Needles in Haystacks: 
On Classifying Tiny Objects in Large Images

Nick Pawlowski\textsuperscript{1}\textsuperscript{*}  Suvrat Bhooshan\textsuperscript{2}  Nicolas Ballas\textsuperscript{2}  Francesco Ciompi\textsuperscript{3}  Ben Glocker\textsuperscript{1}  Michal Drozdzal\textsuperscript{2}
\textsuperscript{1} Biomedical Image Analysis Group, Imperial College London, UK  
\textsuperscript{2} Facebook AI Research  
\textsuperscript{3} Department of Pathology, Radboud University Medical Center, Nijmegen, Netherlands  
n.pawlowski16@imperial.ac.uk

Abstract

In some computer vision domains, such as medical or hyperspectral imaging, we care about the classification of tiny objects in large images. However, most Convolutional Neural Networks (CNNs) for image classification were developed and analyzed using biased datasets that contain large objects, most often, in central image positions. To assess whether classical CNN architectures work well for tiny object classification we build a comprehensive testbed containing two datasets: one derived from MNIST digits and other from histopathology images. This testbed allows us to perform controlled experiments to stress-test CNN architectures using a broad spectrum of signal-to-noise ratios. Our observations suggest that: (1) There exists a limit to signal-to-noise below which CNNs fail to generalize and that this limit is affected by dataset size — more data leading to better performances; however, the amount of training data required for the model to generalize scales rapidly with the inverse of the object-to-image ratio (2) in general, higher capacity models exhibit better generalization; (3) when knowing the approximate object sizes, adapting receptive field is beneficial; and (4) for very small signal-to-noise ratio the choice of global pooling operation affects optimization, whereas for relatively large signal-to-noise values, all tested global pooling operations exhibit similar performance.

1 Introduction

Convolutional Neural Networks (CNNs) are the current state-of-the-art approach for image classification \cite{22, 32, 13, 15}. The goal of image classification is to assign an image-level label to an image. Typically, it is assumed that an object (or concept) that correlates with the label is clearly visible and occupies a significant portion of the image \cite{24, 21, 8}. Yet, in a variety of real-life applications, such as medical image analysis and hyperspectral image processing, only a small portion of the input correlates with the label, resulting in low signal-to-noise ratio. We define this input image signal-to-noise ratio as Object to Image (O2I) ratio. The O2I ratio range for three real-life datasets is depicted in Figure 1. As can be seen, there exists a distribution shift between standard classification benchmarks and domain specific datasets. For instance, in ImageNet dataset \cite{8} the objects fill at least 1\% of the entire image, while in histopathology slices \cite{9} cancer cells can occupy as little as $10^{-6}$\% of the whole image.

Recent works have studied CNNs under different noise scenarios, either by performing random input-to-label experiments \cite{42, 8} or by directly working with noisy annotations \cite{26, 19, 11}. While, it has been shown that large amounts of label-corruption noise hinders the CNNs generalization \cite{42, 8}, it

\textsuperscript{*}Work done as part of an internship at Facebook AI Research.
has been further demonstrated that CNNs can mitigate this label noise by increasing the size of training data [26], tuning the optimizer hyperparameters [18] or weighting input training samples [19, 11]. However, all these works focus on input-to-label corruption and do not consider the case of noiseless input-to-label assignments with small O2I ratios.

To overcome the low signal-to-noise ratio of tiny objects classification tasks, most approaches rely on manual dataset “curation” and collect additional pixel-level annotations such as landmark positions [5], bounding boxes [40, 31] or segmentation maps [9]. This step allows to transform the original needle-in-a-haystack problem into a less noisy but imbalanced classification problem [40, 25]. However, collecting pixel level annotations has a significant cost and might require expert knowledge, and as such, is a bottleneck in the data collection process.

In this paper, we build a testbed to study the performance of CNNs when applied to tiny object classification and investigate the interplay between input signal-to-noise ratio and model generalization. We create two synthetic datasets inspired by the children’s puzzle book Where’s Wally? [12]. The first dataset is derived from MNIST digits and allows us to produce a relatively large number of datapoints with explicit control of the O2I ratio. The second one is extracted from histopathology [9] images where we crop images around lesions and obtain small number of datapoints with an approximate control of the O2I ratio. To the best of our knowledge these datasets are the first ones designed to explicitly stress-test the behaviour of the CNNs in the low input image signal-to-noise ratio.

We develop a classification framework, based on CNNs, and analyze the effects of different factors affecting the model optimization and generalization. Throughout an empirical evaluation, we make the following observations:

- Models can be trained in low O2I regime without using any pixel-level level annotations and generalize if we leverage enough training data. However, the amount of training data required for the model to generalize scales rapidly with the inverse of the O2I ratio. When considering datasets with fix size, we observe an O2I ratio limit in which all tested scenarios fail to exceed random performance.
- We empirically observe that higher capacity models show better generalization. We hypothesize that high capacity models learn the input noise structure and, as result, achieve satisfactory generalization.
- We confirm the importance of model inductive bias — in particular, the model’s receptive field size. Our results suggest that different pooling operations exhibit similar performance, for larger O2I ratios; however, for very small O2I ratios, the type of pooling operation affects the optimization ease, with max-pooling leading to fastest convergence.
We make the code to recreate the datasets and to reproduce our results publicly available at: https://github.com/facebookresearch/Needles-in-Haystacks; we would hope this can serve as a valuable resource facilitating further research into the problem of low signal-to-noise classification scenarios.

2 Related Work

2.1 Tiny Object Classification

Reasoning about tiny objects is of high interest in many computer vision areas, such as medical imaging [9, 2, 32, 34, 35] and remote sensing [41, 30]. However, most of previous papers investigating the small O2I regime assume the availability of pixel-level annotations, which are smartly leveraged at training time to increase input signal-to-noise ratio (e. g. see the CAMELYON17 results review [7]). Differently, in this paper, we investigate the performance of CNNs in a small O2I regime when assuming only the availability of image-level labels.

Other approaches leverage the fact that task-relevant information is often not uniformly distributed across input data, e.g. by using attention mechanisms to process very high-dimensional inputs [27, 4, 11, 20]. However, those approaches are mainly motivated from a computational perspective trying to reduce the computational footprint at inference time.

Some recent research has also studied attention based approaches both in the context of multi-instance learning [16] and histopathology image classification [38]. However, neither of the works report the exact O2I ratio used in the experiments.

2.2 Generalization of CNNs

Understanding the interplay of optimization and generalization of CNNs is an active research area. There are many known factors that affect both the training and validation performances of neural networks. In this section, we briefly highlight the dimensions of optimization and generalization of CNN that are handy in low O2I classification scenarios.

Model capacity. For fixed training accuracy, over-parametrized CNNs tend to generalize better [28]. In addition, when properly regularized and given a fixed size dataset, higher capacity models tend to provide better performance [14, 15]. However, finding proper regularization is not trivial [10].

Dataset size. CNN performance improves logarithmically with dataset size [36]. Moreover, in order to fully exploit the data benefit, the model capacity should scale jointly with the dataset size [26, 36].

Model inductive biases. Inductive biases limit the space of possible solutions that a neural network can learn [10]. Incorporating these biases is an effective way to include data (or domain) specific knowledge in the model. Perhaps the most successful inductive bias is the use of convolutions in CNNs [23]. Different CNN architectures (e. g. altering network connectivity) also lead to improved model performance [14, 15]. Additionally, it has been shown on the ImageNet dataset that CNN accuracy scales logarithmically with the size of the receptive field [6].

3 Experimental testbed

3.1 Is there a Wally in an image?

To study the optimization and generalization properties of CNNs, we build two datasets: one derived from the MNIST [24] dataset and another one produced by cropping large resolution images from the CAMELYON dataset [9]. Each dataset allows to evaluate the behaviour of a CNN-based binary classifier when altering different data-related factors of variation such as dataset size, object size, image resolution and class balance. In this subsection, we describe the data generation process.

Digits: needle MNIST (nMNIST). Influenced by the cluttered MNIST dataset [4], we introduce a scaled up, large resolution cluttered MNIST dataset, suitable for binary image classification. In this dataset, images are obtained by randomly placing a varying number of MNIST digits on a large resolution image canvas. We keep the original 28 x 28 pixels digit resolution and control the O2I
3.2 Pipeline for tiny object classification

Our classification pipeline follows BagNets [6] backbone, which allows us to explicitly control for the network receptive field size. Figure 3 shows a schematic of our approach. As can be seen, the pipeline is built of three components: (1) topological embedding extractor in which we can control for embedding receptive field, (2) global pooling operation that converts the topological embedding into a global embedding, and (3) a binary classifier that receives the global embedding and outputs binary classification probabilities.

**Topological embedding extractor.** The extractor takes as input an image $I$ of size $[w_{img} \times h_{img} \times c_{img}]$ and outputs a topological embedding $E^t$ of shape $[w_{enc} \times h_{enc} \times c_{enc}]$, where $w$, $h$, and $c$ represent width, height and number of channels. Due to the relatively large image sizes, we train the

---

"Alternatively, we could fix canvas image resolution and downscale MNIST digits; however, downscaling might reduce the object quality."  
"We obtain those numbers by using the original MNIST data, we use every digit 3 only once to generate positive images and we balance the dataset with negative images. See supplementary material for class imbalanced data scenarios."
pipeline with small batch sizes and, thus, we replace BagNet-used BatchNorm operation \cite{17} with Instance Normalization \cite{39}.

**Global pooling operation.** Global pooling operation takes as an input topological embedding $E'$ of shape $[w_{enc} \times h_{enc} \times c_{enc}]$ and outputs global image embedding $E'$ of shape $[1 \times 1 \times c_{enc}]$. In the paper, we experiment with four different pooling operations, namely: max, logsumexp, average, and soft attention. In our experiments, we follow the soft attention formulation of \cite{16}. The details about global pooling operations can be found in the supplementary material.

## 4 Experimental results

In this section, we experimentally test how CNNs’ optimization and generalization scale with low and very low O2I ratios. First, we provide details about our experimental setup and then we design experiments to test the following hypotheses: (1) **Image-level annotations**: It is possible to train tiny object classification systems that generalize well without having access to pixel-level annotations; (2) **O2I limit vs. dataset size**: There exist an O2I ratio limit below which the CNNs will experience generalization difficulties and this O2I limit depends on the dataset size; (3) **O2I limit vs. model capacity**: Higher capacity models show better generalization performance; (4) **Inductive bias**: Adjusting receptive field size to match (or exceed) the expected object size leads to better model generalization; (5) **Global pooling operations**: Given recently reported results \cite{16,20}, soft attention based global pooling operation should achieve best results. (6) **Optimization**: We expect to observe generalization difficulties of the models for very low O2I ratios; however, we do not expect to see training problems.

### 4.1 Experimental Setup

We adapted the published code from \cite{6} for the topological embedding extractor and trained the model with cross entropy loss. In all our experiments, we used RMSProp \cite{37} with a learning rate\(^4\) of $\eta = 5 \times 10^{-5}$ and decayed the learning rate multiplying it by 0.1 at 80, 120 and 160 epochs. All models were trained for a maximum of 200 epochs. We used an effective batch size of 32. If the batch did not fit into memory we used smaller batches with gradient accumulation. To ensure robustness of our conclusions, we run every experiment with six different random seeds and report the mean and standard deviation. Throughout the training we monitored validation accuracy, and reported test set results for the model that achieved best validation set performance.

\(^4\)We experimented with setting of $\eta \in \{1, 2, 3, 5, 7, 10\} \times 10^{-5}$ and found $\eta = 5 \times 10^{-5}$ to consistently perform the best.
Figure 5: **Testing the O2I limit.** Subfigure (a) depicts the test set performance as a function of training dataset size for the nMNIST dataset, while subfigures (b) and (c) show the test set performance as a function of model capacity for the nMNIST dataset and the nCAMELYON dataset, respectively.

Figure 6: **Testing the O2I limit.** (a) mean validation set accuracy heatmap for max pooling operation, and (b) minimum required training set size to achieve the noted validation accuracy. We test training set sizes $\in \{1400, 2819, 5638, 7500, 11276, 22552\}$ and report the minimum amount of training examples that achieve a specific validation performance pooling over different network capacities.

### 4.2 Results

In this subsection, we present and discuss the main results of our analysis. Unless stated otherwise, the capacity of the ResNet-50 network is about $2.3 \times 10^7$ parameters. Additional results and analysis are presented in the supplementary material.

**Image-level annotations:** For this experiment, we vary the O2I ratio on nMNIST and nCAMELYON to test its influence on the generalization of the network. Figure 4 depicts the results for the best configuration according to the validation performance: we use max-pooling and receptive field sizes of $33 \times 33$ and $9 \times 9$ pixels for the nMNIST and nCAMELYON datasets, respectively. For the nMNIST dataset, the plot represents the mean over 6 random seeds together with the standard deviation; while for the nCAMELYON dataset we report an average over both the 6 seeds and the crop sizes. We find that our pipeline achieves reasonable test set accuracies for the O2I ratios larger than 0.3% for the nMNIST dataset and the O2I ratios above 1% for the histopathology dataset. For both datasets, smaller O2I ratios lead to poor or even random test set accuracies.

**O2I limit vs. dataset size:** In order to understand better the CNNs’ generalization problems for very small O2I ratios, we test the influence of the training set size on model generalization for the nMNIST data. We tested six different set sizes ($1400, 2819, 5638, 7500, 11276, 22552$). In Figure 5a, we show the results for max-pooling and a receptive field of $33 \times 33$ pixels. We observe that larger datasets lead to better generalization and this increment is more pronounced for small O2I ratios. To gain further insights, we plot a heatmap representing the mean validation set results for all

---

1. We decrease the training set size by selecting a subset of the original set and increase its size by allowing to reuse each digit 3.
2. More precisely, we plot the mean of all pipeline configurations that surpassed 70% training accuracy.
considered O2I and training set sizes (Figure 6a) as well as the minimum number of training examples required to achieve a validation accuracy of 70% and 85% (Figure 6b). We observe that in order to achieve good classification generalization the required training set size should rapidly increase with the decrease of the O2I ratio.

**O2I limit vs. capacity:** In this experiment, we train networks with different capacities — by uniformly scaling the initial number of filters in convolutional kernels by $\{1, 1.5, 2, 3, 4\}$. We show the test set performances as a function of the O2I ratio and the network capacity in Figures 5b and 5c for the nMNIST (with 11k training points) and nCAMELYON data, respectively. On nMNIST, we observe a clear trend, where the model test set performance increases with capacity and this boost is larger for smaller O2Is. We hypothesize, that this generalization improvement is due to the model ability to learn-to-ignore the input data noise, with smaller O2I there is more noise to ignore and, thus, higher network capacity is required to solve the task. However, for the nCAMELYON dataset, this trend is not so pronounced and we attribute this to the limited dataset size (more precisely to the small number of unique lesions). These results suggest that collecting a very large histopathology dataset might enable training of the CNN models using only image level annotations.

**Inductive bias:** In this experiment, we test the effect of the topological embedding receptive field size on model performance. We report the test accuracy as a function of the O2I ratio and the receptive field size for nMINIST in Figure 7a and for nCAMELYON in Figure 7b. Both plots depict results for the global max pooling operation. For nMNIST, we observe that a receptive field that is bigger than the area occupied by one single digit leads to best performances; for example, receptive fields of $33 \times 33$ and $177 \times 177$ pixels clearly outperform the smallest tested receptive field of $9 \times 9$ pixels. However, for the nCAMELYON dataset we observe that the smallest receptive field actually performs best suggesting that most of the class-relevant information is contained in the texture.

**Global pooling operations:** In this experiment, we compare the performance of different pooling approaches. We present the relation between test accuracy and pooling function for different O2I ratios with a receptive field of $33 \times 33$ pixels for nMNIST in Figure 8a and $9 \times 9$ pixels for nCAMELYON in Figure 8b. On the one hand, for the nMNIST dataset, we observe that for the relatively large O2I ratios, all pooling operations reach similar performance; however, for smaller O2Is we see that max-pooling is the best choice. We hypothesize that the global max pooling operation is best suited to remove nMNIST-type of structured input noise. On the other hand, when using the histopathology dataset, for the smallest O2I mean and soft attention poolings reach best performances; however, these outcomes might be affected by the relatively small nCAMELYON dataset used for training.

**Optimization:** In our large scale nMNIST experiments (when using $\approx$ 11k datapoints), we observed that some of the configurations have problems fitting the training data\footnote{We chose the maximum factor so that the largest resolution images still fit in our available GPU memory. For images with O2I ratio 0.07 the available GPU memory prevented us from testing networks with higher capacity.}. In some runs, after significant efforts put into model hyperparameter selections, the training accuracy was close to random. To investigate this issue further, we followed the setup of randomized experiments from \cite{42, 3} and we substituted the nMNIST datapoints with data points that were sampled from an isotropic Gaussian distribution. On the one hand, we observed that all the tested setups of our pipeline were able to memorize the Gaussian samples, while, on the other hand, most setups were failing memorize the nMNIST dataset for small and very small O2I ratios – suggesting that our nMNIST data is harder to memorize than isotropic Gaussian noise. To provide the reader with some experimental evidence, we depict time to fit the training data (in epochs) in Figure 9a as well as number of successes in Figure 9b for different O2I ratios and pooling method\footnote{We did not observe optimization problems for small sizes of the nMNIST nor for nCAMELYON datasets.}. We observe that the optimization gets progressively harder with O2I decrease and that max pooling is the most robust to this decrease. Moreover, we note that the optimization is consistent across random seeds, where all trainings are either successful or fail to converge\footnote{We define an optimization to be successful if it the train set accuracy surpassed 99%.}. We argue that the nMNIST structured noise and its compositionality may be a “harder” type of noise for the CNNs than Gaussian isotropic noise.

\footnote{We spent significant effort adapting optimization hyperparameters to unsuccessful runs and were unable to make them fit the training data.}
5 Conclusions

Although low input image signal-to-noise scenarios have been extensively studied in signal processing field (e.g. in tasks such as image reconstruction), less attention has been devoted to low signal-to-noise classification scenarios. Thus, in this paper we identified an unexplored machine learning problem, namely image classification in low and very low signal-to-noise ratios. In order to study such scenarios, we built two datasets that allowed us to perform controlled experiments by manipulating the input image signal-to-noise ratio and highlighted that CNNs struggle to show good generalization for low and very low signal-to-noise ratios even for a relatively elementary MNIST-based dataset. Finally, we ran a series of controlled experiments that explore both a variety of CNNs’ architectural choices and the importance of training data scale for the low and very low signal-to-noise classification. One of our main observations was that properly designed CNNs can be trained in low O2I regime without using any pixel-level level annotations and generalize if we leverage enough training data; however, the amount of training data required for the model to generalize scales rapidly with the inverse of the O2I ratio. Thus, with our paper (and the code release) we invite the community to work on data-efficient solutions to low and very low signal-to-noise classification.

11 We ran more than 750 experiments each with 6 different seeds.
Our experimental study has some limitations: First, due to the lack of large scale dataset that allows for explicit control of the input signal-to-noise ratios, we were forced to carry most of analysis on synthetically built nMNIST datasets. As a real life dataset, we used crops from hystopathology CAMELYON dataset; however, due to relatively small number of unique lesions we were unable to scale all hystopathology experiments to the extent of the nMNIST experiments, and, as result, some conclusions might be affected by the limited dataset size. Second, all the tested models improve the generalization with larger dataset sizes; however, scaling datasets such as CAMELYON to tens of thousands of datapoints might be prohibitively expensive. Instead, further research should be devoted to developing computationally-scalable, data-efficient inductive biases that can handle very low signal-to-noise ratios with limited dataset sizes. Finally, we studied low signal-to-noise scenarios only for binary classification scenarios; further investigation should be devoted to multi-class problems. We hope that this study will stimulate more research in image classification for low signal-to-noise input scenarios.

Acknowledgements

We like to thank Josh Romoff, Mido Assran, Adriana Romero, and Pascal Vincent for useful feedback and insightful discussions.

References


A Datasets

In this section, we provide additional details about the datasets used in our experiments.

A.1 Needle MNIST

Needle MNIST (nMNIST) dataset is designed as a binary classification problem: *Is there a 3 in this image?*. To generate nMNIST, we use the original training, validation and testing splits of the MNIST dataset and generate different nMNIST subsets by varying the object-to-image (O2I) ratio, resulting in O2I being 19.1%, 4.8%, 1.2%, 0.3%, and 0.075%. We define positive images as the ones containing exactly one digit 3 and negative images as images without any instance of it. We keep the original MNIST digit size and place digits randomly onto a clear canvas to generate a sample of the nMNIST dataset. More precisely, we adapt the O2I ratio by changing the canvas size, resulting in nMNIST image resolution being in $64 \times 64$, $128 \times 128$, $256 \times 256$, $512 \times 512$, and $1024 \times 1024$ pixels. To assign MNIST digits to canvas, we split the MNIST digits into two subsets: digit-3 versus clutter (any digit from a set of \{0, 1, 2, 4, 5, 6, 7, 8, 9\}). For the positive nMNIST images, we sample one digit 3 (without replacement) and $n$ digits (with replacement) from the digit-3 and clutter subsets, respectively. For the negative nMNIST images, we sample $n + 1$ instances from the clutter subset. We adapt $n$ to keep approximately constant object density for all canvas and choose $n$ to be 2, 5, 25, 100, and 400 for canvas resolutions $64 \times 64$, $128 \times 128$, $256 \times 256$, $512 \times 512$, and $1024 \times 1024$, respectively. As result, for each value of O2I ratio, we obtain 11276, 1972, 4040 of training, validation and testing images, out of which 50% are negative and 50% are positive images. We present both positive and negative samples for different O2I ratios in Figure 10.

![Figure 10: Example images from our MNIST dataset with different O2I ratios. Top row images represent positive examples — digit 3 is present (marked with red rectangle), while bottom row depicts negative images. Note that for visualization purposes all images have been rescaled to the same resolution.](image)

A.2 Needle CAMELYON

Needle CAMELYON (nCAMELYON) is designed as a binary classification task: *Are there breast cancer metastases in the image or not?*. We rely on the pixel-level annotations within CAMELYON to extract samples for nCAMELYON. We use downsampling level 3 from the original whole slide image using the MultiResolution Image interface released with the original CAMELYON dataset. For positive examples, we identify contiguous regions within the annotations, and take 50 random crops around each contiguous region ensuring that the full contiguous region is inside the crop, and total number of lesion pixels inside the crop are in the desired O2I ratio. The negative crops are...
taken from healthy images randomly filtering for images that are mostly background using a heuristic that the average green pixel value in the crop is below 200. Since CAMELYON dataset contains images acquired by 5 different centers, we split training, validation and test sets center-wise to avoid any contamination of data across the three sets. All crops coming from center 3 are part of the validation set, and all crops coming from center 4 are part of the test set. All images are generated for resolutions 128 × 128, 256 × 256, 512 × 512, and 1024 × 1024 and are split into 4 different O2I ratios: (100 − 50)%, (50 − 10)%, (10 − 1)%, and (1 − 0.1)%.

Figure 11 shows examples of images from nCAMELYON dataset, Table 1 presents number of unique lesions in each dataset, and Table 2 depicts number of dataset images stratified for image resolution and O2I ratios.

### Table 1: Number of unique lesions extracted for each set of the nCAMELYON data for different O2I ratios and crop sizes.

<table>
<thead>
<tr>
<th>Crop Size</th>
<th>O2I ratio</th>
<th>128</th>
<th>256</th>
<th>512</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Train</td>
<td>Val</td>
<td>Test</td>
<td>Train</td>
</tr>
<tr>
<td>(50 - 100) %</td>
<td>20</td>
<td>0</td>
<td>8</td>
<td>27</td>
</tr>
<tr>
<td>(10 - 50) %</td>
<td>84</td>
<td>12</td>
<td>16</td>
<td>101</td>
</tr>
<tr>
<td>(1 - 10) %</td>
<td>176</td>
<td>17</td>
<td>18</td>
<td>227</td>
</tr>
<tr>
<td>(0.1 - 1) %</td>
<td>33</td>
<td>5</td>
<td>5</td>
<td>93</td>
</tr>
</tbody>
</table>

### B Experimental Setup

In this section, we provide additional details about the pipeline used in the experiments. More precisely, we formally define global pooling operations and provide detailed description of the different architectures.
Table 2: Number of crops extracted for each set of the nCAMELYON data for different O2I ratios and crop sizes. Note that the dataset is balanced (e.g., 50% are positive images and 50% are negative). Moreover, for positive images we have relatively small number of unique cancer regions as noted in Table 1.

<table>
<thead>
<tr>
<th>Crop Size</th>
<th>128</th>
<th>256</th>
<th>512</th>
</tr>
</thead>
<tbody>
<tr>
<td>O2I ratio</td>
<td>Train</td>
<td>Val</td>
<td>Test</td>
</tr>
<tr>
<td>(50 - 100)%</td>
<td>1000</td>
<td>0</td>
<td>400</td>
</tr>
<tr>
<td>(10 - 50)%</td>
<td>4200</td>
<td>600</td>
<td>800</td>
</tr>
<tr>
<td>(1 - 10)%</td>
<td>8686</td>
<td>850</td>
<td>900</td>
</tr>
<tr>
<td>(0.1 - 1)%</td>
<td>1488</td>
<td>247</td>
<td>207</td>
</tr>
<tr>
<td>negative</td>
<td>19608</td>
<td>6000</td>
<td>6100</td>
</tr>
</tbody>
</table>

B.1 Global pooling operations

In our experiments, we are testing four different global pooling functions: max-pooling, mean-pooling, logsumexp and soft attention. The max pooling operation simply returns the maximum value per each channel in the topological embedding. This operation can be formally defined as:

$$ E^{l} = \max_{w} \max_{h} E_{[w,h]}^{t}. $$

(1)

Alternatively, one could use an average pooling operation that computes mean value for each channel in the topological embedding. This pooling operation can be formally defined as:

$$ E^{l} = \frac{1}{w_{enc} h_{enc}} \sum_{w=1}^{w_{enc}} \sum_{h=1}^{h_{enc}} E_{[w,h]}^{t}. $$

(2)

Finally, attention based pooling include additional weighting tensor $a$ of dimension $(w_{enc} \times h_{enc} \times e_{enc})$ that rescales each topological embedding before averaging them. This operation can be formally defined as:

$$ E^{l} = \sum_{w=1}^{w_{enc}} \sum_{h=1}^{h_{enc}} a_{[w,h]} \cdot E_{[w,h]}^{t} $$

(3)

$$ s.t. \sum_{w=1}^{w_{enc}} \sum_{h=1}^{h_{enc}} a_{[w,h]} = 1 $$

(4)

In our experiments, following [16], we parametrize the soft-attention mechanisms as $a_{[w,h]} = \text{softmax}(f(E_{spat})_{[w,h]})$, where $f(\cdot)$ is modelled by two fully connected layers with tanh-activation and 128 hidden units.

B.2 Model architecture details

We adapt the BagNet architecture proposed in [6]. An overview of the architectures for the tested three receptive field sizes is shown in Table 3. We depict the layers of residual blocks in brackets and perform downsampling using convolutions with stride 2 within the first residual block. Note that the architectures for different receptive fields differ in the number of $3 \times 3$ convolutions. The rightmost column shows a regular ResNet-50 model. The receptive field is decreased by replacing $3 \times 3$ convolutions with $1 \times 1$ convolutions. We increase the number of convolution filters by a factor of 2.5 if the receptive field is reduced to account for the loss of the trainable parameters. Moreover, when testing different network capacities we evenly scale the number of convolutional filters.
B.3 Initial Exploration Phase

Before committing to a single optimization scheme, we evaluated a variety of optimizers (Adam, RMSprop and SGD with momentum), learning rates ($\eta \in \{1, 2, 3, 5, 7, 10\} \times 10^{-5}$), and 3 learning rate schedules. Here, we only report the results for the configuration that performed best in the initial exploration phase.

C Additional results

In this section, we provide additional experimental results as well as additional visualizations of the experiments presented in the main body of the paper.

C.1 Class-imbalanced classification

In many medical imaging datasets, it is common to be faced with class-imbalanced datasets. Therefore, in this experiment, we use our nMNIST dataset and test CNNs generalization under moderate and severe class imbalanced scenario. We alter the training set class balance by altering the proportion of positive images in the training dataset and use the following balance values 0.01, 0.1, 0.25, 0.5, 0.75, 0.9 and 0.99, where a value of 0.01 means almost no positive examples and 0.99 indicates very low number of negative images available at training time. Moreover, we ensure that the dataset size is constant ($\approx 11$k) and only the class-balance is modified. We run the experiments using the O2I ratio of 1.2%, three receptive field sizes ($9 \times 9$, $33 \times 33$ and $177 \times 177$ pixels) and four pooling operations (mean, max, logsumexp and soft attention). For each balance value, we train 6 models using 6 random seeds and we oversample the underrepresented class. The results are depicted in Figure 12. We observe that the model performance drops as the the training data becomes more unbalanced and that max pooling and logsumexp seem to be the most robust to the class imbalance.

C.2 Increase of model capacity for small dataset sizes.

We also tested the effect of model capacity increase while having access only to a small dataset (3k class-balanced images) and contrast it with a larger dataset of $\approx 11$k training images. We run this experiment on the nMNIST dataset using a network with $2.3 \times 10^7$ parameters using global max pooling operation and three different receptive field sizes: $9 \times 9$, $33 \times 33$ and $177 \times 177$ pixels. The results are depicted in Figure 13. It can be seen that the model’s capacity increase does not lead to better generalization, for small size datasets of $\approx 3$k.

C.3 O2I limit vs. dataset size

In this section, we report additional results for all tested global pooling operations on O2I limit vs. dataset size. We plot a heatmaps representing the validation set results for all considered O2I and training set sizes (Figure 14) as well as the minimum number of training examples required to achieve a validation accuracy of 70% and 90% (Figure 15).

Figure 12: Impact of the training set balance on model accuracy for different pooling operations and receptive field sizes.
Figure 13: Impact of the network capacity on the generalization performance dependent on the training set size for nMNIST at O2I ratio = 1.2%. The improvement based on the increased network capacity shrinks with smaller training set.

Figure 14: Testing the O2I limit. Validation set accuracy heatmap for max, logsumexp, mean and soft attention poolings. We test training set sizes $\in \{1400, 2819, 5638, 7500, 11276, 22552\}$ and report the average validation accuracy.

C.4 Weakly supervised object detection: nMNIST

We test the object localization capabilities of the trained classification models by examining their saliency maps. Figure 16 shows examples of the nMNIST dataset with the object bounding box in blue and the magnitude of the saliency in red. We rescale the saliency to $[0, 1]$ for better contrast. However, this prevents the comparison of absolute saliency values across different images. In samples containing an object of interest, the models correctly assign high saliency to the regions surrounding the relevant object. On negative examples, the network assigns homogenous importance to all objects. We localise an object of interest as the location with maximum saliency. We follow [29] to quantitatively examine the object detection performance using the saliency maps of the models. We plot the corresponding average precision in Figure 17. We find that the detection performance deteriorates for smaller O2I ratios regardless of the method. This is aligned with the classification accuracy. For small O2I ratios, max-pooling achieves the best detection scores. On larger O2I ratios, logsumexp achieves the best scores.

C.5 Weakly supervised object detection: nCAMELYON

We qualitatively show object detection on nCAMELYON in Figures 18-21 for True Positives, True Negatives, False Positives and False Negatives. We observe weak correlation between segmenta-
Figure 15: **Testing the O2I limit.** Minimum required training set size to achieve the noted validation accuracy. We test training set sizes $\in \{1400, 2819, 5638, 7500, 11276, 22552\}$ and report the minimum amount of training examples that achieve a specific validation performance pooling over different network capacities.

(a) $y = 1, \hat{y} = 1$
(b) $y = 1, \hat{y} = 0$
(c) $y = 1, \hat{y} = 0$
(d) $y = 0, \hat{y} = 0$

(e) $y = 1, \hat{y} = 1$
(f) $y = 1, \hat{y} = 0$
(g) $y = 1, \hat{y} = 0$
(h) $y = 0, \hat{y} = 0$

(i) $y = 1, \hat{y} = 1$
(j) $y = 1, \hat{y} = 0$
(k) $y = 1, \hat{y} = 0$
(l) $y = 0, \hat{y} = 0$

(m) $y = 1, \hat{y} = 1$
(n) $y = 1, \hat{y} = 0$
(o) $y = 1, \hat{y} = 0$
(p) $y = 0, \hat{y} = 0$

Figure 16: Example images from the nMNIST validation set and their corresponding saliency maps in red. We generate the saliency maps by calculating the absolute of the gradients with respect to the input image using max-pooling, a receptive field of 33, and ResNet-50 capacity. From top to bottom, we show random examples for O2I ratios of $\{19.14, 4.79, 1.20, 0.30\}\%$. We annotate the object of interest with a blue outline. The captions show the true label $y$ and the prediction $\hat{y}$. 
Figure 17: Average precision for detecting the object of interest using the saliency maps for nMNIST. We adapt [29] and use the localize an object by the maximum magnitude of the saliency. We use the magnitude of the saliency as the confidence of the detection. We count wrongly localised objects both as false positive and false negative. For images without object of interest, the we increase the false positive count only. We plot results for max-pooling, a receptive field of 33, a training set with 11276 examples and ResNet-50 capacity. (a) shows the dependence of the AP on the pooling method using $RF = 33 \times 33$, (b) shows the dependence on the receptive field using max-pooling.

Figure 17: Average precision for detecting the object of interest using the saliency maps for nMNIST. We adapt [29] and use the localize an object by the maximum magnitude of the saliency. We use the magnitude of the saliency as the confidence of the detection. We count wrongly localised objects both as false positive and false negative. For images without object of interest, the we increase the false positive count only. We plot results for max-pooling, a receptive field of 33, a training set with 11276 examples and ResNet-50 capacity. (a) shows the dependence of the AP on the pooling method using $RF = 33 \times 33$, (b) shows the dependence on the receptive field using max-pooling.

tion maps and saliency maps, signifying that the classifier was able to focus on the object of interest instead of looking at superficial signals in the data.
Figure 18: Example True Positive Images of nCAMELYON validation sets and their corresponding segmentation maps with saliencies overlaid.
Figure 19: Example True Negative Image of nCAMELYON validation sets and corresponding saliency map.

Figure 20: Example False Negative Image of nCAMELYON validation sets and corresponding segmentation map with saliency overlaid.

Figure 21: Example False Positive Image of nCAMELYON validation sets and corresponding saliency map.
Table 3: Schematic of the architecture of the different topological embedding encoders used in this paper. The operations and their corresponding parameters of the residual blocks are denoted in brackets. The first block within each section performs downsampling using convolutions with stride 2. We use InstanceNorm instead of BatchNorm and test different pooling methods after the topological embeddings.

<table>
<thead>
<tr>
<th>RF=9</th>
<th>RF=33</th>
<th>RF=177</th>
</tr>
</thead>
<tbody>
<tr>
<td>conv, 1 × 1, 64</td>
<td>conv, 1 × 1, 64</td>
<td>conv, 1 × 1, 64</td>
</tr>
<tr>
<td>conv, 3 × 3, 64</td>
<td>conv, 3 × 3, 64</td>
<td>conv, 3 × 3, 64</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 64</td>
<td>conv, 1 × 1, 64</td>
<td>conv, 1 × 1, 64</td>
</tr>
<tr>
<td>conv, 1 × 1, 160</td>
<td>conv, 1 × 1, 160</td>
<td>conv, 1 × 1, 160</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 160</td>
<td>conv, 1 × 1, 160</td>
<td>conv, 1 × 1, 160</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
</tr>
<tr>
<td>conv, 3 × 3, 128</td>
<td>conv, 3 × 3, 128</td>
<td>conv, 3 × 3, 128</td>
</tr>
<tr>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
</tr>
<tr>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
</tr>
<tr>
<td>conv, 1 × 1, 320</td>
<td>conv, 1 × 1, 320</td>
<td>conv, 3 × 1, 328</td>
</tr>
<tr>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
</tr>
<tr>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
</tr>
<tr>
<td>conv, 1 × 1, 320</td>
<td>conv, 1 × 1, 320</td>
<td>conv, 3 × 1, 328</td>
</tr>
<tr>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
</tr>
<tr>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
<td>conv, 1 × 1, 128</td>
</tr>
<tr>
<td>conv, 1 × 1, 320</td>
<td>conv, 1 × 1, 320</td>
<td>conv, 3 × 1, 328</td>
</tr>
<tr>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
</tr>
<tr>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
</tr>
<tr>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
</tr>
<tr>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
</tr>
<tr>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
</tr>
<tr>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
<td>conv, 1 × 1, 256</td>
</tr>
<tr>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
<td>conv, 1 × 1, 640</td>
</tr>
<tr>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
<td>conv, 1 × 1, 1024</td>
</tr>
<tr>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
</tr>
<tr>
<td>conv, 1 × 1, 1280</td>
<td>conv, 1 × 1, 1280</td>
<td>conv, 1 × 1, 1280</td>
</tr>
<tr>
<td>conv, 1 × 1, 2048</td>
<td>conv, 1 × 1, 2048</td>
<td>conv, 1 × 1, 2048</td>
</tr>
<tr>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
<td>conv, 1 × 1, 512</td>
</tr>
<tr>
<td>conv, 1 × 1, 1280</td>
<td>conv, 1 × 1, 1280</td>
<td>conv, 1 × 1, 1280</td>
</tr>
<tr>
<td>conv, 1 × 1, 2048</td>
<td>conv, 1 × 1, 2048</td>
<td>conv, 1 × 1, 2048</td>
</tr>
</tbody>
</table>