

Out-of-Distribution Detection for Automotive Perception

Julia Nitsch^{1,2}, Masha Itkina³, Ransalu Senanayake³, Juan Nieto², Max Schmidt¹, Roland Siegwart², Mykel J. Kochenderfer³, and Cesar Cadena²

Abstract—Neural networks (NNs) are widely used for object classification in autonomous driving. However, NNs can fail on input data not well represented by the training dataset, known as out-of-distribution (OOD) data. A mechanism to detect OOD samples is important for safety-critical applications, such as automotive perception, to trigger a safe fallback mode. NNs often rely on softmax normalization for confidence estimation, which can lead to high confidences being assigned to OOD samples, thus hindering the detection of failures. This paper presents a method for determining whether inputs are OOD, which does not require OOD data during training and does not increase the computational cost of inference. The latter property is especially important in automotive applications with limited computational resources and real-time constraints. Our proposed approach outperforms state-of-the-art methods on real-world automotive datasets.

I. INTRODUCTION

Neural network (NN) perception systems currently provide state-of-the-art object classification performance [1]–[4]. Softmax normalization is ubiquitously used by NNs for uncertainty estimation. However, such NNs tend to fail on out-of-distribution (OOD) data by assigning incorrect classifications with high confidence [5]. Although softmax tends to perform well on data that follows the training distribution (D_{in}), it assigns overconfident values to OOD samples (D_{out}) due to the fast-growing exponential function [6]. If novel objects appear during inference, the NN could classify them incorrectly with high confidence [6]–[10]. For example, if a NN is designed to classify road users and is therefore trained on samples of pedestrians, cars, trucks, and cyclists, it may eventually classify a deer with high confidence as a car. The deer is an OOD sample for the NN since it was not included in the training data and, thus, the NN misclassifies it as shown in Fig. 1. Hence, these confidences output by the NN pose multiple risks such as decreasing the overall perception accuracy and hiding failures, which reduces system reliability and forces autonomous vehicles to take more conservative actions. To avoid the restriction to conservative actions in general, it is important to detect these perception errors and only then take appropriate measures such as switching to a safe fallback mode in order to ensure safe execution [5].

The literature discusses various approaches for identifying D_{out} . One category of approaches uses NN archi-



Fig. 1: A NN-based classifier with a softmax output layer trained on road users can reliably classify cars that were not present in D_{in} . However, if an OOD object, such as a deer, is processed during inference, the NN may incorrectly assign high confidence to it. Our approach can detect these OOD objects and classify them as such while continuing to reliably classify D_{in} objects.

tures that have implicit OOD detection [11]–[13], but these methods often increase computational costs. Another category of approaches is dedicated OOD detection methods, which include training techniques such as auxiliary losses or modifications to the NN architecture [6], [14], [15]. These methods usually require OOD data during development. This paper presents a threshold-based OOD detection approach that combines auxiliary training techniques with post hoc statistics that capture network characteristics after training. This combination improves the area under the precision recall curve (AUPR) metric compared to state-of-the-art methods. Additionally, our approach does not require D_{out} during training and comes without additional computational costs at inference time. The latter attribute, in particular, is important for automotive applications that run on limited resources with real-time constraints. During training, our proposed method uses an auxiliary Generative Adversarial Network (GAN) [16] to produce D_{out} data that encourages the object classifier to assign low confidences to samples on or outside the decision boundary. Post hoc, the parameters of class-conditioned Gaussian distributions over the bottleneck layer of the NN are computed from the training data. A sample is classified as D_{out} during inference based on its distance to the previously computed Gaussian distributions. Our proposed method is validated on an object classification task using real-world automotive datasets, including KITTI [17] and nuScenes [18].

Our contributions are as follows. We present an OOD detection approach that does not require an externally collected D_{out} dataset and comes without additional computational costs during inference. We empirically validate our OOD detection method on real-world data with multiple post

¹Ibeo Automotive Systems GmbH, {julia.nitsch, max.schmidt}@ibeo-as.com

²Autonomous Systems Lab, ETH Zurich, {jnieto, rsiegwart, cesarc}@ethz.ch

³Stanford Intelligent Systems Laboratory, Stanford University, {mitkina, ransalu, mykel}@stanford.edu

hoc distance metrics, demonstrating superior performance to state-of-the-art approaches.

II. RELATED WORK

OOD detection can be categorized into implicit (Section II-A) and explicit (Section II-B) detection techniques. Implicit OOD detection techniques can naturally detect OOD samples as a byproduct of their design, while dedicated OOD detection approaches consider auxiliary losses during training, additional architectural components, or post hoc network statistics.

A. Implicit OOD Detection Techniques

Bayesian Neural Networks (BNNs) can identify samples from D_{out} by design unlike Maximum Likelihood Estimation (MLE)-based approaches [11], [19]. BNNs represent model uncertainty using parameterized distributions over NN weights. NN ensembles can also represent model uncertainty by using a collection of weights [19], [20]. Both of these methods can be used for OOD detection. Although BNNs and NN ensembles are promising research directions, current state-of-the-art automotive perception usually relies on MLE-based deep NNs [1]–[4] due to lower computational costs. Hence, in our paper, we follow this line of research. Monte Carlo (MC) dropout [21] has gained popularity for uncertainty-based OOD detection [12], [13]. MC dropout is a simple, effective method for epistemic uncertainty estimation that does not require an explicit D_{out} dataset to be available during training. In contrast to BNNs, which are trained to compute model uncertainty, MC dropout measures the uncertainty by applying dropout to the NN during inference. For this, MC dropout requires multiple forward passes during inference, which is unsuitable for applications that run on limited resources and have real-time constraints.

Normalizing flows (NFs) have also been used for OOD detection using the learned feature space [22]. However, the memory footprint of NFs is unsuitable for larger inputs and, thus, Wellhausen *et al.* [23] apply NFs only to the bottleneck vector of a NN. We follow the latter approach in modeling distributions over the bottleneck vector, but instead of NFs, we fit class-conditioned Gaussian distributions following Lee *et al.* [24], which add no extra memory footprint to the NN.

B. Dedicated OOD Detection Techniques

Variational Autoencoders (VAEs) [25]–[27] and adversarially trained AEs [28] can specifically be developed for OOD detection. Latent space distances and reconstruction losses of bidirectional GANs [29] are used for D_{out} classification [30], [31]. However, these methods incur additional computational costs during inference.

NN architecture components like decoders [6], additional output neurons [15], or auxiliary loss functions [14] are used for OOD detection. However, these methods require explicit D_{out} datasets during training. Golan *et al.* [32] circumvent the need for an explicit D_{out} dataset by applying geometric transformations to the input data, such as flipping, rotating, or translating images, during training. However, the same

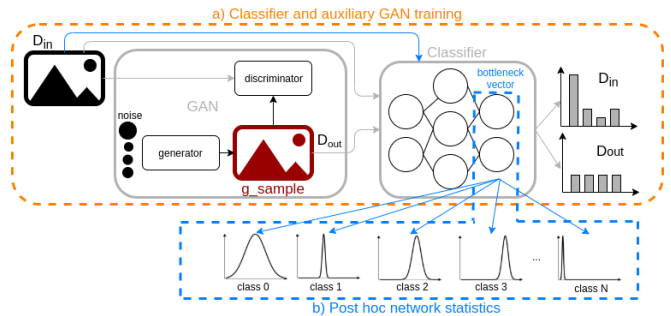


Fig. 2: **a)** depicts the processing of D_{in} and the generation of D_{out} on the decision boundary of the classifier. **b)** depicts the post hoc computation of class-conditioned Gaussian distributions on D_{in} . During inference, a threshold identifies D_{out} based on the distance to these distributions.

transformation must be applied during inference to detect OOD samples, which adds computational cost. Classifiers have been trained on feature space distances [33], [34] to detect OOD samples during inference. We do not train explicitly on feature distances but apply an auxiliary loss to assign low confidences to generated OOD examples. We thus maximize the distance from our generated D_{out} samples to the D_{in} dataset implicitly.

Post hoc methods, such as that proposed by Lee *et al.* [24], compute network statistics on an already trained network to detect OOD samples. Combining auxiliary training methods from Hendrycks *et al.* [14] with post hoc statistics from Lee *et al.* [24] has been proposed by Papadopoulos *et al.* [35], but they require a carefully designed D_{out} dataset. Lee *et al.* [36] avoid the design of D_{out} by using an auxiliary GAN to generate D_{out} during training and an additional loss function that assigns uniform distribution to D_{out} . In our work, we also use a GAN to produce D_{out} samples during training. Following Papadopoulos *et al.* [35], we combine this auxiliary training procedure with post hoc statistics and investigate multiple distance metrics for OOD detection. With this combination, we circumvent the need for D_{out} dataset collection and outperform the state-of-the-art approach from Lee *et al.* [36].

III. METHOD

We propose an uncertainty-based OOD detection approach that combines auxiliary training techniques with post hoc statistics. An overview of the proposed method is shown in Fig. 2. Similar to Lee *et al.* [36], we use an auxiliary GAN to produce D_{out} during training to encourage the object classifier to assign low confidence to samples on and outside the decision boundary. We extend the approach of Lee *et al.* [36] by proposing an additional post hoc component to the OOD detection method, thereby improving performance. We compute the parameters of class-conditioned Gaussian distributions over the weights of the bottleneck layer of the NN based on the training data. Class-conditioned Gaussian distributions are a reasonable choice for modeling distributions on pre-trained features according to the analysis by Lee *et al.* [24]. During inference, a distance computation to the Gaussian distributions facilitates the identification of D_{out}

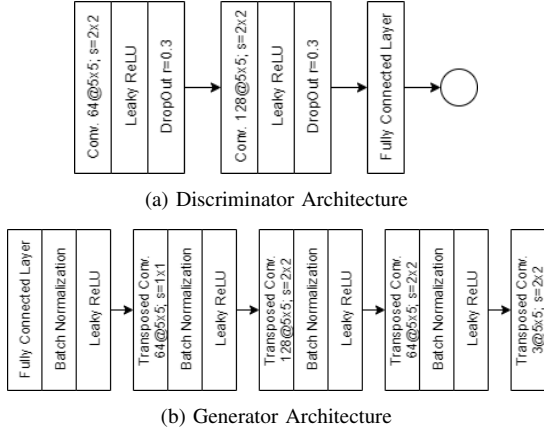


Fig. 3: The discriminator (Fig. 3a) consists of two convolutional layers with 5×5 kernels, strides of 2×2 , and leaky ReLU activations followed by a dropout layer with a dropout rate of 0.3. The first and second layers produce 64 and 128 feature maps, respectively. The convolutions are followed by a fully connected layer with a single output. The first block of the generator (Fig. 3b) consists of a fully connected layer with batch normalization and a leaky ReLU activation. Then, the network contains three transposed convolution blocks with 5×5 kernels, batch normalization, and leaky ReLU activations. The last block consists of only a transposed convolution with 5×5 kernel.

through an empirically determined threshold. We explore different distance metrics in our evaluation. Our proposed approach does not require an explicit OOD dataset during training and does not add computation costs during inference which makes it suitable for real-world applications.

A. Training

A GAN architecture consists of two components: a generator and a discriminator. The generator synthesizes data samples such that the discriminator would incorrectly classify these generated samples (D_{out}) as regular input data (D_{in}). The discriminator is optimized to distinguish between the generated samples and the real input. The discriminator loss in Eq. (1), the generator loss in Eq. (2), and the object classification loss in Eq. (3) are jointly trained (see Algorithm 1) following [36].

The discriminator loss is computed to distinguish samples from D_{in} and D_{out} , and is thus defined as the sum of the binary cross-entropy (BCE) losses from D_{in} and from D_{out} :

$$\mathcal{L}_d = \text{BCE}(\text{dis}(D_{in}), 1) + \text{BCE}(\text{dis}(\text{gen}(\mathbf{n})), 0) \quad (1)$$

where \mathbf{n} is the standard Gaussian noise vector, gen is the generator output, and dis is the discriminator output. In our construction, the generator loss in Eq. (2) features an additive term that serves to encourage the network to output samples on the decision boundary of the object classifier. Hence, the generator is not only trained to fool the discriminator, but also to encourage the object classifier to assign low confidences to samples on or outside the decision boundary. This is achieved through the additive Kullback-Leibler (KL) divergence term between the classifier output and the uniform distribution. The generator loss is:

$$\mathcal{L}_g = \text{BCE}(\text{dis}(\text{gen}(\mathbf{n})), 1) + \text{KL} \left[\text{cls}(\text{gen}(\mathbf{n})) \parallel \frac{1}{n_c} \right] \quad (2)$$

where n_c is the number of classes, $\frac{1}{n_c}$ is the uniform distribution over classes, and cls is the output of the classification network with softmax normalization. Similarly, the classifier

weights are updated to classify D_{in} correctly using the cross entropy loss (CE) and to assign a uniform distribution to D_{out} with the same KL term as in \mathcal{L}_g (see Eq. (2)). This KL term trains the generator to create samples on the decision boundary of the classifier and the same term encourages the classifier to assign uniform distribution to these samples. We denote the ground truth label as ℓ . The classifier loss is defined as:

$$\mathcal{L}_{cls} = \text{CE}(\text{cls}(D_{in}), \ell) + \text{KL} \left[\text{cls}(\text{gen}(\mathbf{n})) \parallel \frac{1}{n_c} \right]. \quad (3)$$

The sequential learning procedure is demonstrated in detail in Algorithm 1.

Algorithm 1 Joint Training Loss

```

for epoch in epochs do
   $batches\_din \leftarrow \text{split } D_{in} \text{ into batches of batch\_size}$ 
  for (data,  $\ell$ ) in  $batches\_din$  do
     $\mathbf{n} = \text{sample\_n}()$ 
    # 1) update discriminator
     $\mathcal{L}_d = \text{BCE}(\text{dis}(data), 1) + \text{BCE}(\text{dis}(\text{gen}(\mathbf{n})), 0)$ 
    update dis w.r.t.  $\mathcal{L}_d$ .
    # 2) update generator
     $\mathcal{L}_g = \text{BCE}(\text{dis}(\text{gen}(\mathbf{n})), 1) + \text{KL} \left( \text{cls}(\text{gen}(\mathbf{n})), \frac{1}{n_c} \right)$ 
    update gen w.r.t.  $\mathcal{L}_{gen}$ .
    # 3) update classifier
     $\mathcal{L}_{cls} = \text{CE}(\text{cls}(data), \ell) + \text{KL} \left( \text{cls}(\text{gen}(\mathbf{n})), \frac{1}{n_c} \right)$ 
    update cls w.r.t.  $\mathcal{L}_{cls}$ .
  end for
end for

```

In contrast to [36], we propose a different architecture for the discriminator (see Fig. 3a) and generator (see Fig. 3b) due to stability issues encountered during training on automotive datasets. The main differences between our discriminator architecture and that of Lee *et al.* [36] are as follows. We use a smaller number of convolutional layers with larger 5×5 kernels. We also replace batch normalization with dropout regularization since we empirically found better performance with this regularization method. We hypothesize that the larger kernels might be beneficial due to larger input sizes compared to the datasets used in [36]. Within the generator, we insert a fully connected layer and again use kernels of size 5×5 . We found empirically that the addition of the fully connected layer accelerated the generator training. Similar to Lee *et al.* [36], we use the VGG-13 architecture [37] for the classification network. We use a 100-dimensional standard Gaussian noise vector \mathbf{n} as input to the generator network to produce D_{out} . The discriminator (dis) takes as input data of shape $height \times width \times 3$ with a value range of $[0, 1]$. The discriminator outputs a confidence value in $[0, 1]$, where 1 is the highest confidence that the input belongs to D_{in} . The generator (gen) processes \mathbf{n} to synthesize data samples of the same shape and value range as D_{in} . All weights are initialized with the Xavier initialization [38], biases are initialized with zero, and the network is trained with the Adam optimizer [39]. The initial learning rate of 2×10^{-4} is exponentially decreased every 30000 iterations with a decay rate of 0.5. The network is trained for 100 epochs with a batch size of 128.

B. Post Hoc Network Statistics

Having trained the network, we now want to compute the parameters of class-conditioned Gaussian distributions over the logits, also referred to as the bottleneck vector, of the classification network. The class-conditioned Gaussian is a reasonable modeling choice for the parameter distribution according to Lee *et al.* [24]. The distance to the Gaussian distribution deemed most likely by the softmax distribution is used to identify OOD samples. We first consider the cosine similarity measure, which is a known distance metric for comparing high dimensional feature vectors and, thus, an effective means for OOD detection:

$$\text{CosSim}(\mathbf{x}, \boldsymbol{\mu}_c) = \frac{\mathbf{x} \cdot \boldsymbol{\mu}_c}{\|\mathbf{x}\| \|\boldsymbol{\mu}_c\|} \quad (4)$$

where \mathbf{x} is the logit vector from the classifier for a test input, $\boldsymbol{\mu}_c$ is the mean vector, and c is the most likely class according to the softmax distribution. Since the cosine similarity does not take into account the dispersion of the features, we also consider computing the Mahalanobis distance as suggested by Lee *et al.* [24]:

$$d_{M_c} = \sqrt{(\mathbf{x} - \boldsymbol{\mu}_c)^T \boldsymbol{\Sigma}_c^{-1} (\mathbf{x} - \boldsymbol{\mu}_c)} \quad (5)$$

where $\boldsymbol{\Sigma}_c$ is the covariance matrix. Since d_{M_c} is not bounded, which is required for the common interpretation of confidence measures, we compute the confidence based on the chi-square (χ^2) distribution. $d_{M_c}^2$ follows the χ^2 distribution where the degrees of freedom correspond to the feature dimensions. This probability is then used for OOD detection [40], [41]. Unlike our proposed method, Lee *et al.* [24] require an explicit, pre-determined D_{out} during training in order to perform OOD detection during inference.

IV. EXPERIMENTS

We consider two classification training regimes in our experiments: (1) the classifier is trained using the standard cross entropy loss (CE loss) and (2) the classifier is trained using the sequential losses in Eq. (1) - Eq. (3) (joint loss). For both sets of experiments, the predicted class label is the most likely class according to the softmax layer. For the predicted class, the following post hoc confidence measures are computed to detect D_{out} : largest softmax probability mass amongst all classes (softmax), mutual information (MI) from MC dropout [21], cumulative density function (CDF) of the χ^2 distribution (ours), and cosine similarity (ours). The joint loss training with softmax probabilities inspired by [36], serves as a baseline to our proposed combination with post hoc statistics (χ^2 and CosSim). We compare our proposed method against MC dropout using $T = 100$ inference steps as it is a popular method for OOD detection [12], [13]. We do not baseline against [24] since this approach requires a D_{out} dataset during the development phase.

A. Datasets

We evaluate the proposed OOD detection method on two real-world automotive datasets: KITTI [17] and nuScenes [18]. We extract *Car*, *Truck*, *Cyclist*, and *Pedestrian* object classes from the KITTI dataset represented as $192 \times 256 \times 3$ patches following the train/test split as suggested by Nitsch *et al.* [42]. Objects from the nuScenes dataset include ten different classes (*Barrier*, *Bicycle*, *Bus*,

Car, *Construction Vehicle*, *Bike*, *Officer*, *Cone*, *Trailer*, *Truck*) with a patch size of $128 \times 128 \times 3$. We follow the train/validation split proposed by Caesar *et al.* [18]. In our experiments, the nuScenes validation set serves as the test set, because the test labels have not been released to the public. The KITTI and nuScenes datasets both serve as D_{in} , while the ImageNet [43] test set is chosen as D_{out} . The D_{in} datasets are used for training whereas the D_{out} dataset is purely used for OOD detection evaluation. The whole ImageNet test set is considered as D_{out} although it might contain object classes from D_{in} (e.g. cars). However, the amount of overlap between the classes in D_{in} and D_{out} is comparably small and it is the same for all methods during evaluation.

B. Evaluation Metrics

We report the *Detection Accuracy* and the *Area Under Precision Recall (AUPR) curve* as done in related literature [24], [36]. Following the notation from Lee *et al.* [36], the *Minimum Error Probability* e is stated as:

$$e = 1 - \min_{\tau} \{ P(q(\mathbf{x}_{in}) \leq \tau) P(\mathbf{x}_{in}) + P(q(\mathbf{x}_{out}) > \tau) P(\mathbf{x}_{out}) \} \quad (6)$$

where \mathbf{x}_{in} and \mathbf{x}_{out} belong to D_{in} and D_{out} , respectively, P is the sample probability of \mathbf{x} belonging to D_{in} or D_{out} , q is the confidence score of the evaluated metric (e.g. softmax, cosine similarity), and τ describes the best possible threshold between the confidence scores for D_{in} and D_{out} . The *Detection Accuracy* is defined as:

$$\text{Detection Accuracy} = 1 - e. \quad (7)$$

The *Detection Accuracy* reflects the classification result only for the best possible threshold τ given knowledge of the confidence scores of the evaluated metric for D_{in} and D_{out} . Therefore, it should be considered in combination with a threshold independent measure, such as *Area Under Precision Recall (AUPR) curve*, as done in related literature [24], [36]. The AUPR is a suitable measure of the classification performance on class-imbalanced datasets, which is the case in our experiments. There are two subcategories in the AUPR metric: *AUPR-in* (D_{in} positive class) and *AUPR-out* (D_{out} positive class). The *AUPR-in* metric is central to evaluating the performance of OOD detection as it characterizes how well D_{in} is correctly identified during the classification task. For completeness, we report both *AUPR-in* and *AUPR-out*, as is done in [24], [36].

C. Quantitative Results

Table I and Table II show the results on the automotive datasets, KITTI (D_{in}) and nuScenes (D_{in}), with the ImageNet test set serving as D_{out} . The best result is highlighted in **bold** and the second best in *italics*. The results in Table I and Table II confirm that the joint loss scheme is superior to the regular NN training for OOD detection. Furthermore, the cosine similarity is amongst the best results in all experiments with a clear advantage on the *AUPR-in* metric. When considering the post hoc approaches to OOD detection on their own (CE term in Eq. (3)), we found the cosine similarity to still be the superior choice for standard CE loss trained classifiers. χ^2 -based detection

TABLE I: D_{in} KITTI - D_{out} ImageNet

	Acc.% \uparrow	Output	Detection acc. % \uparrow	AUPR \uparrow in	AUPR \uparrow out
CE loss	94.09	softmax	51.98	62.14	86.42
		MC dropout [44]	84.61	54.67	82.51
		χ^2 (ours)	86.49	76.12	65.20
		CosSim (ours)	86.15	81.34	80.08
joint loss	93.30	softmax [36]	84.61	78.95	94.67
		MI	84.61	60.47	90.56
		χ^2 (ours)	88.16	76.40	60.71
		CosSim (ours)	89.61	89.86	90.25

TABLE II: D_{in} nuScenes - D_{out} ImageNet

	Acc.% \uparrow	Output	Detection acc. % \uparrow	AUPR \uparrow in	AUPR \uparrow out
CE loss	88.56	softmax	83.85	64.52	81.67
		MC dropout [44]	83.76	55.11	78.87
		χ^2 (ours)	83.80	65.92	64.40
		CosSim (ours)	84.98	88.82	82.84
joint loss	88.85	softmax [36]	87.40	74.97	90.64
		MI	83.79	56.88	82.12
		χ^2 (ours)	83.83	66.97	63.74
		CosSim (ours)	87.13	91.51	87.90

achieves comparable results but is nevertheless outperformed by the cosine similarity measure. We hypothesize that further improvements to covariance estimation may lead to better OOD detection performance with the χ^2 -based uncertainty.

For the KITTI experiments (Table I), the cosine similarity metric achieves a +5% better *Detection Accuracy* than softmax as well as a significant difference of +10.91% in the *AUPR-in* metric. We hypothesize that its slightly lower performance on *AUPR-out* compared to the baseline might be due to classes in the ImageNet test set overlapping with classes in D_{in} . The ImageNet test set does not provide labels, and therefore, it was not possible to easily filter out overlapping classes. Thus, we posit that our method is better able to discern the true OOD examples out of the imperfect D_{out} dataset. For the NuScenes experiments (Table II), similar *Detection Accuracy* is reported for the softmax and cosine similarity approaches. However, in the *AUPR-in* metric, the cosine similarity metric clearly outperforms softmax with +15% improvement while sacrificing only 3% on the *AUPR-out*. Furthermore, the cosine similarity outperforms the MC dropout baseline on the *Detection Accuracy* and *AUPR-in* metrics in both datasets. Our approach has the advantage of being real-time capable, unlike MC dropout, which requires $T = 100$ forward passes of the NN.

D. Qualitative Results

Qualitative OOD detection results are shown on a network trained with the joint loss using the nuScenes dataset (D_{in}). Fig. 4 shows example road users that are not present in the nuScenes dataset alongside OOD detection results from the softmax [36] and cosine similarity (ours) detectors. The threshold used to classify a sample as D_{in} or D_{out} is the optimal τ evaluated in the *Detection Accuracy* in Table II. The car in Fig. 4a is not present in the nuScenes dataset (D_{in}) but visually belongs to the same distribution as the cars in the dataset, and is correctly classified as D_{in} . The example in Fig. 4b is a *beer bike* which can be seen in



(a) Basel. [36]: D_{in} Ours: D_{in} (b) Basel. [36]: D_{out} Ours: D_{out} (c) Basel. [36]: D_{in} Ours: D_{out}

Fig. 4: The OOD detection results are computed using softmax (baseline [36]) and cosine similarity (ours) uncertainty measures from a network trained with the joint loss on the nuScenes dataset. Our approach classifies all objects **correctly**, whereas the baseline **fails** on the horse-drawn carriage example (Fig. 4c).

select German cities. This road user is not in the distribution of the nuScenes training data and both the softmax and the cosine similarity accurately classify it as D_{out} . Fig. 4c shows a *Fiaker*, which is a special horse-drawn carriage unique to the city of Vienna and not present in the nuScenes dataset. The cosine similarity metric correctly detects it as D_{out} whereas the softmax metric incorrectly classifies it as D_{in} . Although the baseline network was trained with auxiliary training techniques, softmax still assigns high probability to the horse-drawn carriage in Fig. 4c, classifying it as D_{in} and mistaking it for a car with high certainty. This example highlights that the addition of post hoc statistics adds value to the auxiliary training methods in OOD detection.

V. CONCLUSION AND FUTURE WORK

In this paper, we introduce an approach that effectively combines auxiliary training techniques and post hoc statistics to perform OOD detection. We investigate different post hoc metrics during inference to identify OOD samples. Our method with the cosine similarity metric achieves the best *AUPR-in* performance on real-world datasets over the MC dropout [44] and softmax [36] baseline approaches for OOD detection. In particular, the combination of generative networks during training and the post hoc computed class-conditioned Gaussian distributions achieves promising performance. We highlight that our proposed approach does not necessitate the definition and recording of an explicit D_{out} dataset and only requires a single inference step of the NN.

As future work, our approach can be applied to the field of anomaly detection to recognize scenarios that are not yet present or underrepresented in D_{in} . For example, a flat truck tire lying on the highway is a rarely recorded scenario but poses a high safety risk. Automated addition of these rare cases to the training database is important to make automotive perception robust and thereby ensure safe driving maneuvers. Although these scenarios might be manually annotated, they could easily be missed in the thousands of hours of data required for automotive validation processes.

ACKNOWLEDGEMENT

This work was funded in part by the Ford-Stanford Alliance and supported by the National Center of Competence in Research (NCCR) Robotics through the Swiss National Science Foundation.

REFERENCES

- [1] C. R. Qi, W. Liu, C. Wu, H. Su, and L. J. Guibas, "Frustum PointNets for 3D object detection from RGB-D data," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 918–927.
- [2] P. Bhattacharyya and K. Czarnecki, "Deformable PV-RCNN: Improving 3D object detection with learned deformations," *arXiv preprint arXiv:2008.08766*, 2020.
- [3] B. Zhu, Z. Jiang, X. Zhou, Z. Li, and G. Yu, "Class-balanced grouping and sampling for point cloud 3D object detection," *arXiv preprint arXiv:1908.09492*, 2019.
- [4] X. Zhu, Y. Ma, T. Wang, Y. Xu, J. Shi, and D. Lin, "SSN: Shape signature networks for multi-class object detection from point clouds," *European Conference on Computer Vision (ECCV)*, pp. 581–597, 2020.
- [5] N. Sünderhauf, O. Brock, W. Scheirer, R. Hadsell, D. Fox, J. Leitner, B. Upcroft, P. Abbeel, W. Burgard, M. Milford, et al., "The limits and potentials of deep learning for robotics," *International Journal of Robotics Research*, vol. 37, no. 4-5, pp. 405–420, 2018.
- [6] D. Hendrycks and K. Gimpel, "A baseline for detecting misclassified and out-of-distribution examples in neural networks," *International Conference on Learning Representations (ICLR)*, 2017.
- [7] K. Nguyen and B. O'Connor, "Posterior calibration and exploratory analysis for natural language processing models," *Conference on Empirical Methods in Natural Language Processing*, 2015.
- [8] D. Yu, J. Li, and L. Deng, "Calibration of confidence measures in speech recognition," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 19, no. 8, pp. 2461–2473, 2011.
- [9] J. Provost Foster, F. Tom, and K. Ron, "The case against accuracy estimation for comparing induction algorithms," in *International Conference on Machine Learning (ICML)*, 1998, pp. 445–453.
- [10] A. Nguyen, J. Yosinski, and J. Clune, "Deep neural networks are easily fooled: High confidence predictions for unrecognizable images," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 427–436.
- [11] Y. Ovadia, E. Fertig, J. Ren, Z. Nado, D. Sculley, S. Nowozin, J. Dillon, B. Lakshminarayanan, and J. Snoek, "Can you trust your model's uncertainty? Evaluating predictive uncertainty under dataset shift," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2019, pp. 13 991–14 002.
- [12] A. Sedlmeier, T. Gabor, T. Phan, L. Belzner, and C. Linnhoff-Popien, "Uncertainty-based out-of-distribution detection in deep reinforcement learning," *International Symposium on Applied Artificial Intelligence (ISAAI)*, 2019.
- [13] A. Loquercio, M. Segù, and D. Scaramuzza, "A general framework for uncertainty estimation in deep learning," *IEEE Robotics and Automation Letters (RA-L)*, vol. 5, no. 2, pp. 3153–3160, 2020.
- [14] D. Hendrycks, M. Mazeika, and T. Dietterich, "Deep anomaly detection with outlier exposure," *International Conference on Learning Representations (ICLR)*, 2019.
- [15] T. DeVries and G. W. Taylor, "Learning confidence for out-of-distribution detection in neural networks," *arXiv preprint arXiv:1802.04865*, 2018.
- [16] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," ser. *Advances in Neural Information Processing Systems (NeurIPS)*, MIT Press, 2014, pp. 2672–2680.
- [17] A. Geiger, P. Lenz, and R. Urtasun, "Are we ready for autonomous driving? The KITTI vision benchmark suite," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2012.
- [18] H. Caesar, V. Bankiti, A. H. Lang, S. Vora, V. E. Liong, Q. Xu, A. Krishnan, Y. Pan, G. Baldan, and O. Beijbom, "nuScenes: A multimodal dataset for autonomous driving," *arXiv preprint arXiv:1903.11027*, 2019.
- [19] L. V. Jospin, W. Buntine, F. Boussaid, H. Laga, and M. Bennamoun, "Hands-on Bayesian neural networks—a tutorial for deep learning users," *arXiv preprint arXiv:2007.06823*, 2020.
- [20] A. Wehenkel and G. Louppe, "You say normalizing flows I see Bayesian networks," *arXiv preprint arXiv:2006.00866*, 2020.
- [21] Y. Gal and Z. Ghahramani, "Dropout as a Bayesian approximation: Representing model uncertainty in deep learning," in *International Conference on Machine Learning (ICML)*, 2016, pp. 1050–1059.
- [22] N. Marchal, C. Moraldo, H. Blum, R. Siegwart, C. Cadena, and A. Gawel, "Learning densities in feature space for reliable segmentation of indoor scenes," *IEEE Robotics and Automation Letters (RA-L)*, vol. 5, no. 2, pp. 1032–1038, 2020.
- [23] L. Wellhausen, R. Ranftl, and M. Hutter, "Safe robot navigation via multi-modal anomaly detection," *IEEE Robotics and Automation Letters (RA-L)*, vol. 5, no. 2, pp. 1326–1333, 2020.
- [24] K. Lee, K. Lee, H. Lee, and J. Shin, "A simple unified framework for detecting out-of-distribution samples and adversarial attacks," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2018, pp. 7167–7177.
- [25] J. An and S. Cho, "Variational autoencoder based anomaly detection using reconstruction probability," *Special Lecture on IE*, vol. 2, no. 1, pp. 1–18, 2015.
- [26] M. A. Lee, M. Tan, Y. Zhu, and J. Bohg, "Detect, reject, correct: Crossmodal compensation of corrupted sensors," *arXiv preprint arXiv:2012.00201*, 2020.
- [27] M. Sensoy, L. Kaplan, F. Cerutti, and M. Saleki, "Uncertainty-aware deep classifiers using generative models," *AAAI Conference on Artificial Intelligence (AAAI)*, 2020.
- [28] M. Sabokrou, M. Khalooei, M. Fathy, and E. Adeli, "Adversarially learned one-class classifier for novelty detection," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 3379–3388.
- [29] J. Donahue, P. Krähenbühl, and T. Darrell, "Adversarial feature learning," *arXiv preprint arXiv:1605.09782*, 2016.
- [30] H. Zenati, C. S. Foo, B. Lecouat, G. Manek, and V. R. Chandrasekhar, "Efficient gan-based anomaly detection," 2018.
- [31] H. Zenati, M. Romain, C.-S. Foo, B. Lecouat, and V. Chandrasekhar, "Adversarially learned anomaly detection," in *IEEE International Conference on Data Mining (ICDM)*, 2018, pp. 727–736.
- [32] I. Golan and R. El-Yaniv, "Deep anomaly detection using geometric transformations," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2018, pp. 9758–9769.
- [33] J. Snell, K. Swersky, and R. Zemel, "Prototypical networks for few-shot learning," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2017, pp. 4077–4087.
- [34] M. Tan, Y. Yu, H. Wang, D. Wang, S. Potdar, S. Chang, and M. Yu, "Out-of-domain detection for low-resource text classification tasks," in *Conference on Empirical Methods in Natural Language Processing and the International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, 2019, pp. 3566–3572.
- [35] A.-A. Papadopoulos, M. R. Rajati, N. Shaikh, and J. Wang, "Outlier exposure with confidence control for out-of-distribution detection," *arXiv preprint arXiv:1906.03509*, 2019.
- [36] K. Lee, H. Lee, K. Lee, and J. Shin, "Training confidence-calibrated classifiers for detecting out-of-distribution samples," *International Conference on Learning Representations (ICLR)*, 2018.
- [37] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *International Conference on Learning Representations (ICLR)*, 2015.
- [38] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2010, pp. 249–256.
- [39] D. Kingma and J. Ba, "Adam: A method for stochastic optimization," *International Conference on Learning Representations (ICLR)*, Dec. 2014.
- [40] P. J. Rousseeuw and B. C. Van Zomeren, "Unmasking multivariate outliers and leverage points," *Journal of the American Statistical Association*, vol. 85, no. 411, pp. 633–639, 1990.
- [41] P. J. Rousseeuw and K. V. Driessen, "A fast algorithm for the minimum covariance determinant estimator," *Technometrics*, vol. 41, no. 3, pp. 212–223, 1999.
- [42] J. Nitsch, J. Nieto, R. Siegwart, M. Schmidt, and C. Cadena, "Learning common and transferable feature representations for multimodal data," *IEEE Intelligent Vehicles Symposium (IV)*, 2020.
- [43] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2009.
- [44] H. Blum, P.-E. Sarlin, J. Nieto, R. Siegwart, and C. Cadena, "Fishyscapes: A benchmark for safe semantic segmentation in autonomous driving," in *IEEE International Conference on Computer Vision Workshops*, 2019.