Unsupervised out-of-distribution detection using kernel density estimation

Ertunc Erdil  Krishna Chaitanya  Ender Konukoglu

Computer Vision Lab, ETH Zurich
Sternwartstrasse 7, Zurich 8092, Switzerland
ertunc.erdil@vision.ee.ethz.ch

Abstract

Deep neural networks achieve significant advancement to the state-of-the-art in many computer vision tasks. However, accuracy of the networks may drop drastically when test data come from a different distribution than training data. Therefore, detecting out-of-distribution (OOD) examples in neural networks arises as a crucial problem. Although, majority of the existing methods focuses on OOD detection in classification networks, the problem exist for any type of networks. In this paper, we propose an unsupervised OOD detection method that can work with both classification and non-classification networks by using kernel density estimation (KDE). The proposed method estimates probability density functions (pdfs) of activations at various levels of the network by performing KDE on the in-distribution dataset. At test time, the pdfs are evaluated on the test data to obtain a confidence score for each layer which are expected to be higher for in-distribution and lower for OOD. The scores are combined into a final score using logistic regression. We perform experiments on 2 different classification networks trained on CIFAR-10 and CIFAR-100, and on a segmentation network trained on Pascal VOC datasets. In CIFAR-10, our method achieves better results than the other methods in 4 of 6 OOD datasets while being the second best in the remaining ones. In CIFAR-100, we obtain the best results in 2 and the second best in 3 OOD datasets. In the segmentation network, we achieve the highest scores according to most of the evaluation metrics among all other OOD detection methods. The results demonstrate that the proposed method achieves competitive results to the state-of-the-art in classification networks and leads to improvement on segmentation network.

1 Introduction

Deep neural networks (DNNs) can perform predictions on test images with very high accuracy when the training and testing data come from the same distribution. However, the prediction accuracy decreases rapidly if the test image is sampled from a different distribution than the training data. Furthermore, DNNs make predictions in such cases with high confidence [1]. This creates a big obstacle when deploying neural networks for real applications especially the ones which have zero tolerance for error such as autonomous driving and medical diagnosis. Therefore, it is crucially important to improve the robustness of the DNN architectures and prevent them from making big mistakes [2]. Detection of OOD samples can play a key role for building such architectures. Despite the success of existing OOD detection methods in the literature, most of them are designed to operate on classification networks. However, OOD detection is important not only for classification networks but also for the other ones such as segmentation and detection.

Preprint. Under review.
Recently, Lee et al. proposed an OOD detection method named as “Mahalanobis” in [18] that achieved the state-of-the-art results for OOD detection for image classification networks. The method assumes that the class conditional pdfs of the features at the intermediate layers of a DNN can be represented by a Gaussian density for the in-distribution data. The parameters of each class conditional Gaussian are estimated by computing the empirical mean and co-variance using the in-distribution training images and the corresponding class labels. At test time, a test image is evaluated at the estimated densities to obtain a confidence score to be used for OOD detection, which is expected to be higher for in-distribution and lower for OOD.

Motivation: Lee et al. [18] present state-of-the-art results on classification networks trained on a number of computer vision benchmark datasets. Despite the success of [18], there are two important points that limit its application on tasks other than classification: 1) Estimating class conditional densities of image features requires class label information of images which may not be available for the tasks other than classification. 2) Gaussian assumption about the class conditional densities in the feature space may not hold for some datasets which can diminish performance. These points motivate us to extend [18] and propose a new OOD detection method that can be used in non-classification DNNs as well as the classification ones, and does not need make any assumption about the underlying pdfs of the feature spaces.

Contribution: In this paper, we propose an unsupervised OOD detection method using kernel density estimation. The proposed method estimates the pdfs of features obtained at different layers of DNNs using kernel density estimation (KDE) [22]. Our method extends [18] by estimating the feature densities using KDE which eliminates the need for using class labels and making parametric assumption about the underlying pdf, unlike the Gaussian assumption in [18], for the feature space. Therefore, our method can be used for OOD detection in both classification and non-classification DNNs.

Once the pdfs at different layers of a DNN are estimated using the in-distribution training images, a test image is evaluated at the densities to obtain a confidence score from each layer. Analogous to [18], the proposed method trains a logistic regression classifier for OOD detection from the computed scores. Lee et al. [18] use adversarially perturbed images to simulate OOD images when training the classifier. In addition to this strategy, one can have access to many different datasets that are known to be OOD for a DNN model which can also be used for training. In our experiments, we use both strategies and investigate its effect on the OOD detection performance.

Performing KDE for high dimensional data is non-trivial [24]. One reason of this is the difficulty of determining the optimal kernel sizes for each training data sample that is used in density estimation. We use the k-nearest neighbor method for determining kernel sizes [25] whose parameter is k itself. In this paper, we propose a method to automatically determine the optimal k value to eliminate the need for an exhaustive search to find the optimal kernel sizes.

We perform experiments on 2 different classification networks trained on CIFAR-10 and CIFAR-100 datasets [16] by using 6 different computer vision datasets as OOD. We compare the results with 3 different OOD detection methods proposed by Hendryks et al. [13], Liang et al. [19], and Lee et al. [18] which are primarily designed for OOD detection in classification networks.

In addition to the classification experiments, we perform experiments on a segmentation network trained on Pascal VOC dataset [10] by using 4 different semantic segmentation datasets as OOD. We compare the proposed method with the modified version of [18] and a recent OOD detection work [14] that also does not require image labels.

2 Related work

There have been recent efforts for developing OOD detection methods for DNNs in the literature. Hendrycks and Gimpel [13] propose a baseline that exploits probabilities from softmax outputs of a classification network for detecting misclassified and OOD examples. Liang et al. [19] propose a method called ODIN that uses the softmax scores as in [13]. Before computing the scores, they scale the inputs of softmax with a constant called temperature scaling and apply a small adversarial perturbation to the input which aim to further increase the distance between in and out-of-distribution examples. DeVries and Taylor [8] introduce a confidence estimation branch (CEB) that is used along with softmax probabilities. The network is trained such that softmax probabilities are updated...
We denote the mean feature vector obtained at the lth layer of a DNN by \( \hat{x}_l \). This is derived from \( x_{tr_l} \) by taking the mean of each channel separately. For example, for a feature map with dimensions \( D \times H \times W \), where \( D \) is height, \( H \) is width, and \( W \) is depth, we obtain \( D \times 1 \) vector \( y_{tr_l} \) by taking the mean of each channel. Weights of logistic regression classifier: \( \alpha_l \) are obtained using (4.1). OOD detection using the proposed method for a test image \( x \) is defined as follows:

\[
\hat{x}_l = \frac{1}{N} \sum_{i=1}^{N} K(||f_l(x) - f_l(x_u)||_1; \sigma_l^2)
\]

Output: Confidence score of \( x \): \( C_x \).

**Algorithm 1:** OOD detection using the proposed method for a test image \( x \).

**Input:** Test Image: \( x \).
- Random subset of training images: \( \bar{X}_{tr_l} = \{x_{u1}, x_{u2}, \ldots, x_{uN}\} \);
- Weights of logistic regression classifier: \( \alpha_l \);
- Set of kernel sizes: \( \sigma_l \).

**Output:** Confidence score of \( x \): \( C_x \).

```python
for l ← 1 to L do
    Perform KDE at layer \( l \): \( \hat{p}_l(x) = \frac{1}{N} \sum_{i=1}^{N} K(||f_l(x) - f_l(x_u)||_1; \sigma_l^2) \)
end
return \( C_x = \sum_{l=1}^{L} \alpha_l \hat{p}_l(x) \)
```

### 3.1 Computing the confidence scores

KDE is a nonparametric density estimation method that estimates the underlying pdf of data through its samples without requiring any label information nor parametric assumption about the underlying pdf. In the proposed method, we estimate the pdfs of in-distribution dataset in the feature spaces obtained at the intermediate layers of a DNN using KDE. However, direct application of KDE to the feature spaces of a large network is challenging. The feature spaces can be very high dimensional in DNNs and performing KDE on high dimensions is non-trivial due to curse of dimensionality [24]. In order to reduce the dimensions, we do not use the feature maps directly but use their channel-wise mean. For example, for a feature map with dimensions \( C \times H \times W \) where \( C \) is number of channels, \( H \) is height, and \( W \) is width, we obtain \( C \times 1 \) vector by taking the mean of each channel separately. We denote the mean feature vector obtained at the \( l^{th} \) layer of a DNN by \( f_l(x) \) for an input image \( x \). KDE has been defined over the distances between data samples to deal with the high dimensional data in different applications [5,15]. We follow a similar procedure when defining the pdf at the \( l^{th} \)
We empirically demonstrate that this assumption holds in many test cases and the confidence score
$p_l(x) \approx \hat{p}_l(x) = \frac{1}{M} \sum_{i=1}^{M} \mathcal{K}(d(f_l(x), f_l(x_i)); \sigma^l_l)$(1)
where $p_l$ is the true density of $f_l$ and $\hat{p}_l$ is its estimation using KDE, $d(\cdot, \cdot)$ is a distance function
between the features, and $\mathcal{K}(\cdot; \sigma^l_l)$ is the kernel with kernel size $\sigma^l_l$. In the proposed method, we
choose $\mathcal{K}$ as 1D Gaussian kernel with zero mean. We describe how we set the kernel size $\sigma^l_l$ in Sec. 3.3 in more
detail.

Note that, in order to estimate $p_l$ in Eq. (1), KDE needs to remember all in-distribution training images
in $X_{tr}$. However, in real applications where $M$ can be very large, storing $X_{tr}$ may not be feasible
and the summation over $M$ images in Eq. (1) can take very long. Improving the computational and
memory efficiency of KDE-based methods are possible by defining an unbiased estimator [9]. We
achieve this by selecting a random subset of $X_{tr}$ such that
$\tilde{X}_{tr} = \{x_{u_1}, x_{u_2}, \ldots, x_{u_N}\} \subset X_{tr}$
where $\{u_1, u_2, \ldots, u_N\} \subset \{1, 2, \ldots, M\}$ is a random subset of indices generated by sampling from
a Uniform density, $\mathcal{U}(1, M)$, without replacement and $N << M$. Using the random subset, we
replace the unbiased estimator in Eq. (1) with a computationally more efficient unbiased estimator
$p_l(x) \approx \tilde{p}_l(x) = \frac{1}{N} \sum_{i=1}^{N} \mathcal{K}(d(f_l(x), f_l(x_{u_i})); \sigma^l_l).$(2)

In Eq. (2), as the distance metric $d(\cdot, \cdot)$ we use the $L_1$, i.e. $d(f_l(x), f_l(x_{u_i})) = \|f_l(x) - f_l(x_{u_i})\|_1$
in our experiments. One can consider using other distance metrics such as $L_2$ which we investigate
in some experiments presented in the supplementary material.

Once we obtain the confidence scores $\tilde{p}_l(x)$ for each layer $l$, we compute the final confidence score as
$C_x = \sum_{l=1}^{L} \alpha_l \tilde{p}_l(x)$ (3)
where $\alpha_l$ are the parameters of a logistic regression classifier which we describe next in Sec. 3.2.

3.2 Learning logistic regression parameters $\alpha_l$

The proposed method computes the final confidence score $C_x$ from the scores predicted at each layer
$l$ using a logistic regression classifier with parameters $\alpha_l$ (see Eq. (3)). Training the classifier to learn
$\alpha_l$ requires having access to both in-distribution and OOD images. Although, the in-distribution
images, $X_{tr}$, are already available, it is difficult to capture all possible images not included in $P_{in}$. Lee et al. [13]
propose using adversarial examples as samples from $P_{out}$ to train a similar classifier. Another alternative could be using other datasets that are freely available and are known to be OOD.

In our experiments, we investigate the effect of both approaches on the OOD detection performance.
Once the OOD samples are obtained using one of the approaches, the classifier is trained by giving
the confidence scores $\tilde{p}_l$ as input where the labels are provided as positive for in-distribution images
and negative for the OOD ones.

The classifier is trained to distinguish the scores $\tilde{p}_l(x)$ of in-distribution images from the OOD ones.
As described above, this is achieved by using only a set of samples from $P_{out}$. Even though the OOD
space is very large to capture with such a small sample set, we have a prior knowledge that most of
the images in the OOD space are likely to produce lower scores than the in-distribution ones. The
classifier trained on the scores places a decision boundary between the lower and the higher scores,
and the assumption is that the boundary generalizes for most of the in-distribution and OOD images.
We empirically demonstrate that this assumption holds in many test cases and the confidence score
obtained by the classifier $C_x$ is better than the individual scores of the layers $\tilde{p}_l(x)$ for OOD detection.

3.3 Determining kernel size

Kernel size, $\sigma$, is a crucial parameter of KDE since it significantly effects the shape of the estimated
density. Setting $\sigma$ to a large value leads to very smooth pdfs, reducing the likelihood of the observed
samples as well as other samples from the same distribution. On the other hand, setting $\sigma$ to a very small value leads to very peaky distributions only attributing high probability to observed samples, assigning very low probability to unobserved samples from the same distribution.

Therefore, finding an optimal $\sigma$ value is quite important in order to capture the underlying pdf of data [24].

In the proposed method, as given in Eq. (2), we use a different $\sigma^l_i$ value for each training sample $x_i$ used for fitting a KDE and at each layer $l$.

We compute $\sigma^l_i$ using the $k$-nearest neighbor method ($k$NN) [25]. More specifically, we compute the distance between $f_l(x_i)$ and $f_l(x_j)$ for all $j \in [1, N], i \neq j$ and set $\sigma^l_i$ as the $k^{th}$ smallest value. We denote the set of all $\sigma^l_i$ values by $\sigma$.

A parameter of the $k$NN method is the $k$ itself. We propose a method to automatically select the most appropriate $k$ value from a set of candidate values denoted by $k$. In this method, we use the training images in $X_{tr}$ and their adversarially perturbed version $X_{adv}$ to select the $k \in k$ that maximizes the following quantity

$$k_l = \arg \max_{k \in k} \sum_{x \in X_{tr}} \hat{p}_l(x) - \sum_{x' \in X_{adv}} \hat{p}_l(x')$$

where $k_l$ indicates the optimum $k$ value in layer $l$. In this method, we aim to find a $k$ value that yields the highest difference between the in-distribution data and the simulated OOD data $X_{adv}$. In our experiments, we choose $k_l$ from the candidate set $k = \{10, 20, 50, 100, 200, 300, 350, 400, 450, 500\}$ using the described method.

4 Experimental results

4.1 Datasets and network architectures

We evaluate the performance of the proposed approach on both classification and segmentation networks, and compare with the state-of-the-art OOD detection methods. In the classification experiments, we use two different networks that are trained on CIFAR-10 and CIFAR-100 [16] which contain images from 10 and 100 classes, respectively. Both datasets contain 50000 training and 1000 test images where each one is a $32 \times 32$ color image. We compare the proposed method with the Baseline method [12], ODIN [19], and Mahalanobis [18] which are primarily designed for OOD detection in classification networks. We perform OOD detection on the ResNet [12] models trained on CIFAR-10 and CIFAR-100 by Lee et al. [18] using all method [4].

We use 6 different datasets as OOD: SVHN [21] contains 26032 images of house numbers in Google street-view images. Resized TinyImageNet (Tin-rs) and cropped TinyImageNet (Tin-cr) consist of 10000 $32 \times 32$ RGB test images which are obtained by resizing and cropping a subset of the original ImageNet dataset [7], respectively. Resized LSUN (LSUN-rs) and cropped LSUN (LSN-cr) contain 10000 RGB test images with size $32 \times 32$ and they are obtained by resizing and cropping a subset of the original LSUN dataset [29]. iSUN is a subset of SUN data set [27] that contains 8925 RGB images resized to $32 \times 32$.

In the experiments on segmentation networks, we train a DeepLabV3 [3] architecture that has ResNet [12] as a backbone network on Pascal VOC dataset [10]. Pascal VOC dataset contains 14644 annotated training images and 1449 test images. We compare the proposed method with 2 different ODD detection methods: modified version of Mahalanobis [18] and the self-supervised learning-based (SSL) method proposed in [14]. Mahalanobis is originally designed for OOD detection in classification networks and it requires class labels for each image in the in-distribution dataset. In order to modify Mahalanobis for non-classification networks, we assign the same label to all images. We use the same DeepLabV3 network to evaluate the modified Mahalanobis. SSL uses a self-supervised rotation network for OOD detection. Since SSL performs OOD detection on a network that is independent from the main network, it can be used for both classification and non-classification networks. In order to compare with SSL [14], we randomly rotate the training images in Pascal VOC

---

1 Pretrained models are available at https://github.com/pokaxpoka/deep_Mahalanobis_detector
2 Tin-rs, Tin-cr, LSUN-rs, LSUN-cr, and iSUN are available at https://github.com/facebookresearch/odin
3 The model parameters will be made available.
dataset and train a neural network that predicts the rotation angle using a ResNet architecture. Then, the confidence scores for OOD detection are obtained for a test image by taking the maximum of the softmax probabilities as proposed in [14] for classification networks.

In these experiments, we use 4 different datasets as OOD. KITTI [1] is a semantic segmentation dataset that contains 200 test images of street scenes. Berkeley Deep Drive (BDD) [28] also contains images of street scenes similar to KITTI and includes 2000 test images. COCO [20] and Places [30] are the other semantic segmentation datasets that we use as OOD which contains 17124, and 328500 test images, respectively. We use a random subset of 10000 images of the Places dataset in our experiments for computational purposes.

4.2 Evaluation methods

We used the same evaluation methods that have been commonly used for evaluation OOD detection methods in the literature [13,19,18]. Note that in all methods, we take the in-distribution as positive class and out-of-distribution as negative class.

**FPR at 95% TPR:** False positive rate (FPR) is measured when the true positive rate (TPR) of 95% is reached at a certain threshold. The false positive rate is calculated as FPR=FP/(FP+TN) and true positive rate is calculated as TPR=TP/(TP+FN) where TP, FP, TN, and FN represent true positive, false positive, true negative, and false negative, respectively.

**Detection error:** This metric measures the probability of wrong classification when TPR is 95%. We denote the detection error by $P_{err}$ and compute as $P_{err}=0.5(1-TPR+FPR)$.

**AUROC:** The Area Under the Receiver Operating Characteristic curve (AUROC) is a threshold independent method that measures the area below Receiver Operating Characteristic (ROC) curve [6]. ROC curve reflects the relationship between TPR and FPR values as the threshold changes. AUROC takes its highest value at 100% when the detection is perfect.

4.3 Quantitative results

In this section, we present the quantitative results obtained on both classification and segmentation networks introduced in Sec. 4.1.

In the classification experiments, we compare the proposed method with 3 best performing methods from the recent literature on 6 OOD datasets. ODIN and Mahalanobis methods have important parameters that significantly effect their performance. We choose these parameters from the list of values given in the original papers by using a validation set that contains in-distribution training images and their adversarially perturbed versions. The best-performing parameters in terms of FPR at 95% TPR are chosen for each in-distribution dataset. For the proposed method, we set $N=1000$ in both classification and segmentation experiments. We investigate the performance of the proposed method as a function of $N$ in the supplementary material.

In Table 1, we present the quantitative OOD detection results on a network trained on CIFAR-10 dataset. Note that there are two different results for both Mahalanobis and the proposed method in each OOD dataset in the table. We present results for each strategy that we use to sample OOD images for training the logistic regression classifier as discussed in Sec. 3.2. In Table 1, the first row of each OOD dataset correspond to the results obtained by training the classifier using adversarial images (e.g. FPR at 95% TPR result is 2.44 for SVHN) whereas the second one correspond to training by using the remaining OOD datasets (e.g. FPR at 95% TPR result is 12.63 for SVHN). Note that in the latter one, we exclude the target OOD dataset and use the remaining ones for training. For example, when SVHN is OOD dataset, OOD examples to train the logistic regression are chosen from TIN-rs, TIN-cr, LSUN-rs, LSUN-cr, and iSUN.

According to the quantitative results in Table 1, the proposed method with logistic regression on adversarial examples achieves better results than the remaining three methods in SVHN, TIN-rs, LSUN-rs, and iSUN datasets. When we train the logistic regression classifier on the other OOD datasets, we achieve the best results on TIN-rs, LSUN-rs, and iSUN datasets. In the all other cases, we obtain the second best results among all methods.

These parameters are temperature scaling and perturbation magnitude for ODIN and only the perturbation magnitude for Mahalanobis.
Table 1: Quantitative results on distinguishing test set of CIFAR-10 in-distribution data set from several out-of-distribution data sets. ↑ indicates larger value is better and ↓ indicates lower value is better. All values are percentages. Note that we present 2 different results for both Mahalanobis and Ours for each OOD dataset. These results correspond to the ones obtained by regression using adversarial examples and the remaining OOD datasets, respectively as discussed in Sec. 3.2.

Logistic regression classifier is an important part of the proposed method which improves the OOD detection performance of the individual intermediate layers. In order to demonstrate this, we present FPR at 95% TPR results obtained in each layer that we use in CIFAR-10 experiments on all OOD datasets in Table 2. The results demonstrate that there is no significant difference between using adversarial or OOD examples when training the logistic regression classifier in the experiment with CIFAR-10 dataset. Both methods improves the results of the intermediate layers in almost all OOD datasets.

| Layer | SVHN | TIN-rs | TIN-cr | LSUN-rs | LSUN-cr | iSUN |
|-------|-------|--------|--------|---------|---------|------|
| 1     | 81.73 | 88.11  | 49.26  | 87.62   | 51.44   | 89.6 |
| 2     | 10.68 | 16.26  | 46.41  | 9.48    | 33.04   | 17.62|
| 3     | 3.85  | 23.93  | 68.62  | 17.18   | 43.02   | 19.50|
| 4     | 45.65 | 83.15  | 99.72  | 79.67   | 97.64   | 78.62|
| 5     | 26.90 | 24.5   | 27.08  | 19.77   | 18.96   | 20.67|
| Adversarial | 12.63 | 4.61   | 17.56  | 2.86    | 7.57    | 4.19 |
| OOD   | 2.44  | 5.11   | 25.74  | 2.54    | 13.48   | 3.83 |

Table 2: OOD detection results obtained by using the scores at the intermediate layers and the combined results using logistic regression. “Adversarial” and “OOD” refer to training the logistic regression using adversarial samples and the remaining OOD datasets, respectively.

In Table 3 we present the quantitative results obtained on the network trained on CIFAR-100 dataset. OOD detection on the CIFAR-100 network is more difficult compared to the CIFAR-10 experiments. We believe this is because CIFAR-10 network has higher classification accuracy on its in-distribution data (∼ 98%) than the CIFAR-100 network (∼ 80%). This leads to diminished performance in all OOD detection methods. In CIFAR-100 experiments, our method with logistic regression trained on adversarial examples gets the 2nd place on SVHN, TIN-rs, LSUN-rs and iSUN, the 3rd place on TIN-cr and LSUN-cr datasets. When we use the other OOD datasets in logistic regression, our results improve on TIN-rs (from 3rd place to 2nd), LSUN-rs, iSUN (from 2nd place to 1st), and LSUN-cr (from the last place to 2nd) datasets.

We observe that training the logistic regression using the remaining OOD datasets leads to better results compared to using adversarial examples in CIFAR-100 dataset. In particular, FPR at 95% TPR results improve almost 2 and 3 times in TIN-cr and LSUN-cr datasets, respectively. This demonstrate that using the freely available datasets that are known to be OOD could be very useful in OOD detection.
OOD FPR at 95% TPR ↓ Detection Error ↓ AUROC ↑

Baseline [13] / ODIN [19] / Mahalanobis [18] / Ours

SVHN 55.73 / 24.76 / 9.00 / 24.09 30.36 / 14.88 / 7.00 / 14.54 79.34 / 92.13 / 97.63 / 94.66
- / - / 11.87 / 25.76 - / - / 8.43 / 15.38 - / - / 96.38 / 90.41

TIN-rs 58.97 / 33.74 / 24.90 / 34.08 31.98 / 19.37 / 14.95 / 19.54 77.07 / 88.32 / 94.63 / 93.59
- / - / 22.80 / 28.83 - / - / 13.90 / 16.91 - / - / 95.40 / 92.37

TIN-cr 52.69 / 26.85 / 44.24 / 93.99 28.84 / 15.92 / 58.50 / 67.12 9.24 / 45.29 / 51.37
- / - / 27.08 / 56.89 - / - / 13.15 / 12.97 - / - / 84.93 / 77.31

LSUN-rs 64.71 / 37.09 / 26.66 / 28.47 34.85 / 21.04 / 15.83 / 16.73 75.58 / 87.77 / 93.08 / 94.55
- / - / 21.31 / 20.95 - / - / 18.79 / 18.34 - / - / 95.11 / 93.57

LSUN-cr 66.95 / 34.78 / 32.58 / 84.90 35.97 / 19.89 / 10.95 / 44.95 77.19 / 88.94 / 92.19 / 96.50
- / - / 16.91 / 31.69 - / - / 18.79 / 18.34 - / - / 95.93 / 91.13

iSUN 63.26 / 38.21 / 28.86 / 33.49 34.13 / 21.60 / 16.93 / 19.24 75.68 / 86.73 / 93.31 / 93.90
- / - / 26.05 / 25.86 - / - / 15.52 / 15.43 - / - / 94.50 / 92.76

Table 3: Quantitative results on distinguishing test set of CIFAR-100 in-distribution data set from several OOD data sets.

The quantitative results of the segmentation experiments are shown in Table 4. The results demonstrate that the proposed method achieves better OOD detections than the modified Mahalanobis and SSL according to most of the evaluation methods. KITTI and BDD datasets contain street view images and look visually different than the Pascal VOC. On the other hand, COCO and Places datasets are quite similar to Pascal VOC which represent a very challenging case for OOD detection. The proposed method achieves a clear improvement over the other two methods on KITTI and BDD datasets according to all evaluation methods. Although, the performance of our method decreases in COCO and Places datasets, it performs quite similarly with the other methods in this challenging case.

We note that the quantitative results that we obtain in the segmentation experiments are quite low compared to the classification experiments for all OOD detection methods. The modified Mahalanobis tries to model the whole in-distribution dataset using a single Gaussian distribution because the image-level class information is not available. Pascal VOC is a complex dataset and a single Gaussian may not be sufficient for its representation which leads to worse results compared to the proposed method. The proposed method improves the performance to some extent by learning a more representative density function in a non-parametric manner. The other method, SSL, uses the softmax probabilities of an auxiliary rotation task for OOD detection. Neural networks may not need to capture the content of the images in order to perform well on a rotation task. This can explain why rotation network do not achieve good OOD detection results.

Table 4: Quantitative results on distinguishing test set of Pascal VOC in-distribution data set from several OOD data sets.

5 Conclusion

In this paper, we presented an unsupervised OOD detection method using kernel density estimation. The proposed method learns the pdfs of features in the intermediate layers of a DNN using KDE and performs OOD detection by evaluating the test images at the estimated pdfs. KDE does not require
class label information of images for density estimation and does not make any parametric assumption about the underlying pdf of data. Thus, the proposed method can be applied to both classification and non-classification DNNs unlike most of the existing methods in the literature. We present experimental results on two different classification networks and on a segmentation networks. The results demonstrate that the proposed method achieves very competitive OOD detection performance with the state-of-the-art methods on classification networks. Additionally, we present experiments on a segmentation network and we observe that OOD detection in segmentation networks is a more challenging problem than classification network. Although, the proposed method achieves quite clear improvements over the existing methods in some of the segmentation experiments, we believe that the problem is quite challenging and there are still room for improvement in a future research.

Acknowledgements

The presented work was partly funding by: 1. Personalized Health and Related Technologies (PHRT), project number 222, ETH domain. 2. Clinical Research Priority Program Grant on Artificial Intelligence in Oncological Imaging Network, University of Zurich, 3. Swiss Data Science Center (DeepMicroIA), We also thank Nvidia for their GPU donation.

References

[1] Alhaija, H.A., Mustikovela, S.K., Mescheder, L., Geiger, A., Rother, C.: Augmented reality meets computer vision: Efficient data generation for urban driving scenes. International Journal of Computer Vision 126(9), 961–972 (2018)
[2] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., Mané, D.: Concrete problems in ai safety. arXiv preprint arXiv:1606.06565 (2016)
[3] Chen, L.C., Papandreou, G., Schroff, F., Adam, H.: Rethinking atrous convolution for semantic image segmentation. arXiv preprint arXiv:1706.05587 (2017)
[4] Cordts, M., Omran, M., Ramos, S., Rehfeld, T., Enzweiler, M., Benenson, R., Franke, U., Roth, S., Schiele, B.: The cityscapes dataset for semantic urban scene understanding. In: Proceedings of the IEEE conference on computer vision and pattern recognition. pp. 3213–3223 (2016)
[5] Cremers, D., Osher, S.J., Soatto, S.: Kernel density estimation and intrinsic alignment for shape priors in level set segmentation. International journal of computer vision 69(3), 335–351 (2006)
[6] Davis, J., Goadrich, M.: The relationship between precision-recall and roc curves. In: Proceedings of the 23rd international conference on Machine learning. pp. 233–240. ACM (2006)
[7] Deng, J., Dong, W., Socher, R., Li, L.J., Li, K., Fei-Fei, L.: Imagenet: A large-scale hierarchical image database. In: 2009 IEEE conference on computer vision and pattern recognition. pp. 248–255. Ieee (2009)
[8] DeVries, T., Taylor, G.W.: Learning confidence for out-of-distribution detection in neural networks. arXiv preprint arXiv:1802.04865 (2018)
[9] Erdil, E., Yildirim, S., Tasdizen, T., Cetin, M.: Pseudo-marginal mcmc sampling for image segmentation using nonparametric shape priors. IEEE Transactions on Image Processing 28(11), 5702–5715 (2019)
[10] Everingham, M., Van Gool, L., Williams, C.K., Winn, J., Zisserman, A.: The pascal visual object classes (voc) challenge. International journal of computer vision 88(2), 303–338 (2010)
[11] Guo, C., Pleiss, G., Sun, Y., Weinberger, K.Q.: On calibration of modern neural networks. In: Proceedings of the 34th International Conference on Machine Learning. Volume 70. pp. 1321–1330. JMLR. org (2017)
[12] He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition. pp. 770–778 (2016)
[13] Hendrycks, D., Gimpel, K.: A baseline for detecting misclassified and out-of-distribution examples in neural networks. Proceedings of International Conference on Learning Representations (2017)
[14] Hendrycks, D., Mazeika, M., Kadavath, S., Song, D.: Using self-supervised learning can improve model robustness and uncertainty. In: Advances in Neural Information Processing Systems. pp. 15637–15648 (2019)
[15] Kim, J., Çetin, M., Willsky, A.S.: Nonparametric shape priors for active contour-based image segmentation. Signal Processing 87(12), 3021–3044 (2007)
[16] Krizhevsky, A., Hinton, G., et al.: Learning multiple layers of features from tiny images. Tech. rep., Citeseer (2009)
[17] Lee, K., Lee, H., Lee, K., Shin, J.: Training confidence-calibrated classifiers for detecting out-of-distribution samples. In: ICLR 2018. ICLR 2018 (2018)

[18] Lee, K., Lee, K., Lee, H., Shin, J.: A simple unified framework for detecting out-of-distribution samples and adversarial attacks. In: Advances in Neural Information Processing Systems. pp. 7167–7177 (2018)

[19] Li, Y., Li, Y., Srikant, R.: Enhancing the reliability of out-of-distribution image detection in neural networks. arXiv preprint arXiv:1706.02690 (2017)

[20] Lin, T.Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., Zitnick, C.L.: Microsoft coco: Common objects in context. In: European conference on computer vision. pp. 740–755. Springer (2014)

[21] Netzer, Y., Wang, T., Coates, A., Bissacco, A., Wu, B., Ng, A.Y.: Reading digits in natural images with unsupervised feature learning (2011)

[22] Parzen, E.: On estimation of a probability density function and mode. The annals of mathematical statistics 33(3), 1065–1076 (1962)

[23] Ronneberger, O., Fischer, P., Brox, T.: U-net: Convolutional networks for biomedical image segmentation. In: International Conference on Medical image computing and computer-assisted intervention. pp. 234–241. Springer (2015)

[24] Scott, D.W.: Multivariate density estimation: theory, practice, and visualization. John Wiley & Sons (2015)

[25] Silverman, B.W.: Density estimation for statistics and data analysis, vol. 26. CRC press (1986)

[26] Vyas, A., Jammalamadaka, N., Zhu, X., Das, D., Kaul, B., Willke, T.L.: Out-of-distribution detection using an ensemble of self supervised leave-out classifiers. In: Proceedings of the European Conference on Computer Vision (ECCV). pp. 550–564 (2018)

[27] Xu, P., Ehinger, K.A., Zhang, Y., Finkelstein, A., Kulkarni, S.R., Xiao, J.: Turkergaze: Crowdsourcing saliency with webcam based eye tracking. arXiv preprint arXiv:1504.06755 (2015)

[28] Yu, F., Chen, H., Wang, X., Xian, W., Chen, Y., Liu, F., Madhavan, V., Darrell, T.: Bdd100k: A diverse driving dataset for heterogeneous multitask learning. In: The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2020)

[29] Yu, F., Seff, A., Zhang, Y., Song, S., Funkhouser, T., Xiao, J.: Lsun: Construction of a large-scale image dataset using deep learning with humans in the loop. arXiv preprint arXiv:1506.03365 (2015)

[30] Zhou, B., Lapedriza, A., Khosla, A., Oliva, A., Torralba, A.: Places: A 10 million image database for scene recognition. IEEE transactions on pattern analysis and machine intelligence 40(6), 1452–1464 (2017)
A Additional experiments on segmentation networks

In this section, we present additional experimental results for OOD detection on segmentation networks.

A.1 U-Net architecture trained on Pascal VOC

In the main paper, we performed experiments on a DeeplabV3 \cite{3} architecture trained on Pascal VOC dataset \cite{10} and presented OOD detection results of three different OOD detection methods on 4 OOD datasets. We repeat the same experiments with a different neural network architecture, U-Net \cite{23}, to demonstrate the effect of architecture choice to the OOD detection performance. We present the quantitative results obtained in this experiment in Table 5. Note that, we do not include the SSL method \cite{14} in these comparisons since it operates on an auxiliary network detached to the main network and the results will remain same as in Table 4 in the main paper.

| OOD       | FPR at 95% TPR ↓ | Detection Error ↓ | AUROC ↑ | AUPR ↑ |
|-----------|------------------|-------------------|---------|--------|
|           | Mahalanobis / Ours |                   |         |        |
| KITTI     | 95.60 / 99.95    | 50.30 / 52.47     | 29.74 / 14.87 | 5.6 / 4.8 |
|           | 59.09 / 58.71    | 32.04 / 31.85     | 65.59 / 72.14 | 10.84 / 13.65 |
| BDD       | 95.37 / 99.14    | 50.18 / 52.50     | 41.19 / 24.21 | 42.38 / 41.35 |
|           | 70.33 / 56.40    | 37.66 / 30.70     | 56.89 / 74.57 | 47.75 / 63.98 |
| COCO      | 95.04 / 99.95    | 50.05 / 52.47     | 50.55 / 43.02 | 73.51 / 73.73 |
|           | 81.01 / 91.97    | 43.00 / 48.48     | 64.12 / 70.80 | 74.16 / 85.36 |
| Places    | 94.23 / 99.95    | 49.61 / 52.47     | 52.35 / 43.31 | 85.12 / 84.59 |
|           | 82.85 / 93.43    | 43.92 / 49.21     | 62.71 / 70.87 | 84.17 / 92.39 |

Table 5: Quantitative results on distinguishing test set of Pascal VOC in-distribution data set from several OOD data sets on a U-Net network trained on Pascal VOC. ↑indicates larger value is better and ↓indicates lower value is better. All values are percentages. Note that we present 2 different results for both Mahalanobis and Ours for each OOD dataset. These results correspond to the ones obtained by regression using adversarial examples and the remaining OOD datasets, respectively as described in the main paper.

The quantitative results demonstrate that the proposed approach achieves better results than Mahalanobis in most of the cases. When KITTI and BDD are OOD datasets, our method outperforms Mahalanobis in all evaluation methods. When COCO and Places datasets are OOD, both methods perform quite similar. In these datasets, while Mahalanobis produces better results in terms of FPR at 95% TPR and Detection Error, our method performs better in terms of AUROC and AUPR. Table 5 also demonstrates that using the available OOD datasets when training the logistic regression (see Sec. 3.2. in the main paper) leads to improved results compared to using the adversarial images in all OOD datasets.

In Figure 1, we present ROC curves for both Mahalanobis and the proposed method in order to better interpret the results in Table 5. The curves are plotted using the results of logistic regression with the remaining OOD datasets. In KITTI and BDD datasets, we can observe that ROC curve of our method is above Mahalanobis at almost all thresholds. This leads to better AUROC scores for the proposed method in these datasets. The curves reach to a similar level at the higher thresholds which explains having closer results (especially for KITTI) in terms of FPR at 95% TPR. In COCO and Places datasets, ROC curve of the proposed methods are higher than Mahalanobis at the thresholds lower than ~ 55%. Although, Mahalanobis is higher in the rest of the plots, the margins between the two methods are smaller. As a result, the proposed method achieves better results in terms of AUROC while Mahalanobis reaches to 95% TPR before the proposed method.

A.2 Experiments on Cityscapes dataset

In addition to the experiments on segmentation networks (with both DeeplabV3 and U-Net) trained on Pascal VOC dataset, we present experimental results using the same architectures trained on Cityscapes dataset \cite{4}. In these experiments, we use the same OOD datasets that we used in the previous experiments on segmentation networks.

The quantitative results obtained with DeeplabV3 and U-Net architectures are shown in Tables 6 and 7 respectively. The results show that both Mahalanobis and the proposed method achieve the best possible OOD detection results in almost all cases. This may be caused because Cityscapes dataset is significantly different than the OOD datasets. However, the SSL method \cite{14} that uses an auxiliary network for OOD detection achieves very low accuracy compared to the other methods. We hypothesize that the rotation network does not capture the content information from images to solve the rotation task which leads to poor OOD detection performance.
Figure 1: ROC curves for each OOD dataset used in the experiment on a U-Net architecture trained on Pascal VOC.

Table 6: Quantitative results on distinguishing test set of Cityscapes in-distribution data set from several OOD data sets on a DeeplabV3 network trained on Cityscapes.

B Experiments with $L_2$ distance metric in KDE

As we described in Eq. (2) in the main paper, KDE includes a distance metric to perform density estimation. We use $L_1$ distance in all experiments presented in both main paper and previous sections in this supplementary material. In this section, we present additional experimental results by using $L_2$ distance metric instead of $L_1$ in order to show the effect of distance metric choice to the OOD detection results.

We perform this experiment on both CIFAR-10 and CIFAR-100 datasets. The quantitative OOD detection results of the proposed approach using $L_1$ and $L_2$ distance metrics are shown in Table 8. Note that the table contains only FPR at 95% TPR and AUROC results for each dataset for the sake of brevity. The results demonstrate that the difference between $L_1$ and $L_2$ is not significant in most of the results. We observe that $L_1$ performs better in most cases in CIFAR-10 whereas $L_2$ is better in CIFAR-100. However, there is no significant different in any of these cases.
| OOD       | FPR at 95% TPR ↓ | Detection Error ↓ | AUROC ↑  | AUPR ↑  |
|-----------|------------------|-------------------|----------|---------|
|           |                  | Mahalanobis [18] / Ours |          |         |
| KITTI     | 0.0 / 0.0        | 2.50 / 2.50       | 100.0 / 100.0 | 100.0 / 100.0 |
| BDD       | 0.0 / 0.0        | 2.50 / 2.50       | 100.0 / 100.0 | 100.0 / 100.0 |
| COCO      | 0.0 / 0.0        | 2.50 / 2.50       | 100.0 / 100.0 | 100.0 / 100.0 |
| Places    | 0.0 / 0.0        | 2.50 / 2.50       | 100.0 / 100.0 | 100.0 / 100.0 |

Table 7: Quantitative results on distinguishing test set of Cityscapes in-distribution data set from several OOD data sets on a U-Net network trained on Cityscapes.

| OOD       | CIFAR-10         | CIFAR-100        |
|-----------|------------------|------------------|
|           | FPR at 95% TPR   | AUROC            | FPR at 95% TPR   | AUROC            |
|           | $L_1 / L_2$      |                  | $L_1 / L_2$      |                  |
| SVHN      | 2.44 / 2.95      | 99.36 / 99.27    | 24.09 / 26.20    | 94.66 / 94.15    |
|           | 12.63 / 12.96    | 96.07 / 96.06    | 25.76 / 26.23    | 90.41 / 90.64    |
| TIN-rs    | 5.11 / 6.52      | 98.99 / 98.76    | 34.08 / 27.00    | 93.89 / 94.31    |
|           | 4.61 / 5.30      | 98.98 / 98.87    | 28.83 / 31.85    | 92.37 / 92.47    |
| TIN-cr    | 25.74 / 23.77    | 91.69 / 92.43    | 93.99 / 96.11    | 46.87 / 42.84    |
|           | 17.56 / 18.59    | 94.63 / 94.46    | 56.89 / 56.43    | 77.31 / 77.97    |
| LSUN-rs   | 2.54 / 3.94      | 99.44 / 99.16    | 28.47 / 24.61    | 94.55 / 95.18    |
|           | 2.86 / 3.38      | 99.34 / 99.26    | 20.95 / 19.15    | 93.57 / 93.82    |
| LSUN-cr   | 13.48 / 11.34    | 96.99 / 97.34    | 84.90 / 89.41    | 66.50 / 61.02    |
|           | 7.57 / 7.48      | 98.03 / 98.09    | 31.69 / 31.83    | 91.13 / 91.48    |
| iSUN      | 3.83 / 7.71      | 99.26 / 98.95    | 33.49 / 30.20    | 93.90 / 94.63    |
|           | 4.19 / 4.54      | 99.13 / 99.05    | 25.86 / 24.56    | 92.76 / 92.95    |

Table 8: Comparisons of the OOD detection results obtained using $L_1$ and $L_2$ distance metrics when estimating KDE in CIFAR-10 and CIFAR-100 datasets.

### C Results with different $N$ values

As we show in Eq. (2) of the main paper, we use $N$ number of samples from the training set when performing KDE. In the experiments presented in the main paper, we arbitrarily choose $N = 1000$. In this experiment, we demonstrate the effect of different $N$ values to the OOD detection performance. To this end, we perform experiments with $N = 1000$, 2000, 5000 on CIFAR-10 and CIFAR-100 datasets.

We present the quantitative results obtained in this experiment in Table 9. The results demonstrate that increasing $N$ slightly improves the OOD detection results in most cases. However, increasing $N$ brings additional computation cost to the proposed method since the computational complexity of evaluating the pdf estimated by KDE at a single point is $O(N)$. Therefore, one may need to consider the trade-off between accuracy and computation time when determining $N$. Although, we do not observe any significant difference between different $N$ values in our experiments, larger $N$ values may lead to significant improvements on larger datasets.
| OOD     | CIFAR-10                      | CIFAR-100                     |
|---------|-------------------------------|-------------------------------|
|         | FPR at 95% TPR | AUROC | N = 1000/2000/5000 | FPR at 95% TPR | AUROC | N = 1000/2000/5000 |
| SVHN    | 2.44 / 2.57 / 2.86 | 99.36 / 99.36 / 99.36 | 24.09 / 24.86 / 23.02 | 94.66 / 94.54 / 94.69 |
|         | 12.63 / 11.99 / 10.12 | 96.07 / 96.15 / 96.47 | 25.76 / 25.93 / 24.87 | 90.14 / 90.56 / 90.70 |
| TIN-rs  | 5.11 / 5.74 / 5.74 | 98.99 / 98.89 / 98.88 | 34.08 / 32.11 / 30.58 | 93.89 / 94.32 / 94.50 |
|         | 4.61 / 4.92 / 5.01 | 98.98 / 98.96 / 98.95 | 28.83 / 28.40 / 27.96 | 92.37 / 92.21 / 91.82 |
| TIN-cr  | 25.74 / 23.82 / 22.88 | 91.69 / 92.17 / 92.53 | 93.99 / 95.07 / 87.98 | 46.87 / 44.85 / 53.03 |
|         | 17.56 / 17.17 / 16.09 | 94.63 / 94.61 / 94.82 | 56.89 / 57.17 / 58.62 | 77.31 / 77.34 / 76.75 |
| LSUN-rs | 2.54 / 3.41 / 3.36 | 99.44 / 99.28 / 99.26 | 28.47 / 24.82 / 23.96 | 94.55 / 95.31 / 95.20 |
|         | 2.86 / 2.91 / 2.67 | 99.34 / 99.33 / 99.35 | 20.95 / 19.68 / 19.31 | 93.57 / 93.80 / 93.62 |
| LSUN-cr | 13.48 / 12.28 / 11.59 | 96.99 / 97.20 / 97.34 | 84.90 / 86.24 / 79.96 | 66.50 / 64.38 / 70.65 |
|         | 7.57 / 7.78 / 7.31 | 98.03 / 98.01 / 98.14 | 31.69 / 32.57 / 33.77 | 91.13 / 91.16 / 91.12 |
| iSUN    | 3.83 / 4.75 / 4.71 | 99.26 / 99.10 / 99.09 | 33.49 / 29.99 / 30.08 | 93.90 / 94.75 / 94.58 |
|         | 4.19 / 4.14 / 3.98 | 99.13 / 99.13 / 99.15 | 25.86 / 25.45 / 24.62 | 92.76 / 92.87 / 92.57 |

Table 9: OOD detection results obtained by using different number samples, $N = 1000, 2000, 5000$, when performing KDE.