

Evading the Machine Learning Detector: A Virus Perspective

Group 10
Yuan Xiao, Xiaokuan Zhang

04/27/2017

Abstract

In this project, we use different classification algorithms to classify hand-written digits and pixel-displayed letters. The algorithms we use are Naive Bayes, Support Vector Machine and Artificial Neural Networks. For each algorithm, we tune different parameters in order to achieve a better performance. We use accuracy and F-measure to evaluate the performance. Generally speaking, SVM performs best among the three, and Naive Bayes does not work well.

1 Introduction

1.1 Problem Description

Our group wants to solve the problem of classifying hand-written digits and black-and-white rectangular pixel-displayed letters. We have two datasets from UCI machine learning repository [12]. One is hand-written digits dataset [1]. Another is letter recognition dataset [2]. We will introduce them in more detail in Section 4.

1.2 Classification Algorithms

In this report, we test three machine learning algorithms, i.e., Support Vector Machine (SVM), Neural Networks, and Naive Bayes. We will present the detail of algorithms in Section 3.

1.3 Result Summary

For the hand-written digit dataset, after tuning the parameters, the three classifiers can achieve 98.97%, 93.27%, 92.02% accuracy. For the letter dataset, they can reach 95.33%, 82.77%, 74.18% accuracy. We only submit a pdf file and a tex file to Carmen. For a more detailed view of our repository, please visit our repo on github¹.

¹<https://github.com/XiaokuanOSU/AI2report>

2 Background

The hand-written digit dataset was first used in [11]. In the paper they combined different classifiers to obtain a better performance. The letter recognition dataset was first used in [8]. They generated classification rules to distinguish different letters.

3 Methodology

3.1 Support Vector Machine

Support vector machines (SVMs) [6] are supervised learning models that analyze data for classification or regression. Provided with a set of training examples, which are marked with their belonging categories, a SVM algorithm performs to build a model so as to recognize and assign testing examples to the predicted categories.

Besides linear classification, SVMs are also able to efficiently perform non-linear classification when kernel tricks are applied[4] , which will map original input into high-dimensional attribute space.

3.2 Neural Networks

Neural networks, or artificial neural networks [9], simulate the functions of nerve cells of human brain and serve as an important computational approach in machine learning. They typically form a structure of multiple layers of basic perceptrons and support both supervised and unsupervised learning.

Neural networks have a long history, dating back to the 1940s [13]. However, the idea of artificial neural networks was not popular at early days due to its limitation in solving logical calculations [14]. Modern neural networks revived in the past decade, along with the rise of deep learning [3, 15].

3.3 Naive Bayes

Naive Bayes classifier makes use of the Bayes Theorem. It is basically a conditional probability model. It is one of the simplest machine learning algorithms. Compared to Bayesian Networks, Naive Bayes is technically a special case by assuming that all features are conditionally independent from each other given the class label. One of the earliest papers that described this algorithm was from 1970s [7].

4 Experiment

In this project, we used Weka [10] to test different machine learning algorithms. For SVM, we mainly use LibSVM [5]. For Artificial Neural Network, we choose Multilayer Perceptron. For Naive Bayes, we use the default Naive Bayes in Weka. For each algorithm, we use different parameter settings, which will be covered in this section.

4.1 Datasets

We have two datasets, the hand-written digits dataset [1] and the letter recognition dataset [2]. The hand-written digits dataset has 5620 instances. For each instance, there are 1024 attributes (32x32 matrix), whose values are either 0 or 1. An example is shown in Figure ??, which is clearly a '2'. After grouping every 4x4 blocks, the dimension is reduced to 64 (8x8 matrix), and each attribute ranges from 0 to 16. Another is letter recognition dataset [2]. The character images were based on 20 different fonts. It has 20000 instances. For each instance, there are 16 attributes, whose values range from 0 to 15. The attributes are sophisticated, as shown in Figure ?. Some examples of the fonts are shown in Figure ?. More details of the datasets and features can be found by visiting the links.

4.2 Hand-written Digits Classification

4.2.1 Support Vector Machine

As shown in Figure ??, SVM classifiers provide a good performance on the Digit dataset. In the experiment, two key parameters are tuned. One is the kernel type and the other is the complexity parameter. For kernels, the linear kernel and the non-linear polynomial kernel are tested. When the polynomial kernel is applied, 98.97% accuracy can be achieved, and 97.92% accuracy is achieved in cases of the linear kernel.

From the figure, two results can be observed. Firstly, polynomial kernel has better performance than the linear one, regardless of values of the complexity parameter. Secondly, the complexity parameter has little effect on the SVM model in regards to the Digit dataset.

4.2.2 Neural Networks

In order to understand how the many parameters influence the performance of multilayer perceptron in classification, we decide to change only one parameter at a time. The default setting is "-L 0.3 -M 0.2 -N 500 -V 0 -S 0 -E 20 -H a". And the parameters that we are interested in are learning rate, training time and validation threshold.

Figure ?? shows the average performance for different parameter combinations. For default settings, we have the average accuracy of 92.73%. And the root relative squared error is as low as 38.53%. Changing validation threshold to either more or less does not affect the performance at all. And if we let training time be less, the overall accuracy lowers a little, which matches our expectation.

It can be easily noticed that changing learning rate to 0.6 affects the performance heavily. Thus we tested with the same parameter combination again. In Figure ??, when we ran the test again, the accuracy grew to 98.36%. Such inconsistency in the test result showed that the performance of Multipayer Perceptron is influenced by stochastic. If we increase the stochastic by modifying the parameters, the fluctuation grows.

4.2.3 Naive Bayes

The Naive Bayes works well on the Hand-written Digit dataset. In Figure ??, K means whether to use kernel estimator, and D means whether to use supervised discretization. In Figure ??, when K=F, D=F, which is

the worst case scenario, the accuracy and F-measure are still higher than 90%. In the best case ($K=T$, $D=F$), they both exceeds 92%.

4.3 Letter Recognition

4.3.1 Support Vector Machine

Compared with the Digit dataset, the polynomial kernel still has a good performance on the Letter dataset as more than 95% instances are correctly recognized. However, the accuracy from the linear kernel is much lower no matter which values of the complexity parameter are configured. From Figure ??, we can see that only 85% accuracy and F-measure are achieved when the linear kernel is used, whereas those are more than 97% for the Digit dataset.

To explore an insight of which letters have large contribution to inaccurate recognition, an inaccuracy analysis by class is given (Table ??). Although the accuracy from the polynomial kernel is much higher than the linear one, as shown in Table ??, both of them have least accuracy on recognizing letters 'H', 'S', and 'R'.

4.3.2 Neural Networks

The overall performance of Multilayer Perceptron is quite stable. The accuracy is around 82% and the root relative squared error is around 56%. However, there are some classes with relatively low accuracy making the average performance not so good as digit recognition. Table ?? shows the least correct classes: 'G', 'H' and 'S'.

Neural networks do a better job than the other two algorithms in recognizing 'O' and 'Q' and it can correctly tell 'X' apart from 'S'. Changing learning rate higher helps the performance with 'H'.

4.3.3 Naive Bayes

Naive Bayes does not work well on the Letter Recognition dataset. From Figure ??, we can see that the highest accuracy is lower than 75%. Generally speaking, Naive Bayes is not suitable for classifying letters.

In this dataset, we are also interested in which letters Naive Bayes performs worst. Table ?? shows the top 3 worst cases when using Naive Bayes with different parameters. In all three parameter settings, 'H' is always one of the top 3, which means that 'H' is quite hard to classify for Naive Bayes. Also, the same applies to 'S' and 'X', as they appear in two of the three cases.

5 Discussion

5.1 Evaluation Matrix

In our presentation, we used `root relative squared error` to evaluate the performance of our algorithms and falsely claimed that SVM was not suitable for our datasets. However, it makes little sense to evaluate this feature on non-binary datasets. So in the report, we changed it to F-measure.

5.2 Different Libraries of SVM

In our presentation, we only discussed the performance of the polynomial kernel in SMO. To have a comprehensive understanding on the performance of SVMs, experiments based on LibSVM are performed.

Figure ?? compares the accuracy and F-measure between SMO and LibSVM when the polynomial kernel is applied. Surprisingly, although both the complexity and kernel parameters are configured as the same, the accuracy from LibSVM is higher than that from SMO by 12%.

5.3 Parameters of Multilayer Perceptron

Multilayer Perceptron has a number of parameters. In the project, we would like to look into the following specific parameters: learning rate, training time and validation threshold. Other parameters include momentum, seed, `nominalToBinaryFilter`, `hiddenLayers` etc.

Learning rate (-L) stands for the amount the weights are updated. Training time (-N) is the number of epochs to train through. If the validation set is non-zero then it can terminate the network early. Validation threshold (-E) is used to terminate validation testing. The value here dictates how many times in a row the validation set error can get worse before training is terminated.

In our tests, the validation threshold does not affect the performance.

6 Conclusion

To summarize, our algorithms performs well on the hand-written digit dataset. However, all the algorithms we test have difficulties telling similar letters apart.

In particular, Naive Bayes performs badly in letter recognition when $K=F$, $D=F$. With other parameter settings, the correctness is around 75% with small deviation among different letters. In general, it has a better performance in doing digit classification than in letter recognition.

SVM is generally suitable for both letter recognition and digit classification. It performs best among all the three methods. Similar to another two algorithms, the letter recognition performance is a little worse than digit classification. The classes that cannot be correctly classified are: H, S and R.

Multilayer Perceptron is heavily influenced by the parameters that control the stochastics. But generally speaking, its performance is relatively stable. It is also weak in classifying some of the letters, which are G, H and S.

References

- [1] Optical recognition of handwritten digits data set. <http://archive.ics.uci.edu/ml/datasets/Optical+Recognition+of+Handwritten+Digits>.
- [2] Optical recognition of handwritten digits data set. <https://archive.ics.uci.edu/ml/datasets/Letter+Recognition>.
- [3] Yoshua Bengio. Learning deep architectures for ai. *Foundations and trends® in Machine Learning*, 2(1):1–127, 2009.
- [4] Bernhard E Boser, Isabelle M Guyon, and Vladimir N Vapnik. A training algorithm for optimal margin classifiers. In *Proceedings of the fifth annual workshop on Computational learning theory*, pages 144–152. ACM, 1992.
- [5] Chih-Chung Chang and Chih-Jen Lin. Libsvm - a library for support vector machines, 2001. The Weka classifier works with version 2.82 of LIBSVM.
- [6] Corinna Cortes and Vladimir Vapnik. Support-vector networks. *Machine learning*, 20(3):273–297, 1995.
- [7] Richard O Duda, Peter E Hart, et al. *Pattern classification and scene analysis*, volume 3. Wiley New York, 1973.
- [8] Peter W Frey and David J Slate. Letter recognition using holland-style adaptive classifiers. *Machine Learning*, 6:161, 1991.
- [9] Martin T Hagan, Howard B Demuth, Mark H Beale, and Orlando De Jesús. *Neural network design*, volume 20. PWS publishing company Boston, 1996.
- [10] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H Witten. The weka data mining software: an update. *ACM SIGKDD explorations newsletter*, 11(1):10–18, 2009.
- [11] C Kaynak. Methods of combining multiple classifiers and their applications to handwritten digit recognition. Master’s thesis, Institute of Graduate Studies in Science and Engineering, Bogazici University, 1995.
- [12] M. Lichman. UCI machine learning repository, 2013.
- [13] Warren S McCulloch and Walter Pitts. A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics*, 5(4):115–133, 1943.
- [14] Marvin Minsky and Seymour Papert. Perceptrons: An introduction to computational geometry (expanded edn), 1988.
- [15] Jürgen Schmidhuber. Deep learning in neural networks: An overview. *Neural Networks*, 61:85–117, 2015.