A SAMPLE-BASED METHOD FOR SEMANTIC UNDERSTANDING OF NEURAL NETWORK DECISIONS

Anonymous authors
Paper under double-blind review

ABSTRACT

Interpretability in deep learning is one of the largest obstacles to its more widespread adoption in critical applications. A variety of methods have been introduced to understand and explain decisions made by Deep Models. A class of these methods highlights which features are most influential to model predictions. These methods have some key weaknesses. First, most of these methods are applicable only to the atomic elements that make up raw inputs to the model (e.g. pixels or words). Second, these methods generally do not distinguish between the importance of features individually and their importance due to interactions with other features. As a result, it is difficult to explore high-level questions about how models use features during decision-making. We tackle these issues by proposing Sample-Based Semantic Analysis (SBSA). We use Sobol variance decomposition as our sample-based method which allows us to quantify the importance of semantic combinations of raw inputs and highlight the extent to which these features are important individually as opposed to due to interactions with other features. We demonstrate the ability of Sobol-SBSA to answer a richer class of questions about the behavior of Deep Learning models by exploring how CNN models from AlexNet to DenseNet use regions when classifying images. We present three key findings. 1) The architectural improvements from AlexNet to DenseNet manifested themselves in CNN models utilizing greater levels of region interactions for predictions. 2) These same architectural improvements increased the importance that CNN models placed on the background of images 3) Adversarially robust CNNs reduce the reliance of modern CNNs on both of the descrived trends. Our proposed method is generalizable to a wide variety of network and input types and can help provide greater clarity about model decisions.

1 INTRODUCTION

Deep learning models are becoming endemic in various applications. As models are increasingly used for critical applications in medicine such as detecting lung nodules (Schultheiss et al., 2021) or autonomous driving (Li et al., 2021), it is important to either create interpretable models or to make opaque models human interpretable. This paper focuses on the latter. Existing methods developed over the last decade for doing this can be broken down into model agnostic vs model dependent. Model agnostic methods, such as Shapley values (Kononenko et al., 2013) and Integrated Gradients (Sundararajan et al., 2017) weigh the importance of input features without relying on the structure of the model. In contrast, methods such as GradCam (Selvaraju et al., 2017) and GradCam++ (Chattopadhay et al., 2018) are heavily dependent on model architecture.

While both of these methods yield valuable information about models, they share two common gaps. First, neither of them reports metrics that distinguish between the features in input space that are individually important and features that are important because of their interaction with other features. Second, the above methods are generally applied to inputs at their most granular level (pixels, words, etc..). The combination of these two gaps limits the conclusions that Machine Learning practitioners can make about individual model predictions, as well the behavior of models as a whole.

We address these limitations in two key ways. First, we introduce a two-part framework called Sample-Based Semantic Analysis (SBSA). The first part of the framework is a function that generates semantic representations of inputs and is able to map those semantic combinations to real

numbers. The second part of the framework is a black-box sample-based sensitivity method. In this case, the Sobol method which reports the importance of individual features and their interactions. Second, we demonstrate the ability of Sobol-SBSA to answer a richer set of questions than standard interpretability methods by applying it to CNN models in the context of ImageNet. We ask two particular questions. 1) How did CNN model's use of regions evolve as architectures were developed from AlexNet to DenseNet? 2) How do adversarially training robust versions of these models change the manner in which these architectures utilize regions such that they are less likely to exploit spurious correlations?

The key results and contributions of this paper are as follows:

1. We present a general-purpose framework for using sample-based sensitivity methods to analyze the importance of semantic representations of inputs and test it using a variety of black-box methods.
2. We demonstrate that the Sobol method outperforms other popular black box methods, Integrated Gradients, Shapley (Kernel Shap), and LIME, for selecting both the most and least important regions to CNN predictions.
3. We show, *through direct measurement*, that the main impacts of the evolution of CNN architectures were increasing the extent to which they used region interactions and to which they relied on background information in images. Similarly, we show that adversarially robust versions of CNNs reduce both of these effects for modern CNNs.

2 Related Work

In recent years, interest has grown in interpretability methods that can quantify the importance of feature interactions.Janizek et al. (2020) introduced an extension to Integrated Gradients, called Integrated Hessians, that quantified the importance of pairwise interactions of features, while Zhang et al. (2020) built on this work by presenting a similar quantification through Shapley Interactions. While both methods are powerful, they are expensive. These methods require the separate calculation of individual feature importance and interactions, as well as pairwise comparisons in order to quantify interactions.

The work most closely related to ours was done by Fel et al. (2021), who addressed the issue of additional computational expense by using the Sobol method to calculate the importance of regions in ImageNet models. They demonstrated that Sobol outperformed white box methods like Grad-CAM and another black box method, RISE (Petsiuk et al., 2018). However, they did not perform comparisons against other popular black box attribution methods like Integrated Gradients (Sundararajan et al., 2017), Shapley (Kononenko et al., 2013), and Local Interpretable Model-Agnostic Explanations, LIME (Ribeiro et al., 2016). Additionally, they did not demonstrate how the Sobol measurement of both interactive and primary feature importance could be used to answer larger overarching questions about models. Finally, they did not explore how the assumption that input features to a model are uncorrelated limits the circumstances under which Sobol can be used. We address all of these issues in our work.

3 Methodology

In this section, we describe the two components of SBSA and specify how we use it to analyze the importance of image regions in ImageNet. In particular, we describe how we semantically map image regions to quantities that can be analyzed with a sampling-based method, and the specifics of Sobol as a sampling-based sensitivity method.

3.1 Sample-Based Semantic Analysis (SBSA)

Let us define the following variables. $x \in \mathbf{R}^d$ is an input to a model, $f : x \to y \in \mathbf{R}^k$ is a model that takes x as an argument and produces y, $\tilde{x}_i \in \mathbf{R}^d$ is a sample of x, and $N \in \mathbf{Z}$ is a prescribed integer that helps to determine the number of $\tilde{x}_i$ samples generated. Most sample-based sensitivity methods operate by generating a number of samples that is some function of N and d. For example,

$\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{Nd}$. The model is then evaluated on these samples yielding $f(\tilde{x}_1), f(\tilde{x}_2), \ldots, f(\tilde{x}_{Nd})$. Sample-based sensitivity methods, such as Sobol, use these outputs to determine the importance of components of x to the model output, y.

One thing that immediately becomes clear is that for deep learning applications with high-dimensional inputs, such as images, videos, and long documents, applying this process to raw inputs is prohibitively expensive. This issue can be greatly minimized if one turns to semantic representations of inputs instead. In this paper, a semantic representation of an input is defined as follows. **A semantic representation of an input, x, is some combination of the raw components of that input which yields a human recognizable higher order feature, such as the colors or regions of an image or grammatical parts of sentences**. We define this semantic representation as $S \in \mathbf{R}^m$, where $m < d$. Recalling that most sample-based sensitivity methods operate on real numbers, we define two mapping objects.

$$G : x \in \mathbf{R}^d \rightarrow S \in \mathbf{R}^m, \quad G^{-1} : S \in \mathbf{R}^m \rightarrow\approx x \in \mathbf{R}^d \quad m < d \tag{1}$$

$$H : S \in \mathbf{R}^m \rightarrow r \in \mathbf{R}^l, \quad H^{-1} : r \in \mathbf{R}^l \rightarrow\approx S \in \mathbf{R}^m \quad l < m \tag{2}$$

G maps the raw input, x, to some lower dimensional semantic representation S, and H maps the semantic representation to some lower dimension vector of real numbers, r. Both mappings are invertible. Given these mappings, SBSA generates samples of r, $\tilde{r}_1, \tilde{r}_2, \ldots, \tilde{r}_{ld}$. From these samples, samples of the original input are generated by first mapping these samples of real numbers to samples of the semantic representations of x, $\tilde{S}_i$, and then mapping these samples of semantic representations to samples of the raw inputs, $\tilde{x}_i$.

$$\{H^{-1}(\tilde{r}_1), H^{-1}(\tilde{r}_2), \ldots, H^{-1}(\tilde{r}_{Nd})\} = \{\tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_{Nd}\} \tag{3}$$

$$\{G^{-1}(\tilde{S}_1), G^{-1}(\tilde{S}_2), \ldots, G^{-1}(\tilde{S}_{Nd})\} = \{\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{Nd}\} \tag{4}$$

The model is then evaluated on the samples of the raw input, $\tilde{x}_i$. The key here is that since the sampling was done in r, the sensitivity analysis reports the importance of different components of the semantic representations of the input, S. The author's note that, despite the notation, G and H need not be explicit functions. Any mechanism that that provides a mapping between the original inputs, x, semantic components of these inputs, S, and a reduced representation of the semantic components, r, is can be used. Despite the multitude of choices, there are two properties that make a mapping ideal in this context.

Property 1 (Sensitivity) Any change in the reduced representation of semantic components of x should result in a change x. Sample based sensitivity methods observe how different samples of inputs change model outputs in order to determine the importance of different components of the inputs. **Property 1**: insures that all of these samples contribute information to the sample based sensitivity analysis method. **Property 2 (Approximate Reconstruction)**: When using the reduced representation produced from the original input, x, the inverse functions should closely approximate the original input. Sample based sensitivity analysis methods construct samples that are uniformly distributed between 0 and 1, $U \approx [0, 1]^m$. These samples are scaled to the values of the inputs of interest and the value of the original input of interest, r is used as the mean of this uniform distribution (Herman & Usher, 2017). **Property 2** insures that samples of the reduced representation of x will be able to amplify and mask different components of x with approximately equal probability.

In the following section we describe the use of SBSA via image regions.

3.2 Sample-Based Semantic Analysis (SBSA) Applied to ImageNet and Regions

In this section, we illustrate how we perform sensitivity analysis of different regions in ImageNet models based on the SBSA framework. We will first discuss our mapping functions. Then we will detail the Sobol method for sensitivity analysis and the measures of importance that it produces.

Given an image $x \in \mathbf{R}^d$ where $d = W \times L$, our input to semantic mapping function, G, extracts regions of x, R_k. The mapping, H, from the semantic representations to a reduced real number vector, r, is simply the sum of the value of pixels in the region.

$$G : x \in \mathbf{R}^d \rightarrow \{S_1, \ldots, S_l\} \in \mathbf{R}^{l \times w \times h}, \quad S_j = x_{\{t,p\} \in R_k} \in \mathbf{R}^{w \times h} \tag{5}$$

$$H : \{S_1, \ldots, S_l\} \in \mathbf{R}^{l \times w \times h} \rightarrow \{r_1, \ldots, r_l\} \in \mathbf{R}^l, \quad r_j = \sum_{\{t,p\} \in R_k} x_{tp} \tag{6}$$

Finally, the inverse mapping, H^{-1} involves normalizing each region, $\{x_{o:p,r:s}\}_j$ by the sum of the values of the pixel in that region, $\sum_{\{t,p\} \in R_k} x_{tp}$, and multiplying it by r_j. Then assigning the relevant indices in x the new values in the region. When r_j is equal to the summation of pixels in that region from the original image, this simply recovers the original image. When sampled, this reconstructs samples, $\tilde{x}_i$. Mathematically, the inverse mapping is as follows.

$$H^{-1} : \{r_1, \ldots, r_l\} \in \mathbf{R}^l \rightarrow \{S_1, \ldots, S_l\} \in \mathbf{R}^{l \times w \times h}, \quad S_j = r_j \frac{x_{\{t,p\} \in R_k}}{\sum_{\{t,p\} \in R_k} x_{tp}} \tag{7}$$

$$G^{-1} : \{S_1, \ldots, S_l\} \in \mathbf{R}^{l \times w \times h} \rightarrow x \in \mathbf{R}^{W \times L} \tag{8}$$

The above mapping, while simple, satisfies the properties of sensitivity and approximate reconstruction. As a result the samples of $\tilde{r}$, which represents semantic components of x, S, produces image samples, $\tilde{x}$, that amplify and mask regions of the image with relatively equal probability and uniformly. The Saltelli method, (Saltelli et al., 2010), which chooses optimal points in $[0, 1]$ for the Sobol method are used to construct these samples and the model outputs of images are fed to the Sobol method.

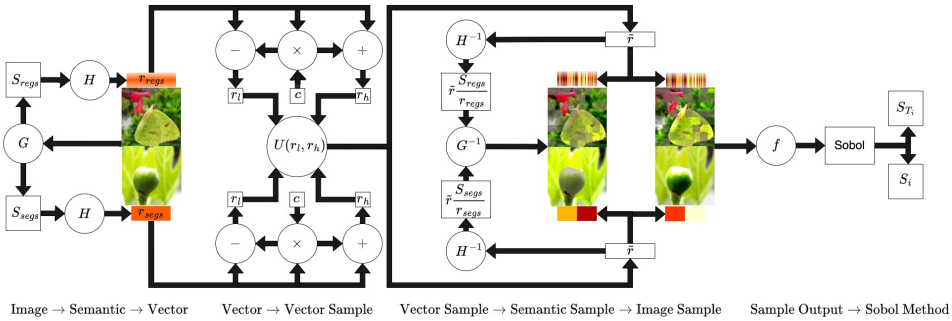


Figure 1: Examples of how our choice of mapping creates samples of images for regions (top) and segments (bottom). The segments are based on the segmentation of the validation set in ImageNet-S 919

Given these mappings, we apply the Sobol Sensitivy method to the low dimensional real vectors, r_j. Here we will briefly give an overview of the Sobol method. For more details about the implementation of Sobol, see Saltelli et al. (2010) and Herman & Usher (2017). The Sobol method is a variance-based sensitivity method. Given a model, $f : (x_1, \ldots, x_d) \in \mathbf{R}^d \rightarrow y$, the variance based first order effect of a component of the input, x, is:

$$V_i = V_{x_i}(E_{\mathbf{x}_{\sim i}}(y_j | x_i)) \tag{9}$$

where y_j is a component of the model output, x_i is a component of the input, x, $\mathbf{x}_{\sim i}$ are samples of the input where all components of the input except for i are varied, and V_{x_i} and $E_{\mathbf{x}_{\sim i}}$ are the variance and expectation over x_i and $\mathbf{x}_{\sim i}$ respectively. The Sobol first-order sensitivity is then the ratio of V_i to the variance of the model output, y_j.

$$S_i = \frac{V_i}{V(y_j)} \tag{10}$$

S_i quantifies the individual importance of the ith component of the input, x, to the jth component of the output, y. This equation essentially states that Sobol first order index, S_i, is the fraction

of the variance of the output, y_j that is accounted for by x_i. What makes Sobol unique is that it simultaneously calculates the importance of the interaction between a component of the input, x_i, and all other components of the input. This is called the total effect index and is calculated as:

$$S_{T_i} = 1 - \frac{V_{\mathbf{x}\sim i}(E_{x_i}(y_j|\mathbf{x}_{\sim i}))}{V(y_j)} = S_i + \sum_{k;k\neq i} S_{ik} + \sum_{k,j;k\neq i,j;j\neq i} S_{ikj} + \dots \tag{11}$$

This equation essentially states that the total effect index for x_i, S_{Ti}, is the difference between 1 and the fraction of the variance of the output, y_j, that is accounted for by all samples of the input in which every component of the input varies, except for i. Dividing both sides of 11 by S_{Ti} yields

$$1 = \frac{S_i}{S_{Ti}} + \sum_{k;k\neq i} \frac{S_{ik}}{S_{Ti}} + \sum_{k,j;k\neq i,j;j\neq i} \frac{S_{ikj}}{S_{Ti}} + \dots \tag{12}$$

The first term in equation 12 reports the extent to which a feature, x_i, is important to the model output due to the feature by itself. The larger the term, the greater the importance of the region by itself. Contrarily, the smaller the term larger the importance of the interaction of the feature to other features. We will refer to as the Primary Index Ratio (PIR) for the rest of the paper.

$$\text{PIR} = \frac{S_i}{S_{Ti}} \tag{13}$$

We implement the Sobol method using the Sensitivity Analysis Library (SALib) (Herman & Usher, 2017), which is an open source implementation of the Saltelli method Saltelli et al. (2010). We note that the number of samples used for the Sobol method is $N(d+2)$. For all of the experiments that follow, $N = 50$.

3.2.1 Choice of Regions

In order to demonstrate the ability of our method to address high level questions about CNNs, and to explore these questions at different levels of semantic representations of an image, we apply our pipeline to three types of regions. 1) equally sized image patches 2) machine annotated semantic segmentations of the ImageNet training set from Salient ImageNet Singla & Feizi (2021) and 3) human annotated semantic segmentations from the ImageNet-S 919 validation set (Gao et al., 2021). Salient ImageNet segments images into core regions (regions that should be important for predictions) and spurious ones. ImageNet-S is a dataset that was created for use in judging image segmentation task. *A key difference between image patches and Salient ImageNet, and ImageNet-S is that ImageNet-S strictly respects boundaries in images where the other two don't.* Figure 1 shows our pipeline when applied to example images from the ImageNet validation set and ImageNet-S 919.

4 Experiments

We demonstrate the validity of our pipeline by showing that Sobol-SBSA is able to accurately rank the importance of regions. We additionally demonstrate that Sobol-SBSA outperforms other standard black box models. Both of these are measured based on multiple measures of the effectiveness of interpretability methods.

With this established, we demonstrate the ability of Sobol-SBSA to answer high level questions about Deep models using CNNs as a case study. We explore three questions. 1) How did the use of region interactions evolve with CNNs? 2) How did the use of objects vs backgrounds evolve with CNNS? 3) What impact did training CNNs robustly have on the firs two questions? We provide quantitative results to these questions by applying Sobol-SBSA to region patches, Salient ImageNet segments, and ImageNet-S segments.

4.1 Comparison of Sobol-SBSA to Other Black Box Models

Our SBSA model can be used with a variety of black box models. Thus, we compare the following two methods against Sobol-SBSA.

- **Shapley (Shap-SBSA) (Kononenko et al., 2013):** Used with SBSA in a similar manner as Sobol-SBSA.
- **LIME (LIME-SBSA) (Ribeiro et al., 2016):** Used with SBSA in a similar manner as Sobol-SBSA.

In addition, we also compare against the following models.

- **Integrated Gradients (Sundararajan et al., 2017):** Cannot be used with SBSA since it requires gradients with respect to pixels. Instead, we aggregate pixel importance in regions and rank region importance based on this aggregation.
- **Random:** A control baseline where regions are randomly selected.

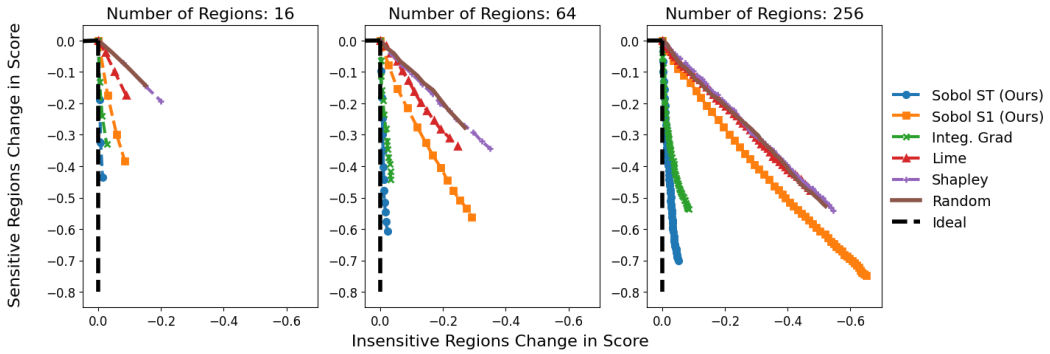


Figure 2: Plots of the change in the ground truth score of the ResNet50 when the top 20% of regions are masked vs the bottom 20% of regions. A steep slope is indicative of a more effective method since it means that the change in ground truth scores are significant when the top 20% of images are masked, but not when the bottom 20% of images are masked. From left to right this is plotted for when the regions are 4×4, 8×8, and 16×16 respectively.

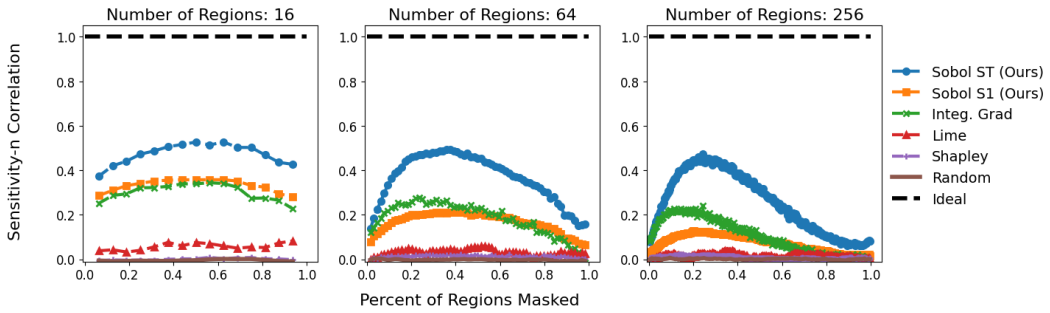


Figure 3: Plots of the sensitivity-n correlation for different sensitivity methods as a function of the percentage of regions masked. The sensitivity methods with values closer to one are more effective. From left to right this is plotted for when the regions are 4×4, 8×8, and 16×16 respectively.

We use two standard metrics for comparing interpretability methods. The first is measuring the change in the ground truth label score of a model when regions, as specified by the sensitivity method, are masked. We mask the top and bottom 20% of regions in an image. The second measurement is sensitivity-n correlation. Sensitivity-n correlation is a quantity proposed by Ancona et al. (2017) for comparing the effectiveness of attribution methods when determining which features are important to a model. Quantitatively, it is a measurement of the Pearson correlation between

$\sum_{i=1}^{n} R_i^c$ and $S_c(x) - S_c(x_{[x_S=0]})$. $\sum_{i=1}^{n} R_i^c$ is the sum of the attributions associated with the n input features that are masked and $S_c(x) - S_c(x_{[x_S=0]})$ is the difference in the score that the model produces when n input features are masked versus when none are. For each value of i, i random features are selected to be masked 100 times and the correlation is averaged over the examined data. A value closer to one means a more effective method.

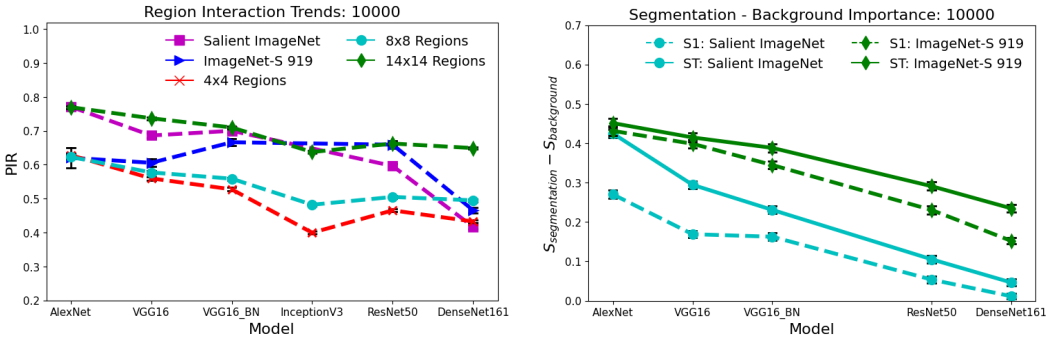
For all methods, we evaluate the importance of regions to ResNet50 on 1000 randomly selected ImageNet validation images. To explore whether or not region size would impact our results, we performed our experiments for 4×4, 8×8, and 16×16 regions. The number of samples is selected as a function of the number of regions, as detailed in section 3.2. For 4×4, 8×8, and 16×16 regions, the number of samples used for all methods are 900, 3300, and 12900 respectively.

Figures 2 and 3 show the results of the masking and sensitivity-n correlations respectively for all regions. Figure 2 plots the change in the model score when the most important regions are masked versus when the least. A steeper curve is more ideal since it means that the sensitivity method significantly decreases the model score when masking the most important regions, but has little impact when masking the least important regions. *The Sobol-SBSA is the most effective by both the masking and sensitivity-n measures*. The key takeaways from the plot are 1) Both Sobol measurements, S_{Ti} and S_i, are more effective at selecting the most important regions in an image, 2) S_{Ti} performs the best overall in picking the most and least important regions in an image, as well as more properly ranking the regions in between (as measured by sensitivity-n), and 3) S_{Ti} is the most robust to changes in region size, followed closely by Integrated Gradients.

4.2 What can Sobol-SBSA Tell us About CNNs Beyond Region Importance?

We have shown Sobol-SBSA's efficacy at ranking the importance of regions to CNN predictions. While Sobol-SBSA outperforms other black box methods in standard interpretability measures, the real advantage offered by Sobol-SBSA over other black box methods is the ability to answer large overarching questions about the behavior of Deep Learning models. We demonstrate this by using Sobol-SBSA to quantify how the use of regions evolves in CNN models from AlexNet to DenseNet161, and to understand the mechanism that causes adversarially robust CNN models to be less susceptible to spurious correlations in the data.

4.2.1 How have CNN Models Evolved their Use of Regions?



(a) The plots of the average mean of PIR for 10000 images for a series of CNN models when applied to images that are partitioned based on segmentations from ImageNet-S and Salient ImageNet, as well as when applied region patches of different sizes. For region patches, this is done for the top 20% of regions in an image as determined by S_T.

(b) The plots of the average difference in importance, S_T and S_i for segmented objects in ImageNet-S and Salient ImageNet as a function of models. 10000 images from each dataset were used.

Figure 4: PIR trends and the difference in importance between segmented objects and background for CNN models

To answer the question as to how the use of regions has changed as CNNs have evolved, we use three quantities derived from Sobol-SBSA. The PIR, defined in equation 13, which states the

extent to which a model relies on the interaction of features The smaller this ratio the larger the interactive effect. We additionally calculate the difference in individual and total importance between the segmented and background portions of an image in ImageNet-S 919 and Salient ImageNet ($S_{T_{segmentation}} - S_{T_{background}} and S_{i_{segmentation}} - S_{i_{background}}$).

We apply Sobol-SBSA to AlexNet, VGG16, VGG16_BN, InceptionV3, ResNet50, and DenseNet161. For all models with the exception of InceptionV3, the number of image patches chosen are 4×4, 8×8, and 14×14. The pre-trained InceptionV3 operates on an image that is 299×299 rather than 224×224. In order to compare similar region sizes, the number of regions for which Sobol-SBSA was applied to InceptionV3 were 5×5, 11×11, and 18×18. We note that we do not test our pipeline on InceptionV3 for ImageNet-S 919 or Salient ImageNet. The Salient ImageNet dataset masks are 224×224 which is not a valid input to the pre-trained InceptionV3. We therefore omit it for both segmentations in order to keep comparisons between the segmentations consistent. All of the results displayed in this section are based on 10000 random samples from the ImageNet validation set.

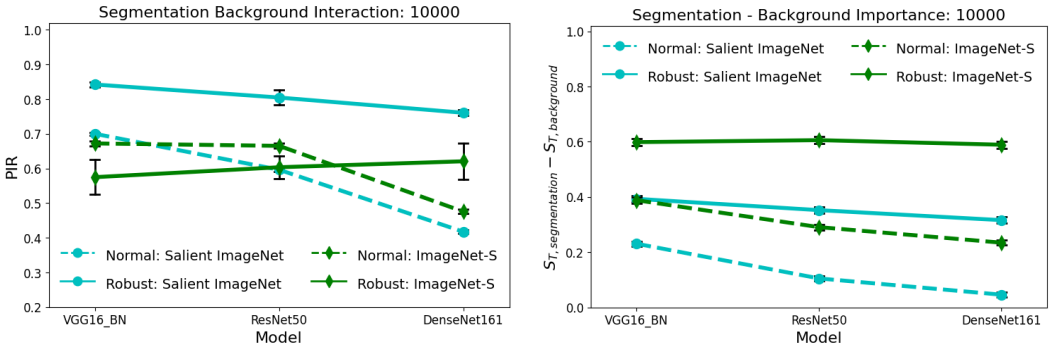
Figure 4a shows the average PIR for AlexNet, VGG16, VGG16_BN, InceptionV3, ResNet50, and DenseNet161 for different region sizes and the segmentations of ImageNet-S and Salient ImageNet. For the region patches, the average is calculated based top 20% of regions as measured by S_{Ti}. The key takeaway from this figure is that *one of results of the architectural changes that yielded modern CNNs was to increase the extent to which models used region interactions when making predictions*. This change was most noticeable for region patches and Salient ImageNet segmentations, both of which partition the images into areas that don't strictly respect boundaries. For ImageNet-S there is a slight decrease in the relative importance of interaction from AlexNet to VGG16, VGG16_BN, and ResNet50 before a large increase in DenseNet161. Figure 4b displays the difference between the importance of segmented parts of the image and the background for both S_T and S_i. For both ImageNet-S and Salient ImageNet, it is seen that this difference decreases as CNNs grow more modern. This figure shows that *another key result of the changes that yielded modern CNNs was to increase the importance of the background of images to model predictions*. To the authors' knowledge, Sobol-SBSA has enabled the first direct measurement of two quantities. The importance of interactions between semantically relevant features and the relative importance between segment objects and background for CNN outputs. The work of which the authors are aware, indirectly quantify the importance of segmented and background regions based on noise applied to these regions (Singla et al., 2022) or quantify the interactions of CNNs exclusively at the image patch level (Brendel & Bethge, 2019)

4.2.2 Why are Adversarialy Robust CNNs Resistant to Spurious Features?

In this section, we explore the mechanism by which Adversarialy robust CNNs are less susceptible to spurious correlations in the data. To do this, we apply Sobol-SBSA to robust versions of VGG16_BN, ResNet50, and DenseNet161 and compare their PIR and difference in the segmentation and background importance to their standard versions. We use pre-trained robust weights from Salman et al. (2020) where the l_2 threat radius was 3. In this case, we

Figure 5a shows the PIR for the normal and robust versions of VGG16_BN, ResNet50, and DenseNet161. We see that when the segmented regions of interest are areas of the image that contain relevant objects to classification, but that do not strictly respect boundaries the impact of Robust models is to greatly decrease the interaction between core and background areas for all models. This is not the case for segmentations defined by ImageNet-S, which strictly respect object boundaries. We see that the robust versions of VGG16_BN and ResNet50 do not greatly impact the extent to which these models rely on interactions between objects and the background, though the robust version of DenseNet161 does. Figure 5b show the average difference in importance between segmented objects and the background for 10000 images in the ImageNet-S and Salient ImageNet datasets. We see that for all models, and both forms of segmentation, the robust version of these CNN models placed larger relative importance on the segmented objects than their vanilla counterparts. Figure 6 shows an example of this trend.

We have shown through direct measurement that CNN models trained to be adversarially robust are resistant to exploiting spurious correlations in the data both because they reduce the extent to which models rely on image backgrounds, and because they reduce the extent to which models rely on interactions between core and background regions of an image.



(a) The plots of the average mean of PIR when Sobol-SBSA is applied to segmented and background objects in SalientImageNet and ImageNet-S for normal an robust models. 10000 images were used in their respective datasets.

(b) The plots of the average difference in importance, S_T, for segmented objects in ImageNet-S and Salient ImageNet when applied to normal and robust models. 10000 images from each dataset were used.

Figure 5: PIR trends and the difference in importance between segmented objects and background for CNN models

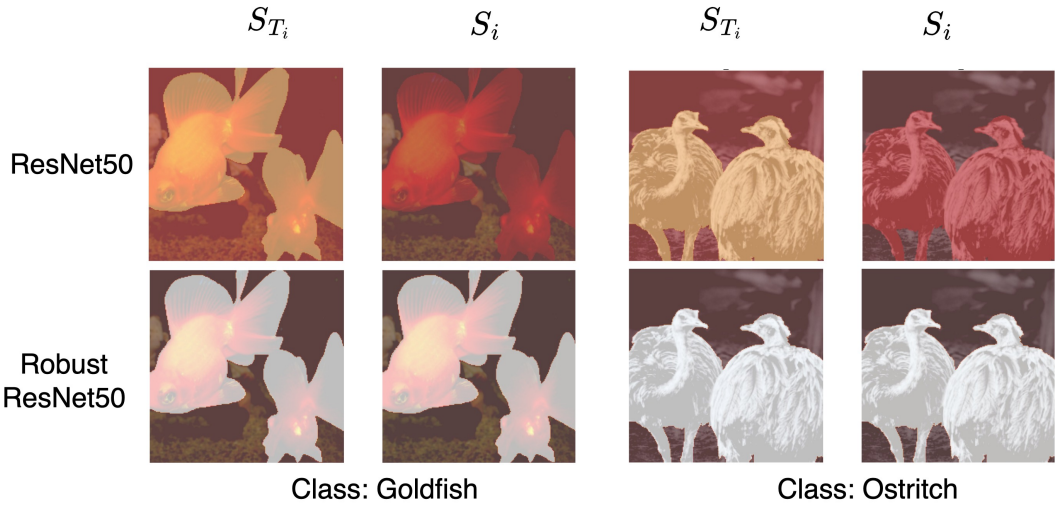


Figure 6: A sample result of the Sobol-SBSA when applied to an segmentations determined by the ImageNet-S dataset for the normal and robust versions of ResNet50. We see that the normal version of ResNet50 gives substantial importance to the background when classifying these images, but the Robust ResNet50 focuses only on the segmented objects.

4.2.3 The Limit of Sobol-SBSA

While the Sobol-SBSA is a powerful method, it has a similar weakness to other sample-based black box methods. It assumes that the input features that it is analyzing are uncorrelated. When this is not the case, the ability of Sobol to decompose importance into independent subsets of the feature space is weakened (Li et al., 2010). This manifests itself in the Sobol Indices, which are supposed to satisfy the property that PIR ≤ 1, having at least some input features for which PIR > 1.

In the case of regions, the assumption of uncorrelated input features breaks down as regions become smaller in size since the regions will tend more to belong to the same object on an image (the wing of a bird). We observe this in two ways. First, we examine figure 4a and note that PIR increases as the region sizes increase as region size decreases. This is intuitively an incorrect result since interactive effects should be greater for smaller regions, as demonstrated by Brendel & Bethge (2019). To

confirm that this result is due to a breakdown in Sobol assumptions we calculate the average percent of regions for which PIR > 1 across all models for a given region size. For 4×4, 8×8, and 14×14 regions the percent of regions for which PIR > 1 are 22%, 33%, and 39% respectively. The key takeaway here is that *Sobol-SBSA is should be used to compare how models use identically correlated features*. A key direction for future work is to implement a version of Sobol-SBSA that accounts for correlations in the data.

5 Discussion and Conclusion

We proposed Sobol-SBSA, a general method for understanding how Deep Learning Models use semantic features when making decisions. We demonstrated the ability of this method to answer richer questions about models by applying it to how CNN models use regions of ImageNet models. We found (1) that the primary impact of the evolution of CNN models was to make greater use of region interactions and to increase the importance of image background to model predictions, and (2) that adversarially robust CNN models are less susceptible to spurious correlations in the data because they force CNN architectures to rely less on region interactions and on image backgrounds.

The Sobol-SBSA method has a variety of potential applications beyond the image/region-based analysis that we presented here. Many different types of input partitioning and input modalities can be analyzed using the SBSA method. For images, the partitioning into image regions can be done via external metadata, such as object detection results. For natural language processing (NLP), the use of SBSA is even more straightforward since words/tokens provide a natural way to partition the input sequence. Hence, our model can be utilized to understand how parts of speech are utilized for different iterations of various NLP models, including translation, classification, and generative text models. Beyond unimodal content, SBSA can also be easily extended to multimodal setups. For example, Sobol-SBSA can be used to measure the strength of bias in Image Captioning systems by quantifying the extent to which parts of an image correspond to which parts of the generated caption. In addition to these applications, there are multiple avenues for future work. These include exploring the combination of Sobol-SBSA with automatic feature detectors, implementing a version of Sobol-SBSA that accounts for input correlations, and exploring whether PIR can be used as a proxy for the robustness of non-CNN Deep Learning models.

Through SBSA and Sobol-SBSA we have proposed a strong foundation for obtaining a richer understanding of how models use semantic representations of inputs, regardless of whether these representations are generated automatically or by end users. We hope that it can be used to both provide clarity about the mechanisms by which Deep Learning makes decisions, and to influence how we further develop these models.

References

Marco Ancona, Enea Ceolini, A. Cengiz Öztireli, and Markus H. Gross. A unified view of gradient-based attribution methods for deep neural networks. *CoRR*, abs/1711.06104, 2017. URL `http://arxiv.org/abs/1711.06104`.

Wieland Brendel and Matthias Bethge. Approximating cnns with bag-of-local-features models works surprisingly well on imagenet. volume 7, 2019.

Aditya Chattopadhay, Anirban Sarkar, Prantik Howlader, and Vineeth N Balasubramanian. Grad-cam++: Generalized gradient-based visual explanations for deep convolutional networks. In *2018 IEEE winter conference on applications of computer vision (WACV)*, pp. 839–847. IEEE, 2018.

Thomas Fel, Rémi Cadène, Mathieu Chalvidal, Matthieu Cord, David Vigouroux, and Thomas Serre. Look at the variance! efficient black-box explanations with sobol-based sensitivity analysis. *CoRR*, abs/2111.04138, 2021. URL `https://arxiv.org/abs/2111.04138`.

Shanghua Gao, Zhong-Yu Li, Ming-Hsuan Yang, Ming-Ming Cheng, Junwei Han, and Philip H. S. Torr. Large-scale unsupervised semantic segmentation. *CoRR*, abs/2106.03149, 2021. URL `https://arxiv.org/abs/2106.03149`.

Jon Herman and Will Usher. Salib: An open-source python library for sensitivity analysis. *Journal of Open Source Software*, 2, 2017. URL `https://doi.org/10.21105/joss.00097`.

Joseph D. Janizek, Pascal Sturmfels, and Su-In Lee. Explaining explanations: Axiomatic feature interactions for deep networks. *CoRR*, abs/2002.04138, 2020. URL https://arxiv.org/abs/2002.04138.

I. Kononenko, E. Štrumbelj, Z. Bosnic, Darko Pevec, M. Kukar, and M. Robnik-Sikonja. Explanation and reliability of individual predictions. *Informatica*, 37, 2013.

Genyuan Li, Herschel Rabitz, Paul E. Yelvington, Oluwayemisi O. Oluwole, Fred Bacon, Charles E. Kolb, and Jacqueline Schoendorf. Global sensitivity analysis for systems with independent and/or correlated inputs. *The Journal of Physical Chemistry A*, 114, 2010. URL https://doi.org/10.1021/jp9096919.

Ying Li, Lingfei Ma, Zilong Zhong, Fei Liu, Michael A. Chapman, Dongpu Cao, and Jonathan Li. Deep learning for lidar point clouds in autonomous driving: A review. *IEEE Transactions on Neural Networks and Learning Systems*, 32, 2021.

Vitali Petsiuk, Abir Das, and Kate Saenko. Rise: Randomized input sampling for explanation of black-box models, 2018. URL https://arxiv.org/abs/1806.07421.

Marco Túlio Ribeiro, Sameer Singh, and Carlos Guestrin. "why should I trust you?": Explaining the predictions of any classifier. *CoRR*, abs/1602.04938, 2016. URL http://arxiv.org/abs/1602.04938.

Hadi Salman, Andrew Ilyas, Logan Engstrom, Ashish Kapoor, and Aleksander Madry. Do adversarially robust imagenet models transfer better? In *ArXiv preprint arXiv:2007.08489*, 2020.

Andrea Saltelli, Paola Annoni, Ivano Azzini, Francesca Campolongo, Marco Ratto, and Stefano Tarantola. Variance based sensitivity analysis of model output. design and estimator for the total sensitivity index. *Computer Physics Communications*, 181, 2010. URL https://doi.org/10.1016/j.cpc.2009.09.018.

Manuel Schultheiss, Sebastian Schober A., Marie Lodde, Jannis Bodden, Juliane Aichele, Christina Müller-Leisse, Bernhard Renger, Franz Pfeiffer, and Daniela Pfeiffer. A robust convolutional neural network for lung nodule detection in the presence of foreign bodies. *Scientific Reports*, 32, 2021.

Ramprasaath R Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *Proceedings of the IEEE international conference on computer vision*, pp. 618–626, 2017.

Sahil Singla and Soheil Feizi. Causal imagenet: How to discover spurious features in deep learning? *CoRR*, abs/2110.04301, 2021. URL https://arxiv.org/abs/2110.04301.

Sahil Singla, Mazda Moayeri, and Soheil Feizi. Core risk minimization using salient imagenet, 2022. URL https://arxiv.org/abs/2203.15566.

Mukund Sundararajan, Ankur Taly, and Qiqi Yan. Axiomatic attribution for deep networks. *International Conference on Machine Learning*, 34, 2017.

Hao Zhang, Yichen Xie, Longjie Zheng, Die Zhang, and Quanshi Zhang. Interpreting multivariate interactions in dnns. *CoRR*, abs/2010.05045, 2020. URL https://arxiv.org/abs/2010.05045.

A APPENDIX

A.1 10K VS 50K EXPERIMENTS

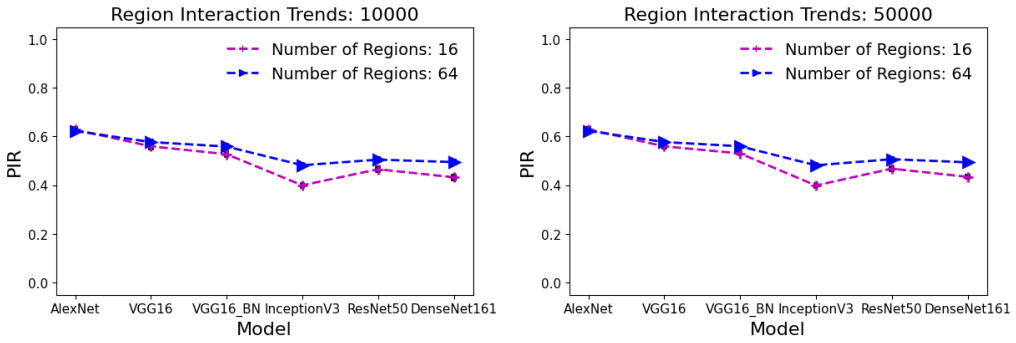


Figure 7: Average PIR for the top 20% of regions when calculated for 10000 and 50000 ImageNet validation images. This is done for 4×4 and 8×8 regions. The results are identical.

We calculated the average PIR for the top 20% of regions for 10000 and 50000 validation images in ImageNet using 4×4 and 8×8 regions respectively. We saw that the results were identical so, for the smaller regions generated when splitting an image into 14×14 regions, we calculated the average PIR for 10000 images to save computational cost.

A.2 RESNET50 VS ROBUST RESNET50 EXAMPLES

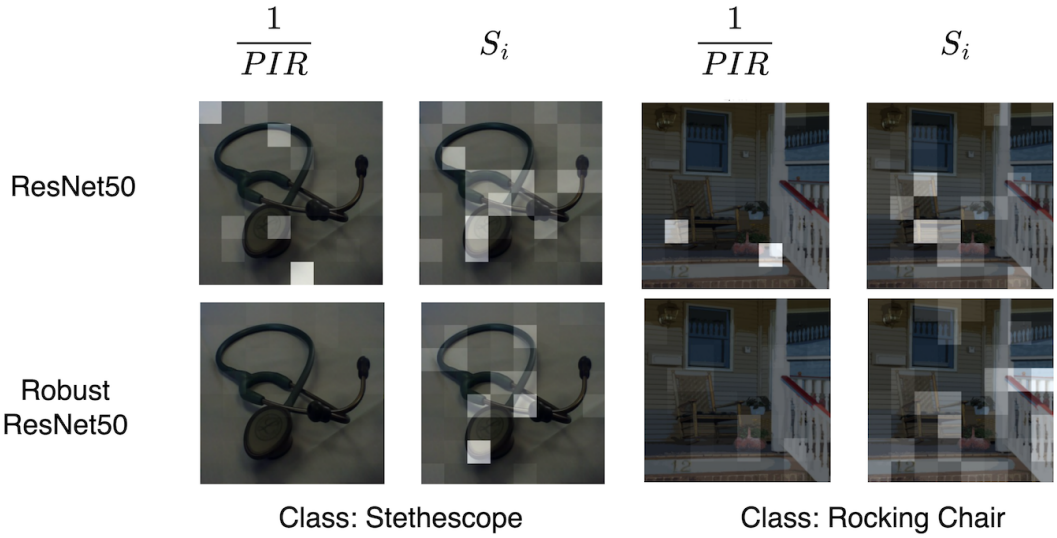


Figure 8: The result of Sobol-SBSA $\frac{1}{\text{PIR}}$ and S_i when applied to a validation images for ResNet50 and RobustResNet50. From $\frac{1}{\text{PIR}}$, we see that ResNet50 exploits interactions with background spurious correlations, white surface background for the *Stethescope* class, and porch background for the *Rocking Chair* class to a much greater degree compared to RobustResNet50. However, both models highlight similar regions of primary importance, as seen from S_i.

Figure 8 shows additional examples of images where both ResNet50 and the Robust ResNet50 looked at similar parts of the image as being of primary importance, S_i, but ResNet50 had stronger interactions with the background of the images which it exploited in making predictions. In this case, ResNet50 interacted with the white background when classifying a stethoscope and the porch when classifying a rocking chair.