VISeR: Visual Self-Regularization

Hamid Izadinia*
University of Washington

Pierre Garrigues*
Twitter

Abstract

We propose using large set of unlabeled images as a source of regularization data for learning robust representation. Given a visual model trained in a supervised fashion, we augment our training samples by incorporating large number of unlabeled data and train a semi-supervised model. We demonstrate that our proposed learning approach leverages an abundance of unlabeled images and boosts the visual recognition performance which alleviates the need to rely on large labeled datasets for learning robust representation. In our approach, each labeled image propagates its label to its nearest unlabeled image instances. These retrieved unlabeled images serve as local perturbations of each labeled image to perform Visual Self-Regularization (VISeR). Using the labeled instances and our regularizers we show that we significantly improve object categorization and localization on the MS COCO and Visual Genome datasets.

1. Introduction

Image recognition has rapidly progressed and extremely effective performance is observed using the ImageNet dataset [22, 7, 35, 17]. Despite this progress, ImageNet is biased towards single object images which is in contrast with photos taken by people typically capturing a range of objects in various context. Also, object categories in ImageNet is a subset of the lexical database WordNet [29] which makes it biased to certain categories and does not match the scope of more general image recognition tasks such as object detection and localization in context. MS COCO [25] and Visual Genome [21] provide realistic benchmark for image recognition systems. MS COCO contains ∼300K images and ∼80 object categories, whereas Visual Genome contains 100K images and thousands of categories. CNNs are also showing the best performance on these datasets [34, 21]. MS COCO and Visual Genome are annotated via crowdsourcing platforms such as Amazon Mechanical Turk and hence is time-consuming and expensive to obtain additional labels. However, we have access to huge quantities of unlabeled or weakly labeled images. For example, the Yahoo Flickr Creative Commons 100M dataset (YFCC) [40] is comprised of a hundred million Flickr photos with user-provided annotations such as photo tags, titles, or descriptions.

*Work was done at Flickr, Yahoo Research.

2. Related work

The recognition and detection of objects that appear “in context” is an active area of research. The most common benchmarks for this task are the PASCAL VOC [10] and MS COCO [25] datasets. It has been shown in [33, 38, 9, 3, 42] that it is possible to classify and localize objects using training data without object bounding box information. We refer to this training data as weakly-supervised. The size of labeled...
“objects in context” datasets is typically small. However, we have access to large amounts of unlabeled web images. The YFCC 100M dataset has one hundred million images that have user annotations such as tags, titles, and description. There has been recent efforts to leverage user annotation to build object classifiers. For instance, [18] proposes a noise model that is able to better capture the uncertainty in the user annotations and improve the classification performance. Annotations are used in [19] and [12] as target labels to learn image features and neural networks from scratch. However, classifier performance is lower when training on noisy data. Contrary to these approaches, we propose a form of curriculum learning [4] where we first train a model on a small set of clean data, and then augment the training set by mining instances from a large set of unlabeled images.

While it is shown that by making small perturbations to the input it is possible to make adversarial examples which can fool machine learning models [39, 23, 24], adversarial examples can be used as a means for data augmentation to improve the regularization capability of the deep models. Our method is related to adversarial training techniques [13, 31, 30] in the sense that additional training instances with small perturbations are created and added to the training data. In contrast, we retrieve real adversarial examples from a large set of unlabeled images. Such instances usually correspond to large perturbations in the input space but follow the natural distribution of the data which is analogous to the adversarial perturbations. We call our retrieved image instances as Regularizer and use them to re-train the model and further improve performance.

Using semi-supervised learning, classifiers can be trained via labeled and unlabeled data such as in Naive Bayes, EM algorithm [32], ensemble methods [5] and propagating labels based on similarity as in [43]. In our case, the size of the unlabeled set is three orders of magnitude larger than the labeled set. The size of unlabeled set is critical in order for the label propagation to work effectively; and we propose approximations using MapReduce to make the search practical [6]. Large-scale nearest neighbor search is used for a variety of tasks such as scene completion [16], image editing with the PatchMatch algorithm [2], image annotation with the TagProp algorithm [15], and image captioning [8]. Similarly labels can be propagated using semantic segmentation [14]. This method is applied on ImageNet which has a bias towards a single object appearing in the center of the image. We focus on images where objects appear in context.

3. Proposed Method

Multiple instance learning for multilabel classification: We adopt a fully convolutional neural network architecture [26] which produces the output of a $H \times W \times N$ tensor for $N$ object classes. For each object class the corresponding heatmap provides information about the object location as illustrated in Figure 2. We use VGG16 [36] as base architecture and implement our algorithm via TensorFlow [1].

We are given a set of annotated images $A = \{(x_i, y_i)\}_{i=1,...,n}$, where $x_i$ is an image and $y_i = (y_i^1, \ldots, y_i^N) \in \{0, 1\}^N$ is a binary vector determining which object category labels are present in $x_i$. Let $f^l_i$ be the object heatmap for the $l$th label in the final layer of the network. The probability at location $j$ is given by applying a sigmoid unit to the logits $f^l_j$, e.g. $p^l_j = \sigma(f^l_j)$. We have a weakly labeled setting and do not have access to object locations. We incorporate a multiple instance learning approach with Noisy-OR operation [28, 41, 11]. The probability for label $l$ is given by Equation 1. For learning the parameters of the FCN, we use stochastic gradient descent to minimize the cross-entropy loss $\mathcal{L}$ formalized in Equation 2.

$$p^l = 1 - \prod_{j=1}^N (1 - p^l_j). \quad (1)$$

$$\mathcal{L} = \sum_{l=1}^N -y^l \log p^l - (1 - y^l) \log (1 - p^l) \quad (2)$$

Visual Self-regularization: Deep neural networks are vulnerable to adversarial examples [39]. Let $x$ be an image and $\eta$ a small perturbation such that $||\eta||_\infty \leq \epsilon$. If the perturbation is aligned with the gradient of the loss function $\eta = \epsilon \text{sign}({\nabla}_x \mathcal{L})$ which is the most discriminative direction in the image space, then the output of the network may change dramatically, even though the perturbed image $\tilde{x} = x + \eta$ is virtually indistinguishable from the original. [13] suggests that this is due to the linear nature of deep neural networks and show that augmenting the training set with adversarial examples results in regularization similar to dropout. In Virtual Adversarial Training [31] the perturbation is produced by maximizing the smoothness of the local model distribution around each data point. The virtual adversarial example is the point in an $\epsilon$ ball around the datapoint that maximally perturbs the label distribution around that point as measured by the Kullback-Leibler divergence:

$$\eta = \arg \min_{r:||r||_2 \leq \epsilon} KL[p(y|x, \theta) \parallel p(y|x + r, \theta)] \quad (3)$$

We propose to draw perturbations from a large set of unlabeled images $\mathcal{U}$ whose cardinality is much higher than $A$. For each example $x$, we use the example $\tilde{x}$ that is nearby in the space defined by the penultimate layer in our fully convolutional network. This layer contains spatial and semantic information about the objects present in the image, and therefore $x$ and $\tilde{x}$ have similar semantics and composition while they may be far away in pixel space. We consider the cosine similarity metric to find samples which are close to each other in the feature space and for efficiency we compute the dot product of the L2 normalized feature vectors. Let $\theta$ denote the optimal parameters found after minimizing the cross-entropy loss using the training data in $A$, and $f_0(x)$ be the L2 normalized feature vector obtained from
We are able to run the search in a few hours, with the majority (similar to adversarial training) to find the nearest neighbor to 284x715 Localization: Semi-Supervised Multilabel Object Categorization and 4. Experiments each sample in another sample in then the algorithm will output either no nearest neighbor or not guarantee that we can retrieve the nearest neighbor for the image feature representation. Note that our method does of the time being in the mapper phase where we compute $k$ samples examples are sampled from a similar semantic distribution as opposed to noise. We also used the $\epsilon$ perturbation of each labeled sample in the gradient direction (similar to adversarial training) to find the nearest neighbor in unlabeled set and observed similar performance.

Large scale approximate regularizer sample search: We use MapReduce [6] to find approximate nearest neighbors in a distributed fashion since we use the YFCC dataset with 100 million images for our unlabeled set. We first pre-compute the feature representations $f_\theta(x_i)$ for $x_i \in \mathcal{A}$. The size of $\mathcal{A}$ for datasets such as MS COCO or Visual Genome is small enough that it is possible for each mapper to load a copy into memory. A mapper then iterates over samples $x \in \mathcal{U}$, computes the feature representation $f_\theta(x)$ and its inner product with the pre-computed features in $\mathcal{A}$. It emits tuples for the top $k_m$ matches that are keyed by the index in $\mathcal{A}$, and also contain the index in $\mathcal{U}$ and similarity score. After the shuffling phase, the reducers can select for each sample in $\mathcal{A}$ the $k_r$ closest samples in $\mathcal{U}$. We use $k_m = 1000$ and $k_r = 10$. We are able to run the search in a few hours, with the majority of the time being in the mapper phase where we compute the image feature representation. Note that our method does not guarantee that we can retrieve the nearest neighbor for each sample in $\mathcal{A}$. Indeed, if for a sample $x_i$ there exists $k_m$ samples $x_j$ such that $f_\theta(x_j)^T f_\theta(x_i) \geq f_\theta(x_i)^T f_\theta(x_i)$, then the algorithm will output either no nearest neighbor or another sample in $\mathcal{U}$. However we found our approximate method to work well in practice.

4. Experiments

Semi-Supervised Multilabel Object Categorization and Localization: We use MS COCO [25] and Visual Genome [21] as our source of clean training data and YFCC [40] for the source of unlabeled images with the images presented in Visual Genome or MS COCO discarded from YFCC. The data is 14TB and is stored in Hadoop Distributed File System. We conduct distributed nearest-neighbor search via a CPU cluster. For training and evaluation, we use the standard split used in [25] for MS COCO and only use object category annotations in the Visual Genome.

We evaluate via the object classification and point-based object localization task introduced in [33] and use the mean Average Precision (AP) metric. Tables 1 and 2 summarize classification and localization results on the MS COCO and Visual Genome datasets. We compare our performance with [33, 38, 3]. To handle the uncertainty in object localization, [33] considers the last fully connected layers of the network as convolution layers and a max-pooling layer is used to hypothesize the possible location of the object in the images. In contrast, we use Noisy-OR as our pooling layer. In [38], a multi-scale FCN network called ProNet is proposed that aims to zoom into promising object-specific boxes for localization and classification. Our method uses a single fully convolutional network, is simpler and has a lighter architecture as compared to ProNet. In all tables ‘FullyConn’ refers to the standard VGG16 architecture while ‘FullyConv’ refers to the fully convolutional version of our network (see Figure 2). The Noisy-OR loss is abbreviated as ‘N-OR’, and we denote our algorithm with ViSTeR.

As shown in Table 1, our proposed algorithm reaches 50.64% accuracy in the object localization on the MS COCO dataset which is more than a 4% boost over [38] and a 9.5% boost over [33]. Also, without doing any regularization and by only using Noisy OR (N-OR) paired with a fully convolutional network, we obtain higher localization accuracy than Oquab et al. [33] and different variants of ProNet [38]. In the object classification task, our ViSTeR outperforms baselines of [38, 33] by a margin of more than 4.5% and gains an accuracy of 75.48% for the MS COCO dataset. Other variants of [38] are less accurate than our fully convolutional network architecture with Noisy-OR pooling (‘FullyConv, N-OR’). In Table 1 and 2, we compare three forms of regularization: adversarial training (‘AT’) [13], virtual adversarial training
Table 1. Classification and localization mean AP on MS COCO.

<table>
<thead>
<tr>
<th>Method</th>
<th>Classification</th>
<th>Localization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oquab et al. [33]</td>
<td>62.8</td>
<td>41.2</td>
</tr>
<tr>
<td>ProNet (proposal) [38]</td>
<td>67.8</td>
<td>43.5</td>
</tr>
<tr>
<td>ProNet (chain cascade) [38]</td>
<td>69.2</td>
<td>45.4</td>
</tr>
<tr>
<td>ProNet (tree cascade) [38]</td>
<td>70.9</td>
<td>46.4</td>
</tr>
<tr>
<td>Bency et al. [3]</td>
<td>54.1</td>
<td>49.2</td>
</tr>
<tr>
<td>FullyConn</td>
<td>66.68</td>
<td>–</td>
</tr>
<tr>
<td>FullyConv,N-OR</td>
<td>72.52</td>
<td>47.47</td>
</tr>
<tr>
<td>FullyConv,N-OR,AT [13]</td>
<td>74.38</td>
<td>49.75</td>
</tr>
<tr>
<td>FullyConv,N-OR,VAT [31]</td>
<td>74.30</td>
<td>49.42</td>
</tr>
<tr>
<td>FullyConv,N-OR,ViSER</td>
<td><strong>75.48</strong></td>
<td><strong>50.64</strong></td>
</tr>
</tbody>
</table>

Figure 5. Localization result of ViSER on MS COCO validation.

('VAT') [31], and our Visual Self-Regularization (ViSER) using the YFCC dataset as source of unlabeled images.

Object-in-Context Retrieval: To qualitatively evaluate ViSER, we show several examples of the Regularizer retrieved instances in Figure 4. The unlabeled images retrieved by our approach have high similarity with the queried labeled image. Furthermore, most of the objects in the labeled images also appear in the retrieved images which demonstrates the effectiveness of our label propagation approach.

Figure 1 shows the results of our ViSER approach on the ‘Bus’ category. We visualize the t-SNE [27] grid map [20] of the whole set of images labeled as ‘Bus’ which includes instances from both the labeled images in the MS COCO and unlabeled instances from the YFCC dataset. To produce the t-SNE visualization we take the output of the penultimate layer of our network as explained in Section 3. A different background color (blue vs. green) is assigned to images depending on whether they are from the labeled or unlabeled set. Notice that it is challenging to determine the color corresponding to each dataset as photos are from a similar domain. It suggests that there are many images in the large unlabeled web resources that can potentially be used to populate the fully annotated datasets with more examples.

Figure 5 shows qualitative performance of “FCN,N-OR,ViSER” for multi-label localization. We visualize the object localization score maps with high probability localization regions shown in green and localized objects displayed by red dots. Several examples of the localization score maps produced by “FCN,N-OR” and “FCN,N-OR,ViSER” are shown in Figure 3. We see that “FCN,N-OR,ViSER” can locate both small and big objects more accurately.

Classification on Synthetic Data: To evaluate the ability of our algorithm to leverage unlabeled data to regularize learning, we generate a synthetic two-class dataset with a multimodal distribution as shown via contour visualization of the estimated model distribution in Figure 6. The dataset contains 16 training instances (each class has 8 modes with random mean and covariance for each mode and 1 random sample per mode is selected), 1000 unlabeled and 1000 test samples. We linearly embed the data in 100 dimensions. We use a neural network with two fully connected layers of size 100, each followed by a ReLU activation and optimized via the cross-entropy loss. We compare the generalization behavior of ViSER with the following regularization methods: dropout [37], adversarial training [13], and virtual adversarial training (VAT) [31]. As Table 3 summarizes misclassification test error over 50 runs, our proposed ViSER learns a better local class distribution as adversarial samples follow the true distribution of the data and are less biased to the training instances, compared to the baselines.

Table 2. Classification and localization mean AP on Visual Genome.

<table>
<thead>
<tr>
<th>Method</th>
<th>Classification</th>
<th>Localization</th>
</tr>
</thead>
<tbody>
<tr>
<td>FullyConn</td>
<td>9.94</td>
<td>–</td>
</tr>
<tr>
<td>FullyConv,N-OR</td>
<td>12.35</td>
<td>7.55</td>
</tr>
<tr>
<td>FullyConv,N-OR,AT [13]</td>
<td>13.96</td>
<td>9.05</td>
</tr>
<tr>
<td>FullyConv,N-OR,VAT [31]</td>
<td>13.95</td>
<td>9.06</td>
</tr>
<tr>
<td>FullyConv,N-OR,ViSER</td>
<td><strong>14.82</strong></td>
<td><strong>9.74</strong></td>
</tr>
</tbody>
</table>

Table 3. Classification error on test synthetic dataset (lower is better).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Error(%)</td>
<td>9.24±0.65</td>
<td>9.26±0.71</td>
<td>8.96±0.85</td>
<td>8.94±0.39</td>
</tr>
</tbody>
</table>

5. Conclusion and Future Work

We presented a simple yet effective method to leverage a large unlabeled set accompanied with a small labeled set to train more generalizable representations. Our ViSER approach is able to find Regularizer examples from a large unlabeled set and can achieve significant improvement for visual classification and object localization. In future work, our performance can be further improved by incorporating user provided data such as ‘tags’. Also, our method can be applied for domains beyond visual recognition.
References


