Adapting RANSAC-SVM to Detect Outliers for Robust Classification

Subhabrata Debnath
http://www.cse.iitk.ac.in/~sdebnath

Anjan Banerjee
http://www.cse.iitk.ac.in/~anjan

Vinay Namboodiri
http://www.cse.iitk.ac.in/~vinaypn

Department of Computer Science and Engineering
Indian Institute Of Technology Kanpur
Kanpur
UP, India

In this paper we address the problem of classifying objects where some of the labels in the training data are noisy. This is a common scenario and can be caused by the difficulty of annotation or inadvertently due to human error. In this paper, we consider the wrongly annotated examples to be outliers and try to formulate a robust outlier identification algorithm.

The task of learning a model in the presence of noise has been traditionally solved by the RANSAC algorithm[1]. RANSAC has also been adapted as RANSAC SVM by Nishida and Kurita [3]. The RANSAC-SVM method selects random subsets of the training data and trains small SVMs on them, using the rest of the training data as validation sets. It then chooses the SVM with the smallest validation error to approximate the full training set. However, if the training data is noisy, the validation sets are corrupted, and a faulty submodel may be chosen as optimal.

To address this problem, we propose a modification to RANSAC SVM thereby achieving robustness to noise. The detailed algorithm is given in Algorithm 1.

We are initially given a training set S of n examples from which we draw small random subsets of size k. For each such subset, we train a SVM to obtain a weight vector w_i using the standard support vector formulation given by:

$$\min_{w,b,\xi} \frac{1}{2} w^T w + C \sum_{i=1}^{l} \xi_i \tag{1}$$

$$y_i(w^T \phi(x_i) + b) \geq 1 - \xi_i; \quad \xi_i \geq 0, i = 1, \ldots, l.$$

We then classify the whole set of examples S using w_i and record the predicted labels. The misclassifications that result from this weight vector are aggregated in a vector O of dimension n. The procedure is repeated for many iterations m and examples with misclassifications beyond τ are considered to be outliers. Thus using a quantized score from many models provides us with a better estimate of outlierness.

Algorithm 1 Outlier Robust RANSAC-SVM Adaptation

procedure OUTLIER ROBUST RANSAC-SVM(SetSize k, NumIteration m,Threshold τ)
  for each instance $x_j \in$ Training Set S **do**
    OutlierScore $O(x_j) \leftarrow 0$
  end for
  for i=1 to NumIteration m **do**
    Choose a random $X_i \subset$ Training Set S s.t. $|X_i|$=SetSize k
    $w_i \leftarrow BuildSVMModel(X_i)$ using equation 1.
    $MisclassifiedSet_i \leftarrow GetMisclassifiedInstances(w_i, S)$
    for each instance $x_j \in MisclassifiedSet_i$ **do**
      IncrementByOne(OutlierScore $O(x_j)$)
    end for
  end for
  OutlierSet $S_o \leftarrow \{\}$
  InlierSet $S_i \leftarrow \{\}$
  for each instance $x_j \in$ Training Set S **do**
    if OutlierScore $O(x_j) >$ Threshold τ **then**
      AddToSet(OutlierSet S_o, x_j)
    else
      AddToSet(InlierSet S_i, x_j)
    end if
  end for
  InlierModel $w_{in} \leftarrow BuildSVMModel(InlierSet\ S_i)$
  AdditionalInliers $S_{ai} \leftarrow GetCorrectlyClassifiedInstances(w_{in}, S_o)$
  FinalSet $S_{fi} \leftarrow S_i \cup S_{ai}$
  FinalModel $w_{fi} \leftarrow BuildSVMModel(S_{fi})$
end procedure

We have evaluated our algorithm on the Pascal Voc 2007 dataset. In order to emulate noise, we flipped the labels of 20% of the hardest examples for each of the 20 classes in the dataset. We used distance from the hyperplane as a measure to approximate hardness. The ones closest to the hyperplane are hard in the feature space and are expected to be visually difficult to annotate. We have used linear SVM in all our experiments. To describe each image, we have used responses of the 7th layer of caffe [2] features pre-trained on the Imagenet Large Scale Visual Recognition Challenge 2012 (ILSVRC2012). This gave us a 4096-length feature vector to describe each image. Table shows that using our method we were able to achieve more than 12% improvement over both RANSAC SVM and ordinary SVM.

Our method can also be adapted to identify hard examples in the training data. This is because hard examples are also dissimilar in their feature space as compared to normal examples. Figure 1 shows some of the hard examples identified by our method.

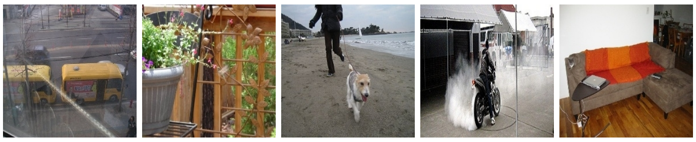

Figure 1: Few visually hard images of VOC 2007 which were detected as outliers by our method. The classes are : bicycle, bird, boat, car and cat

Voc 2007 dataset contains some images labelled as 0 which denote hard positives. We show in table 2 that even after including the 0 labels, we were able to achieve nearly the same performance as normal svm without the 0 labels. Also, our method performed better when 0 labels were not included in both normal svm and our method.

Normal SVM	RANSAC-SVM	Our method
41.2	48.6	62.7

Table 1: Comparison of mean average precision with 20% noisy labels on the Voc 2007 dataset

Normal SVM without 0 labels	Our method with 0 labels	Our method without 0 labels
72.7	72.0	**73.5**

Table 2: Mean average precision of Voc 2007 dataset using normal SVM excluding examples labelled as 0 , our method in the presence of the 0 labelled examples and our method after removing the 0 labelled examples.

Thus we show how a simple adaptation of RANSAC SVM can be used to achieve robustness to noise. We further show how it can be used to detect hard examples in the training data.

[1] Martin A. Fischler and Robert C. Bolles. Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*, 6:381–395, 1981.

[2] Yangqing Jia, Evan Shelhamer, Jeff Donahue, Sergey Karayev, Jonathan Long, Ross Girshick, Sergio Guadarrama, and Trevor Darrell. Caffe: Convolutional architecture for fast feature embedding. In *Proceedings of the ACM International Conference on Multimedia*.

[3] K. Nishida and T. Kurita. Ransac-svm for large-scale datasets. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*.