is then continued on a selection of samples, which is based on a confidence measure. We show that the prediction outputs of the sequence-to-sequence model serve well as a confidence estimation despite the lack of a clear probabilistic interpretation. Training on the iteratively predicted and selected pseudo-labels leads to high performance gains compared to the initial model. See Fig. 1 for an overview of the proposed training scheme. We further investigate the influence of the synthetic dataset and argue that training on such encodes a form of an implicit language model. Additionally, we include a form of consistency regularization that relies on two different augmentation approaches.

II. RELATED WORK

A. Handwritten Text Recognition

Handwritten Text Recognition is a computer vision problem that has been traditionally tackled with machine learning techniques. With text being essentially a sequence of characters represented by features, Hidden Markov Models (HMMs) were the dominant models in the early days of text recognition [1]–[3]. This is mainly due to their capability of jointly solving the recognition and segmentation task. The rise of deep learning and neural networks was significantly influenced by handwriting recognition with MNIST being one of the first successful applications of convolutional neural networks [4]. Recurrent architectures such as Bidirectional or Multidimensional LSTMs rapidly took over the field as they are highly effective in modeling the sequential structure of handwriting [5]–[7]. These models have been predominantly combined with Connectionist Temporal Classification (CTC) layers to decode each single frame followed by a reduction to the resulting character sequence [8]. Due to the long term modeling capacity and the high number of parameters, it is argued that the LSTM based architectures not just learn visual information but also implicitly encode language characteristics similar to a language model [21]. Recently, sequence-to-sequence architectures became increasingly popular. Based on an Encoder-Decoder structure, these models are able to map from differently sized input to output sequences by the use of attention mechanisms [8]–[10].

B. Semi Supervised Learning (SSL)

The widespread use of deep learning is to some extent motivated by the observation that training on larger dataset increases performances, making it often the case of the art if enough training data is available. Semi-supervised learning aims at exploiting the potential power of deep architecture when labeled training data is scarce or not available. Therefore, training is based on unlabeled data in combination with a limited set of labeled samples. Self-training, which is also called pseudo-labeling, has been heavily investigated in this regard [22]–[26]. Its core idea is to use labeled samples to enable the model to make predictions for unlabeled data. The model then considers the predictions to be actual labels and training is continued respectively. While the initial predictions are error prone, this approach is usually combined with a confidence-based selection. A confidence measure identifies erroneous data points, which are neglected. Additionally, works such as [24]–[26] combine self-training with consistency regular- ization. By using multiple augmentation strategies, several perturbed versions of a sample are generated. The fact that all these augmented version share the same label is then exploited for label prediction or during training by introducing a consistency loss.

Adversarial training can be considered another class of methods to adapt a model trained on one domain to a target dataset. Commonly, an additional discriminator is added to the model supposedly to discriminate between source and target domain. Training is performed in such a way, that the discriminator is fooled and not able to distinguish features from both domains. This leads to learning domain independent features improving the generalization capabilities of the model [27]–[29].

C. SSL in Document Analysis

Handwritten document analysis is an area of research where labeled training data is often hard to obtain. Due to the extremely high variance in writing styles and specificities of document collections, in-domain samples are usually required to achieve state-of-the-art performances. This makes semi-supervised approaches highly attractive and several methods have been investigated and proposed.

In the context of document analysis, generating synthetic data is often easily possible. A multitude of true type fonts that resemble handwriting exist and may be used to render an infinite number of synthetic training samples. Works such as [15]–[17] show that solely training models on these synthetic datasets yield poor performances, but it is an efficient way to pretrain and finally finetune the initial model by a limited number of target samples. Multiple works use Generative Adversarial Networks (GANs) to generate more realistic samples of handwritten word images [30]–[32]. In general, these methods either require labeled training data themselves or only marginally improve recognition performances when combining synthesized and labeled training samples.

Several works investigate adaptation strategies for optical character recognition [33], [34]. Starting with models trained on related data that already achieve comparably low error rates, it is shown that performances improve with self-training.

With respect to handwriting data, self-training was shown to be effective for transductive learning in [35]. Other works combine self-training strategies with additional language based supervision from either a lexicon [18] or language models [36]. An approach to adapt a handwriting recognition model from synthetic to real data is proposed in [14]. By using an adversarial domain loss, the authors show that the performance gap between a model trained only on synthetic samples and the state-of-the-art performance with target data can be reduced significantly.
III. TEXT RECOGNITION

In this work, we use a sequence-to-sequence model for HTR. Most design choices and hyperparameters are adopted from [14]. This allows to minimize the influence of different model components and for a fair comparison to the adversarial adaptation strategy proposed in [14]. As discussed in [37], text recognition models generally follow a similar structure. With respect to this framework the key building blocks of the HTR model can be summarized as follows.

1) Feature Extraction: A convolutional neural network serves as a feature extractor. Specifically, a VGG-19-BN architecture [38] maps the input image \( I \in I \) to a two-dimensional feature map \( X \). Its columns are then considered a sequence of feature vectors \( (x_0, x_1, \ldots, x_{N-1}) \) of length \( N \).

2) Sequence Modeling: A two layered Bidirectional Gated Recurrent Unit models the sequential nature of the input image. Therefore, a sequence of contextual feature vectors \( H \) is computed. The respective sequence of vectors \( h_i \in H \), \( (h_0, h_1, \ldots, h_{N-1}) \) constitutes the final encoder output.

3) Prediction: The model uses an attention-based decoder to predict the final output sequence. We use a local attention mechanism with attention smoothing to compute a mask at every time step. Based on the attention mask, a context vector is computed, which is then fed into the decoder. At each time step \( t \), the decoder computes a pseudo-probability distribution \( d \) over the set of characters. The final sequence of characters \( y \in Y \), \( (y_0, y_1, \ldots, y_T) \) results from the character with highest pseudo-probability at each time step \( t \).

The HTR model may be summarized by two functions. First, the encoder function \( G_e : I \rightarrow H \) computes a sequence of feature vectors \( h_i \). The decoder constitutes a function \( G_r : H \rightarrow Y \) that maps the sequence of feature vectors to the final recognition sequence \( y \). During training, the recognition loss \( L_r \), which is essentially the cross entropy between the one hot encoded character and the pseudo-probabilities \( d_t \) at every time step \( t \), is minimized. Additionally, label smoothing is applied with an \( \epsilon = 0.4 \), regularizing the hard classification targets of 0 and 1. For details on the model architecture and choice of hyperparameters, see [9], [14].

IV. METHOD

The proposed method includes two training phases. First, an initial model is derived based on a synthetic dataset, see Sec. IV-A. The model is adapted to the target dataset by a self-training scheme, see Sec. IV-B, that includes consistency regularization, see Sec. IV-C.

A. Synthetic Data Generation

In order to train an initial model, we rely on rendering synthetic word images. Therefore, we follow the same approach as in [7], [14], [18] and use a set of 398 true type fonts that resemble handwriting. During synthesis, we randomly vary the stroke width, the distance between characters, the skew and slant angles. Based on a given string, a gray scale image is rendered, again with randomly chosen intensity values for foreground- and background pixels. The resulting image is then filtered by Gaussian Smoothing.

In order to build a diverse representation of language, we collected text from the top one hundred English books of the Gutenberg Project. The following experiments investigate the question whether the choice of text influences the model’s performance or if independent character models are learned solely based on the visual appearance. Therefore, we created three different datasets:

- **Natural Text**: We rendered the individual word images directly based on the texts as occurring in the respective books. Character and word distributions are kept as found in the natural texts, resulting in about 13 million word images.
- **Uniform**: To remove the influence of the word distribution, we determined the lexicon of unique strings of the text corpus. Based on a uniform word distribution, the same number of images is synthesized.
- **Random**: In order to further investigate the implicit language model learned from the synthetic data, we created a set of randomized word images. Characters are chosen randomly based on their unigram distribution. Word lengths follow the same distribution as found in the natural text corpora. All single character words and single punctuation marks that occur in the natural text are included identically. Furthermore, we capitalize the generated strings and append punctuation marks with the same probability as observed in the original text corpus.

B. Training Scheme

First, we train the recognizer for one epoch on the synthesized word images with additionally including a set of standard augmentations such as blurring or Gaussian noise and geometric transformation, i.e., shear, rotation and rescaling. This initial model then predicts pseudo-labels \( \hat{y}_i \) for the unlabeled target dataset \( u_i \in U, i \in \{0, 1, \ldots, J\} \).

\(^1\)Text corpus based on books downloaded from https://gutenberg.org
As we assume that the predicted labels are highly erroneous, we aim at identifying correct samples using a confidence measure. Based on the hidden state, the context vector and the previous embedding vector, the decoder predicts a set of pseudo-probabilities \( d_i \) at each time step \( t \). For each character, we consider its corresponding activation as a numeric estimation of how confident the network is in the respective prediction. To obtain a confidence estimation over the entire sequence, we take the mean over all character confidences:

\[
e = \frac{1}{T} \sum_{t} \max (d_t) \tag{1}
\]

After computing the word confidences over all samples in the target dataset, all samples with a confidence value below a threshold \( \tau \) are neglected. The procedure of label prediction, confidence estimation, thresholding and training is performed repeatedly for 50 cycles.

### C. Consistency Regularization

This work follows the ideas of FixMatch [26] and applies a form of consistency regularization by introducing an additional augmentation strategy. In the following, we refer to the previously described augmentation strategy as weak augmentation. We additionally use the grid augmentation proposed in [6] in combination with the weak augmentation. This introduces fine grained perturbations on a character level, generally introducing stronger variations. This allows to combine differently perturbed versions of the same sample in a single training batch, see Fig. 2.

In the following, \( A : \mathcal{I} \to \mathcal{I} \) denotes an augmentation function. Let \( \mathcal{U} = \{ u_i : i \in \{ 0, 1, \ldots, B \} \} \) be a batch of unlabeled samples with \( c_i > \tau \) and corresponding pseudo-labels \( \hat{y}_i \). During Training each batch contains two augmented versions of an image, resulting in the following formulation of the training loss \( \ell \).

\[
\ell = \sum_{i=0}^{B} \mathcal{L}_{r}(G_r(A_0(u_i)), \hat{y}_i) + \mathcal{L}_{r}(G_r(A_1(u_i)), \hat{y}_i) \tag{2}
\]

As we compute the recognition loss with respect to a previously fixed pseudo-label, a form of consistency regularization is introduced. The augmentation functions \( A_0 \) and \( A_1 \) constitute either a weak or strong augmentation of the image. Implicitly, the network is not only optimized to predict a potentially erroneous pseudo-label, but also learns that both perturbed versions of the word images share the same label.

## V. Experiments

We evaluate the proposed self-training method on four different datasets, see Sec. V-A. All models are trained with ADAM optimization, a batch size of 32 and an initial learning rate of \( 2 \times 10^{-4} \). We train for a single epoch on the synthetic datasets. In case of the adaptation experiments, we perform 50 cycles of label prediction and train for one epoch on the selected portion of the entire dataset. As a performance measure we consider character (CER) and word error rates (WER) over the respective test sets.

### A. Datasets

We present experiments on four datasets that contain handwriting in the English language. The datasets vary considerably in their size and characteristics and include modern (IAM [39], CVL [40]) and historic documents (George Washington (GW) [41], Bentham (BT) [42]). Multi-writer datasets, such as IAM and CVL, are included to show that the proposed method is not limited to adapt to a single specific writing style. Note, that despite the fact that the CVL dataset also includes German words, we do not make any adaptations in this regard at the synthesis stage and treat the dataset identically to the solely English corporas. For GW, IAM and CVL, we follow the exact same evaluation protocols as described in [14]. For BT we follow [12], as they also report recognition performances not relying on any in-domain samples.

### B. Synthetic Data Generation

We train on synthetically generated word images to derive an initial model. Tab. I presents resulting error rates based on the three different generation procedures. Training on the dataset derived from the natural text corpora yields
Fig. 4. Performances of self-training with different thresholds for the confidence based selection. Each figure reports CERs (orange) and WERs (green). Dashed lines correspond to the performance when no selection is applied and training is performed on all samples. Training diverges for thresholds greater than 0.55, as due to the label smoothing almost no samples surpass a higher threshold.

Fig. 5. Error rates of the initial models on different fractions of the datasets. Samples are sorted by confidence and the error rate is calculated for the confident fraction of the dataset.

TABLE I

PERFORMANCES OF INITIAL MODELS TRAINED ON SYNTHETIC DATASETS

| Method       | GW CER | IAM CER | CVL CER | BT WER |
|--------------|--------|---------|---------|--------|
| Kang [14]    | 26.05  | 56.79   | 26.44   | 54.56  |
| Random       | 40.78  | 88.32   | 38.13   | 73.08  |
| Uniform      | 28.97  | 70.70   | 34.19   | 34.15  |
| Natural      | 25.41  | 62.11   | 21.78   | 48.07  |

The first question to raise is whether the output activations are a suitable measure to identify erroneous samples. See Fig. 3, for exemplary prediction results of the initial model solely trained on synthetic data. Furthermore, we weighted the attention masks of the model with the respective character confidence in order to visualize the area of high and low confidence. Qualitatively, it can be observed that characters or parts of words with low confidences coincide with recognition errors. Image areas of low confidence are often ambiguous and generally result in plausible errors. To further underline the expressiveness of the proposed confidence measure, we show error rates over differently confident parts of the datasets in Fig. 5. Lower error rates can be observed in the more confident parts of the dataset, leading to the conclusion that the output activation effectively results in a numeric value of how confident the network is in its prediction.

C. Confidence Estimation

After training an initial model on the synthetic dataset, we investigate the adaptation capability of the self-training approach. As shown in Tab. II, training on all pseudo-labeled samples with no confidence based selection already leads to performance gains compared to the initial model.

TABLE II

EXPERIMENTS ON DIFFERENT SELECTION STRATEGIES

| Selection       | GW CER | IAM CER | CVL CER | BT WER |
|-----------------|--------|---------|---------|--------|
| Initial         | 25.41  | 62.11   | 21.78   | 48.07  |
| None            | 16.65  | 46.15   | 16.19   | 41.89  |
| Thresholding    | 12.37  | 32.65   | 9.96    | 27.78  |
| Random(∗)       | 16.75  | 43.47   | 13.99   | 37.60  |
| Confidence(∗)   | 12.28  | 31.02   | 10.95   | 29.07  |

TABLE III

CONSISTENCY REGULARIZATION

| Ao(·) | A1(·) | GW CER | IAM CER | CVL CER | BT WER |
|-------|-------|--------|---------|---------|--------|
| weak  | None  | 12.37  | 32.65   | 9.96    | 27.78  |
| strong| None  | 16.17  | 44.24   | 9.87    | 26.44  |
| weak  | 11.74 | 32.99  | 11.04   | 30.98   | 7.59   |
| strong| 10.53 | 30.07  | 8.76    | 25.26   | 8.21   | 25.69 | 9.59 | 26.35 |

The first question to raise is whether the output activations are a suitable measure to identify erroneous samples. See Fig. 3, for exemplary prediction results of the initial model solely trained on synthetic data. Furthermore, we weighted the attention masks of the model with the respective character confidence in order to visualize the area of high and low confidence. Qualitatively, it can be observed that characters or parts of words with low confidences coincide with recognition errors. Image areas of low confidence are often ambiguous and generally result in plausible errors. To further underline the expressiveness of the proposed confidence measure, we show error rates over differently confident parts of the datasets in Fig. 5. Lower error rates can be observed in the more confident parts of the dataset, leading to the conclusion that the output activation effectively results in a numeric value of how confident the network is in its prediction.

In a first experiment, we investigate the influence of the confidence measure. See Fig. 4, for an overview on the performance gains achieved with different threshold values on all datasets. Thresholding the confidence measure and only performing training on more confident parts of the dataset,
consistently improve performances compared to training on all samples. Especially, applying a high confidence threshold of $\tau = 0.55$ results in performance gains over all datasets. Note, that tuning the threshold is generally not possible in the application scenario, as a validation set requires labeled sample. Nonetheless, we appreciate that the threshold value seems to be quite independent from the considered dataset and that, in general, thresholding improves performances. Tab. II presents the error rates when a confidence threshold of $\tau = 0.55$ is incorporated in the self-training scheme.

During training, we observe that an increasing number of samples lie above the threshold. To further underline the expressive power of the confidence measure, we conducted the following experiment. During the first 10 cycles of pseudo-labeling, we train on the most confident 60% of the dataset, followed by training on 80% and 100% for another 20 cycles each, respectively. Using predefined portions of the dataset allows to remove the influence of the confidence measure on the number of selected samples. Therefore, it is possible to directly compare a confidence based selection to simply taking random portions of the dataset. While randomly selecting samples achieves similar performances to training on all samples, the proposed confidence measure improves results. Nonetheless, thresholding the confidence measure performs better in most cases and does not introduce any further hyperparameters except the actual threshold value.

D. Consistency Regularization

As shown in Tab. III, introducing consistency regularization leads to performance gains. We report results for extending the training batch by either an additional weakly or strongly augmented version of the training images. In order to account for the higher number of seen samples, we increased the number of self-training cycles to 100 which did not lead to performance gains. Furthermore, we report results for exclusively training on strongly augmented samples. In our experiments, we observe performance gains already when adding a weakly augmented image to the training batch, indicating the regularization power of the consistency approach. Combining strongly and weakly augmented versions and enforcing consistency between them gives the highest performances in our experiments. This is consistent with the results reported for the evolution from MixMatch to FixMatch as investigated in [24]–[26].

E. Comparison

Tab. IV compares our results to the literature. To this end, we use a threshold of $\tau = 0.55$ and apply consistency regularization with weak and strong augmentations. The work of Kang et al. proposes to perform adaptation from synthetic to real data based on an adversarial domain loss [14]. The proposed pseudo-labeling approach significantly outperforms the domain loss strategy proposed in [14]. We argue that the performance differences are mainly due to the different adaptation methods, as we avoided any model differences and report similar performances before adaptation. A drawback of the domain loss strategy proposed in [14] is that it only aims at regularizing the feature space in such a way that synthetic and real samples are indistinguishable. The observed performance gains are then the result of an implicitly improved generalization capability. In contrast, a pseudo-labeling strategy is highly feasible in the handwriting domain, due to heavy constraints on the possible recognition results. A significant portion of the performance gains may be explained by the implicit language model learned from synthetic data which is then exploited during label prediction. Interestingly, the approach also leads to considerable performance gains even when the initial model is comparably poor, as shown in the experiments on BT. This further encourages the consideration of adaptation strategies as considerable improvements can be achieved when compared to models solely trained on related data, as presented in [12].

VI. CONCLUSIONS

In this work, we propose a self-training method for adapting a sequence-to-sequence HTR model from synthetic to real data. We show that it is possible to use the output activations as confidence estimations, which may be exploited to identify more accurate portions of the pseudo-labeled dataset. Adding consistency regularization techniques leads to further performance gains. The proposed approach is superior to the previously investigated adversarial strategy and we report the highest performances on four dataset with respect to training only on synthetic and unlabeled data. Due to the constraints present in language, we encourage the investigation of self-training approaches in handwriting recognition and document analysis in general as a potentially powerful possibility to reduce the data demand of deep learning models.
[41] V. Lavrenko, T. M. Rath, and R. Manmatha, “Holistic word recognition for handwritten historical documents,” in *Int. Workshop on Document Image Analysis for Libraries*, Palo Alto, CA, USA, 2004, pp. 278–287.

[42] M. Villegas, J. Puigcerver, A. H. Toselli, J. Sánchez, and E. Vidal, “Overview of the ImageCLEF 2016 handwritten scanned document retrieval task,” in *Conference and Labs of the Evaluation forum*, vol. 1609, Evora, Portugal, 2016, pp. 233–253.