On the Usefulness of Deep Ensemble Diversity for Out-of-Distribution Detection

Guoxuan Xia  
Imperial College London  
g.xia21@imperial.ac.uk

Christos-Savvas Bouganis  
Imperial College London  
christos-savvas.bouganis@imperial.ac.uk

Abstract

The ability to detect Out-of-Distribution (OOD) data is important in safety-critical applications of deep learning. The aim is to separate In-Distribution (ID) data drawn from the training distribution from OOD data using a measure of uncertainty extracted from a deep neural network. Deep Ensembles are a well-established method of improving the quality of uncertainty estimates produced by deep neural networks, and have been shown to have superior OOD detection performance compared to single models. An existing intuition in the literature is that the diversity of a Deep Ensemble is an intrinsic indicator of input distributional shift, as the members will disagree more on data that are further away from training data [24, 26]. In this work we: 1. Show that this intuition is not valid for OOD detection for convolutional neural networks (CNNs) at ImageNet-scale. 2. Present an alternative explanation for Deep Ensembles’ superior performance – they are ensembles of binary classifiers that are diverse in their OOD detection errors. 3. Show that even better OOD detection performance can be achieved by averaging a task specific score such as Energy [22] over a Deep Ensemble.

2. Preliminaries

2.1. OOD Detection

We use the problem setting defined in [37] for OOD detection. For a $K$-class classification problem, we wish to predict labels $y \in \mathcal{Y} = \{\omega_k\}_{k=1}^{K}$ given inputs $x \in \mathcal{X} = \mathbb{R}^{D}$. We train a DNN with parameters $\theta$ on finite dataset $\mathcal{D}_{\text{train}} = \{(y^{(n)}, x^{(n)})\}_{n=1}^{N}$ sampled independently from the true joint data distribution $p_{\text{train}}(y, x)$. The network typically models the conditional categorical distribution $P(y|x; \theta)$ using a softmax output layer, and is trained using cross entropy loss. Predictions $\hat{y}$ given test inputs $x^*$ can then be made as $\hat{y} = \arg\max_{\omega} P(\omega|x^*; \theta)$.

During deployment, we expect $x^*$ to be sampled either from the training input distribution $p_{\text{train}}(x)$, or $p_{\text{OOD}}(x)$, where the label space of the latter distribution has no intersection with $\mathcal{Y}$. Predictions on the OOD samples will thus be invalid. In order to detect these samples the objective is then to design a binary classification function,

$$g(x; t) = \begin{cases}  
\text{ID}, & \text{if } U(x) < t \\
\text{OOD}, & \text{if } U(x) \geq t
\end{cases},$$

where $U$ is a predictive uncertainty score (or $-U$ confidence), commonly extracted from the network. The performance can be evaluated using standard metrics for binary classification such as Area Under the ROC curve (AUROC$\uparrow$) and False Positive Rate at 95% True Positive Rate (FPR$@$95$\downarrow$), where arrows ($\uparrow$, $\downarrow$) indicate whether higher or lower is better. The problem is challenging, as.

1. Introduction

Detecting Out-of-Distribution (OOD) data [37], i.e. input data that does not originate from the same distribution a deep neural network (DNN) is trained on, is a task that is attracting an increasing amount of attention in the domain of deep learning for computer vision [4, 6, 9, 10, 12, 13, 20–22, 27, 29, 32, 33, 35, 37, 38]. This is important for applications where passing predictions on OOD data downstream may incur a large cost, e.g. in medicine or autonomous driving.

Deep Ensembles [19] have been shown to reliably be superior for OOD detection compared to single models [17, 24, 31]. An existing intuition for this is that the
the OOD data distribution \(p_{\text{OOD}}(x)\) is not known to the practitioner before deployment.

### 2.2. Deep Ensembles

Deep Ensembles [19] are ensembles of DNNs trained on the same dataset with different random parameter initialisations and data shuffling, \(\Theta = \{\theta^{(m)}\}_{m=1}^M\). The ensemble members can be interpreted as samples from different modes of the Bayesian parameter posterior \(p(\theta | D_{\text{train}})\) [15], which allows their predictions to be more diverse compared to unimodal approximate Bayesian approaches [5]. They have been shown to be a reliable and scalable approach for improving both the predictive performance and quality of uncertainty estimates of DNNs [19, 24, 28, 31].

Following the Bayesian interpretation of Deep Ensembles, we obtain an approximate posterior predictive distribution by averaging over the softmax outputs of the individual ensemble members,

\[
P(y|x, D_{\text{train}}) \approx \frac{1}{M} \sum_{m=1}^{M} P(y|x, \theta^{(m)}) = P(y|x, \Theta),
\]

as well as an uncertainty decomposition [3] in the form of

\[
\mathcal{I}[y, \theta | x, D_{\text{train}}] \approx \left[\frac{1}{M} \sum_{m=1}^{M} P(y|x, \theta^{(m)})\right] \mathcal{H} - \frac{1}{M} \sum_{m=1}^{M} \mathcal{H}[P(y|x, \theta^{(m)})],
\]

where \(\mathcal{H}[\cdot]\) is the entropy of a probability distribution and \(\mathcal{I}[\cdot, \cdot, \cdot, \cdot]\) the (conditional) mutual information (MI) between two random variables. We will refer to the other terms in the above equation as ensemble entropy (Ens.\(\mathcal{H}\)) and average entropy (Av.\(\mathcal{H}\)). MI, when approximated using Eq. (3), measures the diversity of the ensemble, as it is the mean KL-divergence between the predictive distributions of the ensemble members and the ensemble overall,

\[
\mathcal{I}[y, \theta | x, D_{\text{train}}] \approx \frac{1}{M} \sum_{m=1}^{M} \left[\text{KL} \left[ P(y|x, \theta^{(m)}) \right| P(y|x, \Theta) \right].
\]

Av.\(\mathcal{H}\) is a measure of average uncertainty over the ensemble, and we can say that Ens.\(\mathcal{H}\) measures total uncertainty by combining diversity and average uncertainty. Note in

---

2We use a Bayesian framework as it provides convenient metrics, as such we are not particularly concerned with the fidelity of the approximation in Eq. (2). Discussion of this can be found in [15, 36].

3We use the default settings found here https://github.com/pytorch/examples/blob/main/imagenet/main.py. For full details see Appendix B
superior to the average performance of single-model $\mathcal{H}$, MI is unable to outperform the single model baseline. In fact, on iNaturalist, it is $\sim 30\%$ worse. This shows that directly using the diversity of the ensemble to detect OOD data is actually a poor choice in this scenario. We note that inferior MI performance, at ImageNet-scale, has been shown before in \cite{31}. Additionally, the performance is very close between Av.$\mathcal{H}$ and Ens.$\mathcal{H}$, but Av.$\mathcal{H}$ beats Ens.$\mathcal{H}$ in $2/3$ datasets, suggesting MI is a hindrance there. Similar behaviour over most of the other datasets can be observed in Tab. 1.

3.1. Mutual Information Performs Poorly

In order to understand the results in Fig. 1 and Tab. 1, we can consider empirical plots of the conditional distribution of MI given Av.$\mathcal{H}$, as well as the joint distribution. These are shown for ImageNet-200 (ID) and various OOD datasets in Fig. 2. The graded contours represent different values of Ens.$\mathcal{H}$ (lighter means higher), as it is the sum of Av.$\mathcal{H}$ and MI (Eq. (3)). Av.$\mathcal{H}$ is much lower on OOD data – see \cite{29} for a discussion of why. Intuitively, if the average uncertainty is high, then it is difficult for an ensemble to be diverse, as for high diversity the members need to disagree confidently (Eq. (3)). Thus, the MI of high Av.$\mathcal{H}$ OOD data is actually quite low, leading to MI’s poor performance. In other words, MI is failing because Av.$\mathcal{H}$ is performing well.

The notable exception is ImageNet-O, where MI is able to perform the best. We hypothesise that this is due to the adversarial nature of the ImageNet-O data causing the members to be individually more confident (and thus diverse) on the OOD data. A similar effect is observed in \cite{23} for neural machine translation where diversity measures are able to successfully detect pathological overconfidence when models copy OOD inputs rather than translating them.

3.2. Mutual Information Does Not Reliably Contribute to Ensemble Entropy

We see that in Fig. 2 (top) for a given value of Av.$\mathcal{H}$, the behaviour of MI is not that different between the ID and OOD datasets – the diversity does not seem to act as a strong indicator of distributional shift in addition to the average uncertainty. It can also be observed that the actual variation in MI is much lower in comparison to Av.$\mathcal{H}$. Thus, Ens.$\mathcal{H}$ is in fact dominated by Av.$\mathcal{H}$, which explains why their performance is so close. On Textures Ens.$\mathcal{H}$ performs better compared to Av.$\mathcal{H}$, and this suggests that MI is useful in addition to Av.$\mathcal{H}$. Fig. 2 shows that MI given Av.$\mathcal{H}$ is slightly higher on Textures. However, on the other two datasets the opposite is the case – including diversity in addition to average uncertainty harms performance, as the conditional distributions are very similar between ID and OOD.

We note similar results to Fig. 2 are shown in \cite{1}, however the problem framing and conclusions reached in that work are different to ours.

4. An Alternative Explanation

Uncertainty scores derived directly from ensemble diversity don’t seem to reliably contribute to the OOD detection performance of Deep Ensembles at ImageNet-scale. However, the question still remains: why do Deep Ensembles perform better than single models for OOD detection?

4.1. Deep Ensembles as Binary Classifiers

The fact that Av.$\mathcal{H}$ of the ensemble is able to consistently improve OOD detection performance compared to single model $\mathcal{H}$ (Tab. 1) points to a straightforward explanation. If we consider again the binary classification model presented in Eq. (1), we can simply view Deep Ensembles for OOD detection through the same lens we view them for ID prediction. By being diverse in the individual errors they make for OOD detection, their overall OOD detection performance after combination will be better, and this diversity arises from the multimodal nature of the ensemble in parameter space \cite{5}. For a more formal explanation we can consider constructing a binary probabilistic classifier arbitrarily from uncertainty score $U$,

$$P(s = \text{OOD}|x, \theta) = 1 - P(s = \text{ID}|x, \theta) = a U(x; \theta) + b, \quad (5)$$

where $s \in \{\text{ID,OOD}\}$ and $a, b$ are arbitrary parameters such that $U$ is mapped to a valid probability. Note that averaging $U$ over the ensemble is equivalent to averaging $P(s|x; \theta)$. Jensen’s inequality for the binary classification negative log-likelihood (NLL) loss for OOD detection thus states,

$$- \log \left( \frac{1}{M} \sum_{m=1}^{M} P(s|x, \theta^{(m)}) \right) \leq - \frac{1}{M} \sum_{m=1}^{M} \log P(s|x, \theta^{(m)}). \quad (6)$$
Figure 2. Top: empirical conditional histograms of MI|Av.H. The behaviour of MI is quite similar between ID and OOD data, with the exception of Textures being slightly higher. Bottom: joint kernel density estimate plots of MI and Av.H. Contours represent increasing (lighter) values of Ens.H. MI is low for high Av.H OOD data. MI does not contribute significantly to Ens.H.

| Model ID: | ImageNet-200 | OOD mean | Near-ImageNet-200 | Caltech-4S | OpenImages-O | Naturalist |
|----------|--------------|----------|-------------------|------------|--------------|------------|
|          | AUROC† | FPR@95% | AUROC† | FPR@95% | AUROC† | FPR@95% |
| MI       | 86.67 ± 1.4 | 89.82 ± 2.8 | 89.21 ± 2.4 | 91.95 ± 2.4 | 92.94 ± 3.8 | 91.23 ± 4.9 |
| Energy   | 88.22 ± 1.0 | 90.67 ± 2.0 | 90.67 ± 2.0 | 90.67 ± 2.0 | 90.67 ± 2.0 | 90.67 ± 2.0 |
| ResNet-50 | 88.69 ± 1.6 | 92.94 ± 3.5 | 92.94 ± 3.5 | 92.94 ± 3.5 | 92.94 ± 3.5 | 92.94 ± 3.5 |

Table 1. %AUROC↑ and %FPR@95↓ for different uncertainty scores over all OOD datasets. We show mean±std. for single model results. Bold is best performance, underline 2nd or 3rd best. MI performs poorly compared to other uncertainties and even single models. Ens.H and Av.H consistently improve over single model H. Av. Energy is able to improve over single model Energy and is best overall.

We can thus see how averaging \(U(=\mathcal{H})\) over the ensemble leads to better OOD detection as the NLL of the ensemble OOD detector will be lower than the average NLL of the individual ensemble members.

The key intuition is that by ensembling binary classifiers that are diverse such that they make OOD detection errors on different data samples, the ensemble members are able to compensate for each other’s miss-predictions and raise the ensemble performance above their individual average.

4.2. Using a Better OOD Detection Score

Existing work benchmarking Deep Ensembles focuses exclusively on uncertainty scores \(U\) extracted from the softmax outputs of the members. Given the explanation in the previous section, it is natural to ask whether we can improve performance by ensembling a better \(U\). Using Energy \(\log(\sum_k \exp u_k)\), where \(u\) are the logits), and averaging over the ensemble, it can be seen in Tab. 1 that average ensemble Energy is able to improve over single model Energy, as well as produce the best OOD detection results in the whole comparison. We remark that although we have chosen Energy here, we expect any \(U\) with better performance than single model \(H\) to receive a similar uplift upon ensembling.

5. Concluding Remarks

In this work, we show that the existing intuition, that the diversity of a Deep Ensemble is a useful indicator for whether data is OOD, does not hold for ImageNet-scale CNNs. We instead suggest an alternative explanation for Deep Ensembles’ superior OOD detection performance compared to single models: OOD detection is binary classification, and individual Deep Ensemble members produce diverse errors on this binary classification task, so combining them together yields better performance.
References

[1] Taiga Abe, E. Kelly Buchanan, Geoff Pleiss, Richard S. Zemel, and John P. Cunningham. Deep ensembles work, but are they necessary? ArXiv, abs/2202.06985, 2022.

[2] M. Cimpoi, S. Maji, I. Kokkinos, S. Mohamed, and A. Vedaldi. Describing textures in the wild. In Proceedings of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2014.

[3] Stefan Depeweg, Josué Miguel Hernández-Lobato, Finale Doshi-Velez, and Steffen Udluft. Decomposition of uncertainty in bayesian deep learning for efficient and risk-sensitive learning. In ICML, 2018.

[4] Xuefeng Du, Zhaoning Wang, Mu Cai, and Yixuan Li. Vos: Learning what you don’t know by virtual outlier synthesis. ArXiv, abs/2202.01197, 2022.

[5] Stanislav Fort, Huiyi Hu, and Balaji Lakshminarayanan. Deep ensembles: A loss landscape perspective. ArXiv, abs/1912.02757, 2019.

[6] Stanislav Fort, Jie Ren, and Balaji Lakshminarayanan. Exploring the limits of out-of-distribution detection. In NeurIPS, 2021.

[7] Gregory Griffin, Alex Holub, and Pietro Perona. Caltech-256 object category dataset. 2007.

[8] Kaiming He, X. Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 770–778, 2016.

[9] Dan Hendrycks and Thomas G. Dietterich. Benchmarking neural network robustness to common corruptions and perturbations. ArXiv, abs/1903.12261, 2019.

[10] Dan Hendrycks and Kevin Gimpel. A baseline for detecting misclassified and out-of-distribution examples in neural networks. ArXiv, abs/1610.02136, 2017.

[11] Dan Hendrycks, Kevin Zhao, Steven Basart, Jacob Steinhardt, and Dawn Xiaodong Song. Natural adversarial examples. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 15257–15266, 2021.

[12] Yen-Chang Hsu, Yilin Shen, Hongxia Jin, and Zsolt Kira. Decomposition of uncertainty in bayesian deep learning for efficient and risk-sensitive learning. In ICML, 2018.

[13] Rui Huang and Yixuan Li. Mos: Towards scaling out-of-distribution detection for large semantic space. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pages 8706–8715, 2021.

[14] Eyke Hüllermeier and Willem Waegeman. Aleatoric and epistemic uncertainty in machine learning: an introduction to concepts and methods. Mach. Learn., 110:457–506, 2021.

[15] Pavel Izmailov, Sharad Vikram, Matthew D Hoffman, and Andrew Gordon Gordon Wilson. What are bayesian neural network posteriors really like? In International conference on machine learning, pages 4629–4640. PMLR, 2021.

[16] Jakob Nikolas Kather, Cleo-Aron Weiss, Francesco Bianconi, Susanne Maria Melchers, Lothar Rudi Schad, Timo Gaiser, Alexander Marx, and Frank G. Zöllner. Multi-class texture analysis in colorectal cancer histology. Scientific Reports, 6, 2016.

[17] Jihyo Kim, Jiin Koo, and Sangheum Hwang. A unified benchmark for the unknown detection capability of deep neural networks. ArXiv, abs/2112.00337, 2021.

[18] Ivan Krasin, Tom Duering, Neil Alldrin, Vittorio Ferrari, Sami Abu-El-Haija, Alina Kuznetsova, Hassan Rom, Jasper Uijlings, Stefan Popov, Andreas Veit, Serge Belongie, Victor Gomes, Abhinav Gupta, Chen Sun, Gal Chechik, David Cai, Zheyun Feng, Dhyaneesh Narayanan, and Kevin Murphy. Openimages: A public dataset for large-scale multi-label and multi-class image classification. Dataset available from https://github.com/openimages, 2017.

[19] Balaji Lakshminarayanan, Alexander Pritzel, and Charles Blundell. Simple and scalable predictive uncertainty estimation using deep ensembles. In NIPS, 2017.

[20] Kimin Lee, Kibok Lee, Honglak Lee, and Jinwoo Shin. A simple unified framework for detecting out-of-distribution samples and adversarial attacks. In NeurIPS, 2018.

[21] Shiyu Liang, Yixuan Li, and Rayadurgam Srikant. Enhancing the reliability of out-of-distribution image detection in neural networks. arXiv: Learning, 2018.

[22] Weitang Liu, Xiaoyun Wang, John Douglas Owens, and Yixuan Li. Energy-based out-of-distribution detection. ArXiv, abs/2010.03759, 2020.

[23] Andrey Malinin and Mark John Francis Gales. Uncertainty estimation in autoregressive structured prediction. In ICLR, 2021.

[24] Andrey Malinin, Bruno Mlodozeniec, and Mark John Francis Gales. Ensemble distribution distillation. ArXiv, abs/1905.00076, 2020.

[25] Pablo Mesejo, Daniel Pizarro, Armand Abergel, Olivier Y. Rouquette, Sylvain Béorchia, Laurent Poincloux, and Adrien Bartoli. Computer-aided classification of gastrointestinal lesions in regular colonoscopy. IEEE transactions on medical imaging, 2016.

[26] James Munkhte, Andreas Kirsch, Joost R. van Amersfoort, Pablo Mesejo, Daniel Pizarro, Armand Abergel, Olivier Y. Rouquette, Sylvain Béorchia, Laurent Poincloux, and Adrien Bartoli. Computer-aided classification of gastrointestinal lesions in regular colonoscopy. IEEE transactions on medical imaging, 2016.

[27] Eric T. Nalisnick, Akihiro Matsukawa, Yee Whye Teh, Finale Doshi-Velez, and Steffen Udluft. Decomposition of uncertainty in bayesian deep learning for efficient and risk-sensitive learning. In ICML, 2018.

[28] Yaniv Ovadia, Emily Fertig, Jie Ren, Zachary Nado, David Sculley, Sebastian Nowozin, Joshua Dillon, Balaji Lakshminarayanan, and Jasper Snoek. Can you trust your model’s uncertainty? evaluating predictive uncertainty under dataset shift. Advances in neural information processing systems, 32, 2019.

[29] Tim Pearce, Alexandra Brintrup, and Jun Zhu. Understanding softmax confidence and uncertainty. ArXiv, abs/2106.04972, 2021.

[30] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael S. Bernstein, Alexander C. Berg, and Li Fei-Fei. Imagenet large scale visual recognition
challenge. *International Journal of Computer Vision*, 115:211–252, 2015. 2

[31] Max Ryabinin, Andrey Malinin, and Mark John Francis Gales. Scaling ensemble distribution distillation to many classes with proxy targets. In *NeurIPS*, 2021. 1, 2, 3

[32] Yiyou Sun, Chuan Guo, and Yixuan Li. React: Out-of-distribution detection with rectified activations. In *NeurIPS*, 2021. 1

[33] Engkarat Techapanurak, Masanori Suganuma, and Takayuki Okatani. Hyperparameter-free out-of-distribution detection using cosine similarity. In *Proceedings of the Asian Conference on Computer Vision (ACCV)*, November 2020. 1

[34] Grant Van Horn, Oisin Mac Aodha, Yang Song, Yin Cui, Chen Sun, Alex Shepard, Hartwig Adam, Pietro Perona, and Serge Belongie. The inaturalist species classification and detection dataset, 2017. 2

[35] Haoqi Wang, Zhizhong Li, Litong Feng, and Wayne Zhang. Vim: Out-of-distribution with virtual-logit matching. *ArXiv*, abs/2203.10807, 2022. 1, 2, 7

[36] Andrew Gordon Wilson and Pavel Izmailov. Deep ensembles as approximate bayesian inference, Oct 2021. 2

[37] Jingkang Yang, Kaiyang Zhou, Yixuan Li, and Ziwei Liu. Generalized out-of-distribution detection: A survey. *ArXiv*, abs/2110.11334, 2021. 1

[38] Mingtian Zhang, Andi Zhang, and Steven G. McDonagh. On the out-of-distribution generalization of probabilistic image modelling. In *NeurIPS*, 2021. 1
A. Dataset Information

Fig. 3 shows randomly sampled images from each dataset, as well as the number of samples in each. Below we describe the methodology for constructing the Colonoscopy and Noise OOD datasets. We refer to the original papers of the remaining OOD datasets for their corresponding details [11, 13, 16, 17, 35]. We note, for ImageNet-200, there is a slight discrepancy between the number of samples reported in [17] and the number in the authors’ provided datasets. However, we do not believe this affects the validity of our results.

A.1. Noise

10,000 square images are generated to form this dataset. All random samples are generated independently. For each image, each pixel intensity value (across x,y,R,G,B) is sampled from the same distribution. It is a gaussian, \(N(0.5, \sigma^2)\) where \(\sigma\) differs between images. \(\sigma\) is generated by sampling from a unit gaussian and squaring the samples. Intensities are clipped to be in the range [0,1] and mapped to integer values \(\in\{0,...,255\}\). The image widths/heights are sampled from \(\{2,...,256\}\) uniformly. Then, images are scaled to a resolution of \(256 \times 256\) using the lanczos method. The resulting images therefore vary in contrast, intensity and scale (see Fig. 3).

A.2. Colonoscopy

We separate out frames from the colonoscopical videos provided in [25]. The first 10 narrow band imaging (NBI) videos in each class of lesion (hyperplasic, serrated, adenoma) are downloaded. Each video frame is then extracted as an separate image to construct the dataset.

B. Model Training

To construct the Deep Ensemble, 5 independent training runs are performed, with random seeds \(\{1,...,5\}\). ResNet-50 [8] is trained with the default hyperparameters in PyTorch’s ImageNet example. The ensemble members are trained on ImageNet-200 for 90 epochs with batch size equal to 256. Stochastic gradient descent is used with an initial learning rate of 0.1 that steps down by a factor of 10 at epochs 30 and 60. Weight decay is set to \(10^{-4}\), and momentum 0.9. During training images are augmented using RandomHorizontalFlip and RandomResizedCrop, and input to the network at a resolution of \(224 \times 224\).

References:

4. https://github.com/daintlab/unknown-detection-benchmarks
5. https://pillow.readthedocs.io/en/stable/_modules/PIL/Image.html#Image.resize
6. http://www.depeca.uah.es/colonoscopy_dataset/
7. https://github.com/pytorch/examples/tree/main/imagenet
Figure 3. Example images from each dataset, with #samples in each.