DEPARTMENT OF MATHEMATICS

Data Science and Analytics

May 4th 2020

Contents

List of Figures

List of Tables

1 Abstract

Novelty detection is the term which refers to new or unknown data or signals that a machine learning system is not aware of during training. This is one of the fundamental requirements of a good classification or identification system since sometimes the test data contains information about objects that were not known at the time of training the model.Novelty is the another name of Outliers.Outliers are pervading in many computer vision and pattern recognition problems Automatically eliminating outliers especially from images becomes increasingly important and an interesting research topic, especially for Internet inspired vision applications.Research has shown that various machine learning ways applied on several image datasets which showed significant results so far. In this paper, we propose an approach to deal with the outliers in image data using Autoencoders[1] which is robust and differentiate inliners and outliers.Our approach works under a fully unsupervised manner, differing from traditional one-class learning [9] supervised by known positive labels.Based on the existing work the question aries: How autoencoders can outperform the methods which applied earlier?In other words, To what extent autoencoders can deal with the unlabeled data.By design, first convert the image data(MNIST Image data) into a latent-space with the help of deep-learning neural network using activation functions such as Relu and sigmoid with the use of deep-learning neural networks library keras and tensorflow.Extensive experiments conducted on image dataset, which exhibiting strong robustness at a high outlier proportion up to 70

Word Count:241

Keywords: Outliers, Autoencoders, Keras, Tensorflow

2 Introduction

2.1 Background and Motivation

Images have always played a vital role in humans' life and the vision is all about the sense which again plays an important role. with the rapid growth in the digital world, it becomes very easy to generate huge amounts of images. However, what remains the predominant question is to understand the vision of an image and relate it to the object. For example, the wheel is part of the car? many more such questions. whenever we download huge image data from the web most of the time data we get, is unlabeled, moreover, most of the time half of the data we get is irrelevant which led us to nowhere or may generate an unexpected result, this irrelevant data is term as "Outlier[2] in data". The aim of this paper would precisely to focus on removing the unwanted set of data and only keep the relevant image data. In order to discard irrelevant data,

[1]Dimensionally reduction of data
[2]Unknown data or signal

our approach should firstly to label the data and secondly, as per the label, we can further make a decision if the resulted data should be classified as an outlier or not? As the machine learning field is growing fast there are several techniques suggested. One such method which we apply is "Dimensionally Reduction" data which can function in two ways "Principal Component analysis" and "AutoEncoders". In this paper, the focus area of research is "Detection of outliers in images using AutoEncoders" using Nural Networks[3]. There could be few things that help us to connect an image with the vision for instance 1)Bounding Boxes 2) Semantics of the image. So far, a good amount of research has been done in this field. One such study [4] (Nov 27, 2013) "Never Ending Image Learner(NEIL), NEIL, a computer program that runs 24 hours per day, 7 days per week, forever to: (a) semantically understand images on the web; (b) use this semantic understanding to augment its knowledge base with new labeled instances and common-sense relationships; (c) use this dataset and these relationships to build better classifiers and detectors which in turn help improve semantic understanding. Another study [12] has been made by Imagenet and Visipedia. These studies have proven its results up to specific limits. However, these approaches resulted in certain limitations. This paper has been written to introduce further enhancements.

2.2 Limitations

The above studies mentioned have potential limitations. Firstly, downloading images from Imagenet and visipedia [12]weakened since the images had no bounding boxes[4]. Secondly, the "NEIL" method also could not work since it has a fixed vocabulary. NEIL has discovered more than 1700 relationships and labeled more than 400K visual instances of these categories [12] Building classifiers and manually labeling the images got failed since the downloaded images usually have the irrelevant images/outliers.

2.3 Importance

Therefore, the presented research paper will talk about the idea of automatically downloading images and removing outliers from images. Automatically removing outliers from data approach falls under the unsuervised learning[5], Where methods in literature implicitly or explicitly makes an assumption that inliers located in dense areas and outliers not. These dense areas can be estimated by different methods such as statistical methods, neighbor-based method and reconstruction methods. According to me, "reconstruction method" could be a better fit, again reconstruction can be perform in two ways a)Principal component analysis b)Autoencoders. Autoencoders does the non-linear mapping to the data while PCA does linear mapping.

[3] A Series of algorithms

[4] In digital image processing, the bounding box is merely the coordinates of the rectangular border that fully encloses a digital image

[5] Unlabeled Images

2.4 Main Idea

The main idea behind this research paper is to understand the key issues which the outliers in images. with this paper, I have demonstrated the idea of identify the unwanted noise in the data using autoencoders with keras and tensorflow[6]

Word Count:626

3 Literature Review

With the extensive growth in the field of machine learning many researchers studied variety of techniques for image recognition and introduced useful methods to us. Few researchers defined the term "Outlier" in several ways. Some are below

Barnet and Lewis (Barnett and Lewis, 1994) indicate that an outlying observation, or outlier, is one that appears to deviate markedly from other members of the sample in which it occurs.

Johnson (Johnson, 1992) defines an outlier as an observation in a data set that appears to be inconsistent with the remainder of that set of data.

Now,Before diving into the detection technique the obvious question which arises here is "On what basis we can say if the stated data point is an outlier or not"? Again, Outliers can be in any kind of dataset. The goal of this paper is to demonstrate the outlier detection in image dataset. The labels associated with an image denote if that point is normal or an outlier. Labelling is often done manually by a human expert and hence requires substantial effort to obtain the labelled training data set. Based on the extent to which the labels are available, outlier detection techniques can operate in one of the following modes:

Supervised Outlier Detection: In this technique, the availability of training dataset which has labeled data points for both for normal as well as outlier class. When an unseen data point is compared against the model to label which class it belongs to.

Unsupervised Anomaly Detection: In this technique, we do not require any training data points it is assumed that the normal points are far more frequent than the outlier points. Recently, there has been a rise in this technique.

3.1 Related Work

Unsupervised outlier removal has been extensively studied both inside and outside the computer vision literature.The one-class svm method [6, 11] just treats

[6]Deep Learning Library

all training data as positive and the origin point as negative, and learns a max-margin classifier to arbitrate outliers. The key underlying assumption of these methods can be summarized as: positive data are more densely distributed than outliers.There are a wide variety of methods that use reconstruction error for unsupervised outlier removal such as Principal component analysis(PCA) [7], which dimensionally reduce the size of the dataset and learn projection from the data, which have large high variance treated as outliers.Autoencoders also based on the idea of "Reconstruction error", data with large reconstruction error classify as "outlier" these processes enhanced further to make the reconstruction errors more discriminative.Many methods suggested in the field of "outlier detection in images using unsupervised form" few experiments listed below

Experiment1: Most recently, Liu et al. [8] propose an unsupervised one-class learning (UOCL) method that outperforms all the above methods. UOCL utilizes manifold regularization,balanced soft labels and a max-margin classifier. With the use of these ingredients, UOCL has shown state-of-the-art performance for unsupervised outlier removal.

Experiment 2: One-class svm (OCSVM) .We use the implementation of LibSVM [3]. In this method, the amount of identified outliers is proportional to a parameter v. Since the outlier ratio is unknown before training, we just set v based on ground-truth.(Accuracy of the traning set)

Experiment3: Local outlier factor (LOF) [1]. In this method, we set the neighbor number as 10groundtruth[7] outlier ratio to determine outliers as those with highest outlier factors.

[7] Accuracy of traning data

3.2 Comparative Study

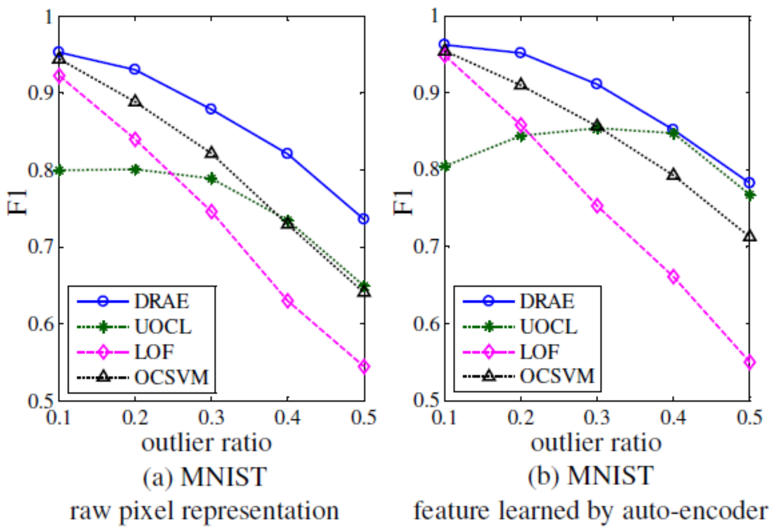

Figure 1: Outlier Ratio Representation
From [12]

1)Comparing AE with LOF and OCSVM, we can see even a naive version of autoencoder outperforms LOF and OCSVM. Note that the outlier ratio is even pre-given for these two methods. This indicates utilizing reconstruction error for unsupervised outlier removal is valid.

2)DRAE also outperforms the state-of-the-art UOCL method, especially at high outlier ratios.

3)Even though the outlier ratio is as large as 70DRAE still achieves a high F1.

Reviewing the literature leads back to the question:Could AutoEncoder be used to improve the accuracy of our anomaly detector?If yes, how AE will outperform all other methods shown above?

Word Count: 723

4 Methodology

To answer the given research question, quantitative methods would be most appropriate to find an answer. Literature on related topics suggests that quantitative methods are most appropriate.By the proposed research paper i will try to answer questions such as Are some deep neural network architectures better than others for anomaly/outlier detection? How autoencoders can be used for anomaly detection using keras, tensorflow and deep learning?

In order to detect the anomalies in the images several approaches have been used so far. However, all those methods are rooted in traditional machine learning.Autoencoders,are a type of algorithm which accepts an input set of data internally, compresses data into latent-space representation and reconstructs the input data from latent representation.To do this task, Autoencoder,accepts two components Encoder: Accept the input and compressed it into latent-space representation. Decoder:attempts to reconstruct the input data from the latent space .Let's look at what autoencoders make so special from an anomaly detection perspective is "Reconstruction Loss".when we train an autoencoder we measure mean squared loss(MSE) between an input image and the reconstructed image from the autoencoder.Firstly, we are going to train our autoencoder on MNIST image dataset.

4.1 Dataset

The MNIST database of handwritten digits [5], available from this page, has a training set of 60,000 examples, and a test set of 10,000 examples. It is a subset of a larger set available from NIST. The digits have been size-normalized and centered in a fixed-size image.There are 4 files:

train-images-idx3-ubyte
train-labels-idx1-ubyte
t10k-images-idx3-ubyte
t10k-labels-idx1-ubyte

Table 1: MNIST Dataset Files

The training set contains 60000 examples, and the test set 10000 examples. The first 5000 examples of the test set are taken from the original NIST training set. The last 5000 are taken from the original NIST test set.we'll be training an autoencoder on the MNIST dataset. The MNIST dataset consists of digits that are 2828 pixels with a single channel, implying that each digit is represented by 28 x 28 = 784 values. The autoencoder we'll be training here will be able to compress those digits into a vector of only 16 values — that's a reduction of nearly 98

4.2 Data Analysis

Let's now suppose that we trained an autoencoder on the entirety of the MNIST dataset

Figure 2: Samples from MNIST Hand Written digit dataset
From [10]

We then present the autoencoder with a digit and tell it to reconstruct it

Figure 3: Reconstructing an image from MNIST dataset
From [10]

Here the autoencoder is able to reconstruct the similar image since we trained the autoencoder already.

4.3 Workflow

Workflow: In order to train [10] an autoencoder we will import tf.keras and NumPy. The class contains 5 essential parameter width: Width of the input images. height: Height of the input images. depth: Number of channels in the images. filters: Number of filters the encoder and decoder will learn, respectively latentDim: Dimensionality of the latent-space representation. Input is then defined for the encoder at which point we use Keras' functional API to loop over our filters and add our sets of CONV - LeakyReLU - BN layers. We then flatten the network and construct our latent vector. The latent-space representation is the compressed form of our data. Now, using the same output will now be used to reconstruct the original input image. Next, using the keras-dense function we will flatten our network and construct the latent vector.In the next step, we will add layers to the network. For that reason,the Activation function Relu[8] has been used(Rectified linear unit) which is generally used in the process of backpropagation.This way we can build our "Encoder".This way,Our encoder begins by accepting a 28x28x1 input volume.In the similar fashion, we can build our decoder as well.A point to note here, when we combine the encoder and decoder to model it into "Autoencoder" we will use sigmoid function as the activation function [10]

4.4 Detect Anomalies in Images

Firstly, we will load our autoencoder and data to make predictions. Important term to note Term:Q-th quartile:The qth quantile of a data set is defined as that value where a fraction of the data is below that value and (1-q) fraction of the data is above that value. compute the q-th quantile of the errors which serves as our threshold to identify anomalies – any data point that our model reconstructed with ¿ threshold error will be marked as an error against the threshold, determines the indices of all anomalies in the data. Thus, any MSE with a value ¿= threshold is considered an outlier.

4.5 Result

Depsite the fact that the autoencoder was only trained on small part of data all 3 digits in the MNIST dataset (67 total samples), the autoencoder does a surpsingly good job [10] at reconstructing them, given the limited data — but we can see that the MSE for these reconstructions was higher than the rest.

4.6 Risks

Deep learning practitioners can use autoencoders to spot outliers in their datasets even if the image was correctly labeled!A recent survey [2],listout the key challenges in this field.

4.7 Future Improvements:

After, reading few research paper i can firmly say that Restricted Boltzmann machine can also do a better job.This works again in a similar fashion. However a bit complex to apply.

Word Count: 840

5 Gantt Chart

Gantt chart is presented below which outlines the planning for my summer project. Project is taking place in the month of June 2020 with the duration of

[8] Activation Function

14 week. Highlights of project planning presented using Horizontal Bar chart also known as "Gantt Chart"

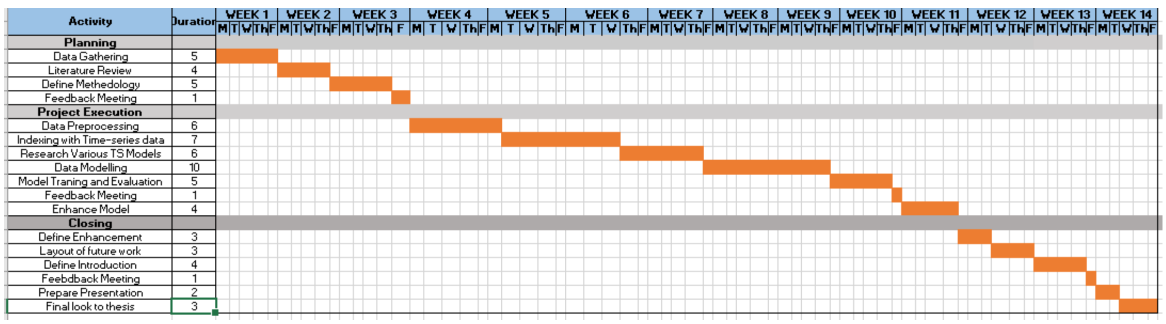

Figure 4: Gantt Chart

References

[1] Markus M Breunig, Hans-Peter Kriegel, Raymond T Ng, and Jörg Sander. Lof: identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, pages 93–104, 2000.

[2] Raghavendra Chalapathy and Sanjay Chawla. Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*, 2019.

[3] Chih-Chung Chang and Chih-Jen Lin. Libsvm: A library for support vector machines. *ACM transactions on intelligent systems and technology (TIST)*, 2(3):1–27, 2011.

[4] Xinlei Chen, Abhinav Shrivastava, and Abhinav Gupta. Neil: Extracting visual knowledge from web data. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 1409–1416, 2013.

[5] Li Deng. The mnist database of handwritten digit images for machine learning research [best of the web]. *IEEE Signal Processing Magazine*, 29(6):141–142, 2012.

[6] Eleazar Eskin, Andrew Arnold, Michael Prerau, Leonid Portnoy, and Sal Stolfo. A geometric framework for unsupervised anomaly detection. In *Applications of data mining in computer security*, pages 77–101. Springer, 2002.

[7] Nathalie Japkowicz, Catherine Myers, Mark Gluck, et al. A novelty de-

tection approach to classification. In *IJCAI*, volume 1, pages 518–523. Citeseer, 1995.

[8] Wei Liu, Gang Hua, and John R Smith. Unsupervised one-class learning for automatic outlier removal. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 3826–3833, 2014.

[9] Manpreet Singh Minhas and John Zelek. Anomaly detection in images. *arXiv preprint arXiv:1905.13147*, 2019.

[10] Adrian Rosebrock. *Deep Learning for Computer Vision with Python: ImageNet Bundle*. PyImageSearch, 2017.

[11] Bernhard Schölkopf, John C Platt, John Shawe-Taylor, Alex J Smola, and Robert C Williamson. Estimating the support of a high-dimensional distribution. *Neural computation*, 13(7):1443–1471, 2001.

[12] Yan Xia, Xudong Cao, Fang Wen, Gang Hua, and Jian Sun. Learning discriminative reconstructions for unsupervised outlier removal. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 1511–1519, 2015.

I would like to mention, Please refer the link: `https://www.pyimagesearch.com/2020/03/02/anomaly-detection-with-keras-tensorflow-and-deep-learning/` for methodology mentioned in this paper.