

Benchmarking Attribution Methods with Relative Feature Importance

Mengjiao Yang
Google Brain
sherryy@google.com

Been Kim
Google Brain
beenkim@google.com

Abstract

Interpretability is an important area of research for safe deployment of machine learning systems. One particular type of interpretability method attributes model decisions to input features. Despite active development, quantitative evaluation of feature attribution methods remains difficult due to the lack of ground truth: we do not know which input features are in fact important to a model. In this work, we propose a framework for Benchmarking Attribution Methods (BAM) with a priori knowledge of *relative* feature importance. BAM includes 1) a carefully crafted dataset and models trained with known relative feature importance and 2) three complementary metrics to quantitatively evaluate attribution methods by comparing feature attributions between pairs of models and pairs of inputs. Our evaluation on several widely-used attribution methods suggests that certain methods are more likely to produce false positive explanations—features that are incorrectly attributed as more important to model prediction. We open source our dataset, models, and metrics.

1 Introduction

The output of machine learning interpretability methods is often assessed by humans to see if one can understand it. While there is much value in this exercise, qualitative assessment alone can be vulnerable to bias and subjectivity as pointed out in Adebayo et al. (2018); Kim et al. (2018). Just because an explanation makes sense to humans does not mean that it is correct. For

instance, edges of an object in an image could be visually appealing but have nothing to do with prediction. Assessment metrics of interpretability methods should capture any mismatch between interpretation and a model’s rationale behind prediction.

Adebayo et al. (2018) explores when certain saliency maps (a type of attribution-based explanation) fail to reflect true feature importance. Specifically, they found that certain attribution methods present visually identical explanations when a trained model’s parameters are randomized (and hence features are made irrelevant to prediction). This suggests that attribution methods are making mistakes, perhaps by assigning high attributions to unimportant features (false positives) and low attributions to important features (false negatives). In this work, we focus on studying the false positive set of mistakes.

One way to test false positives is to identify unimportant features and expect their attributions to be zero. In reality, we do not know the *absolute* feature importance (exactly how important each feature is). We can, however, control the *relative* feature importance (how important a feature is to a model relative to another model) by changing the frequency certain features occur in the dataset. In this work, we propose a framework for Benchmarking Attribution Methods (BAM), which includes 1) a semi-natural dataset and models trained with known relative feature importance (Figure 1) and 2) three metrics for quantitatively evaluating attribution methods. Given relative feature importance from our dataset, our metrics compare attributions between pairs of models (*model dependence*) and pairs of inputs (*input dependence* and *input independence*). Our evaluation of six feature-based and one concept-based attribution methods suggests that certain methods are more likely to produce false positive explanations by assigning higher attributions to less important features. We additionally show that the rankings of attribution methods differ under different metrics; hence, whether a method is good depends on the final task and its metric of choice.

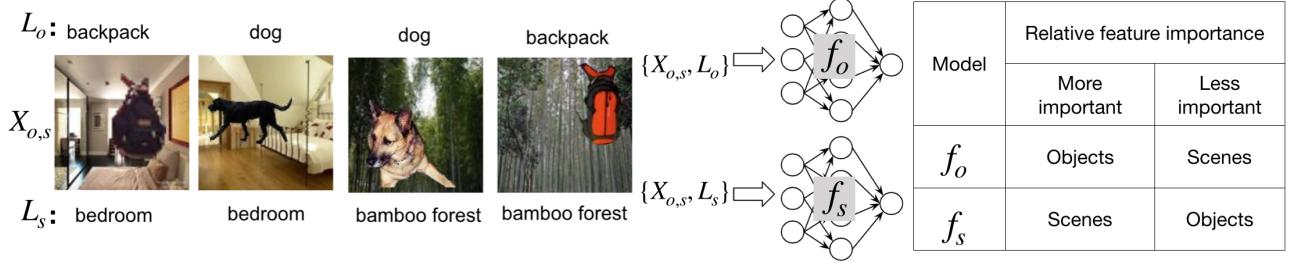


Figure 1: **BAM dataset examples and BAM models.** The object neural network (f_o) is trained with object labels (L_o) and the scene neural network (f_s) is trained with scene labels (L_s).

2 Related work

Prior work on evaluating attribution methods generally falls into four categories: 1) measuring (in)sensitivity of explanations to model and input perturbations, 2) inferring correctness of explanation from accuracy drop upon feature removal, 3) evaluating explanations in a controlled setting with some knowledge of feature importance, and 4) evaluating explanations based on human visual assessment. Our work shares characteristics with the first three: with the knowledge of relative feature importance, we measure when and how attributions should or should not change given models or inputs changing in a controlled way. Different from 4), we only focus on evaluating correctness of attributions, not on how humans understand explanations; our correctness test is a pre-check to more expensive human-in-the-loop evaluations.

Evaluating sensitivity of explanations. This set of work measures how much interpretations change when models (Heo et al., 2019; Adebayo et al., 2018) or inputs (Ghorbani et al., 2018; Alvarez-Melis and Jaakkola, 2018) change. Adebayo et al. (2018) randomized model parameters so that features relevant to the original model are irrelevant to the randomized model. We instead train two models with different labels so that some features are more important to one model than the other. One of our metrics also measures a notion of robustness in explanations (i.e., when attributions should stay invariant) similar to Alvarez-Melis and Jaakkola (2018) and Ghorbani et al. (2018). Our input perturbation, however, is semantically meaningful (e.g., adding a dog to an image). Semantically meaningful perturbations are well-suited for testing attribution methods because they can mislead humans if attributed incorrectly.

Evaluating correctness of explanations. Samek et al. (2017) and its subsequent variations (Fong and Vedaldi, 2017; Ancona et al., 2018; Hooker et al., 2018) remove highly attributed input features and measure the resulting performance degradation. Without re-

training the model, the modified inputs may fall outside of the training data manifold. As a result, it is hard to decouple whether the accuracy drop is due to out-of-distribution data or due to good feature attributions. Retraining, on the other hand, results in a model different from the original one being explained. We enable method evaluation on the original model using in-distribution inputs.

Evaluating with knowledge of feature importance. Most relevant to our work is the controlled experiment in Kim et al. (2018), where the authors created a simple dataset and trained models such that important pixels are known. While Kim et al. (2018) compared their method to saliency maps, no quantitative metrics were given; their results were qualitatively evaluated by human subjects. Our work develops quantitative metrics in a finer-grained setting with semi-natural images.

Evaluating with humans in the loop. This approach either asks humans to use interpretability methods to perform a task or evaluates how often humans can correctly predict model behavior after seeing the explanations (Lakkaraju et al., 2016; Ribeiro et al., 2016; Doshi-Velez and Kim, 2017; Lage et al., 2018; Narayanan et al., 2018; Poursabzi-Sangdeh et al., 2018). Our work is not meant to replace but to complement human-in-the-loop evaluations. We provide an efficient pre-check to make sure that methods correctly assign lower attributions to less important features before involving humans in the evaluation loop.

3 BAM dataset and models

Our goal is to evaluate correctness of feature attributions with respect to their relative importance. For instance, if we paste a gray square to every training image for all classes, we expect this square to matter less to model predictions than the original image region being covered. The same expectation should hold if we instead paste a dog to every image (given that the original images do not contain anything similar to

	f_o		f_s		
	Test set	Test acc.	Test set	Test acc.	
Removing CF	$X_{o,s}$	91.1%	$X_{o,s}$	94.0%	Maintained
	$X_{o,g}$	93.1%	$X_{\emptyset,s}$	95.5%	accu
	% increased in confidence	86.7%		79.5%	$X_{o,g}$
Only keeping CF	$X_{\emptyset,s}$	9.7%	$X_{o,g}$	9.8%	Random

	$X_{o,s}^{0.1}$	$X_{o,s}^{0.2}$	$X_{o,s}^{0.3}$	$X_{o,s}^{0.4}$	$X_{o,s}^{0.5}$	$X_{o,s}^{0.6}$	$X_{o,s}^{0.7}$	$X_{o,s}^{0.8}$	$X_{o,s}^{0.9}$	$X_{o,s}^{1.0}$
Test accuracy in $X_{o,s}$	97%	98%	96%	95%	96%	95%	92%	93%	92%	95%
Test accuracy in $X_{\emptyset,s}$	78%	77%	81%	75%	78%	81%	93%	93%	93%	93%

Figure 2: [Top] Verifying relative feature importance between f_o and f_s . Objects are more important to f_o than they are to f_s . Scenes are more important to f_s than to f_o . [Bottom] Test accuracy of bamboo forest with and without dog CF on models trained with $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 1.0\}$.

dogs). As a result, any explanations that assign higher attributions to dogs than to original pixels covered by dogs are false positives. False positive attributions of dogs have a higher chance of misleading humans because dogs are semantically meaningful.

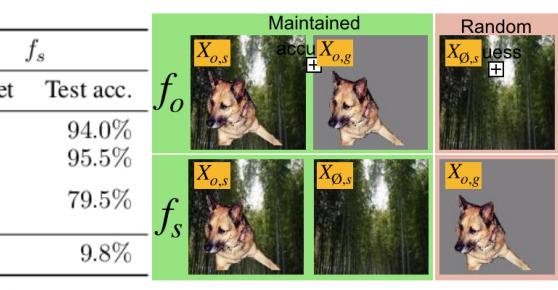
Based on this idea, we propose the BAM framework which includes 1) the BAM dataset and BAM models trained with known relative feature importance and 2) BAM metrics that quantitatively evaluate attribution methods (with and without BAM models). In this section, we describe the dataset and models, which are open sourced at <https://github.com/anonymous>.

3.1 BAM dataset construction

We construct the BAM dataset by pasting object pixels from MSCOCO (Lin et al., 2014) into scene images from MiniPlaces (Zhou et al., 2017), as shown in Figure 1. An object is rescaled to between $1/3$ to $1/2$ of a scene image and is pasted at a randomly chosen location. Each resulting image has an object label (L_o) and a scene label (L_s). Either can be used to train a classifier. BAM dataset has 10 object classes (e.g., backpack, bird, and dog) and 10 scene classes (e.g., bamboo forest, bedroom, and corn field). Every object class appears in every scene class and vice versa. There is a total of $100k$ images ($1k$ images per object-scene class pair). Scene images that originally contain objects from BAM’s object categories are filtered (e.g., no scenes originally have dogs). We denote this set as $X_{o,s}$.

3.2 Common feature (CF) and commonality

We define common feature (CF) as a set of pixels with some semantic meaning (e.g., looks like a dog) that commonly appear in all examples of one or more classes.



The ratio between the number of classes a CF appears in and the total number of classes is the commonality (k) of that CF. For example, a dog CF where dog pixels appear in all images of bamboo forest ($k = 0.1$) is less common than another dog CF where dog pixels appear in all images of bamboo forest, bedroom, and corn field ($k = 0.3$). We denote $X_{o,s}^k$ as a set of inputs where k percent scene classes have a particular CF. We create 10 such sets, $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 1.0\}$, using dog pixels as CF. Each set has $10k$ images with scene labels.

3.3 Relative importance of BAM models

We consider two scenarios where feature importance between models differ: 1) two classifiers trained on different labels (L_o and L_s), and 2) a set of scene classifiers trained with dog CF of different k values.

Training two classifiers with coarse-grained CF. We first train two classifiers using $X_{o,s}$. f_s is the classifier trained with scene labels L_s , and f_o is the classifier trained with object labels L_o . As a result, objects are considered coarse-grained CF (with $k = 1.0$) to f_s . Intuitively, objects should be significantly more important to f_o where they are targets of classification than to f_s where they are CF. To verify this intuition, we remove object pixels from $X_{o,s}$ while leaving the original scenes intact (denoted as $X_{\emptyset,s}$). The accuracy of f_o drops to a random guess, but the accuracy of f_s does not drop at all, as shown in Figure 2. Similarly, when we remove scenes from $X_{o,s}$ by filling background with gray pixels (denoted as $X_{o,g}$), the accuracy of f_s drops to a random guess but the accuracy of f_o does not drop. Knowing that objects are significantly more important to f_o than to f_s , we can test whether methods assign noticeably higher attributions to objects in f_o than in

f_s .

Training scene classifiers with fine-grained CFs. We enable a finer-grained control over relative feature importance between models by training classifiers on sets of inputs whose CFs differ in commonality k . In particular, we train 10 scene classifiers on $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 1.0\}$ with dog CF. By changing k , we can control dog CF’s relative importance to the model. Intuitively, dog CF with a lower k is more important to prediction than dog CF with a higher k . We verify this intuition by removing dog CF and measuring the accuracy drop of bamboo forest (the randomly chosen class that always has dog CF during training for different k). As shown in Figure 2 (bottom), the accuracy drop generally decreases as k increases. This indicates that the relative importance of dog CF also decreases as k increases. With dog CF’s relative importance, we can evaluate methods by comparing CF attributions across the set of models: a method should assign a higher attribution to the CF that is less common.

3.4 Relative importance of BAM inputs

After training f_s on $X_{o,s}$ using L_s , we observe in Figure 2 that the test accuracy of f_s is higher on $X_{\emptyset,s}$ than on $X_{o,s}$ (higher accuracy when object CF is removed). This implies that object CF is less important to f_s than the original scene pixels they cover. In addition, we measure the difference in classification confidence when object CF is removed from the input. As shown in Figure 2, the majority (86.7%) of the correctly classified inputs have increased classification confidence (in the rest classification confidence roughly stays the same). With relative importance between inputs with and without CF, we can test if methods assign lower attributions to object CF than the scene pixels being covered.

So far we have considered when feature importance between inputs are different. We can create another scenario (without requiring the BAM dataset or BAM models) where feature importance between inputs are similar. This allows us to test if methods assign similar attributions to inputs whose features have similar importance.

4 Metrics with/without BAM dataset

We propose three complementary metrics to evaluate attribution methods: model contrast score (*MCS*), input dependence rate (*IDR*), and input independence rate (*IIR*). These metrics measure the difference in attributions between two models given the same input (*MCS*), between two different inputs to the same model (*IDR*), and between two functionally similar inputs (*IIR*). The measurements can then be compared against the rel-

ative feature importance between models and inputs established in Section 3. *MCS* and *IDR* require the BAM dataset and BAM models, whereas *IIR* applies to *any* model given *any* inputs. Our metrics are by no means exhaustive—they only focus on false positive explanations, but they demonstrate how differences in attributions can be used for method evaluation, enabling development of additional metrics. BAM metrics are cheap to evaluate and therefore can serve as a pre-check before conducting expensive human-in-the-loop evaluations.

4.1 Setup

First, we define a way to compute the average attribution that a saliency method assigns to an image region. Taking the average is acceptable because we only care about *relative* feature importance. We denote $e \in \mathbb{R}^d$ as a saliency map whose values are normalized to $[0, 1]$, and $I_c \in \mathbb{R}^d$ as a binary mask where pixels inside a region c have a value of 1, and 0 everywhere else. Given an input image $x \in \mathbb{R}^d$ and a model $f : \mathbb{R}^d \mapsto \mathbb{R}^m$, we define $g_c \in \mathbb{R}$ as the average attribution of pixels in region c , namely

$$g_c(f, x) = \frac{1}{\sum I_c} \sum e(f, x) \odot I_c.$$

We further define concept attribution, $G_c \in \mathbb{R}$, as the average of g_c over a set of correctly classified inputs (X_{corr}), where region c represents some human-friendly concept (e.g., objects) in each input:

$$G_c(f, X) = \frac{1}{|X_{corr}|} \sum_{x \in X_{corr}} g_c(f, x).$$

We only consider correctly classified inputs so that classifiers’ mistakes are not propagated to attribution methods. Note that the above definition of G_c is only needed for feature-based explanations but not for concept-based explanations that compute their own G_c such as TCAV (Kim et al., 2018). Our metrics also apply to these methods as long as they provide a G_c value between $[0, 1]$. Now we define our three metrics.

4.2 Model contrast score (*MCS*)

Once we have a CF that appears in every class, one option is to directly compare G_c values of that CF across methods, and expect G_c to be small. However, there is a catch: a meaningless e that always assigns 0 (unimportant) to all features would seem to perform well. Even without such a bogus e , two attribution methods may operate on two different scales, so directly comparing G_c could be unfair.

Section 3.3 introduced relative feature importance between models—some input features are more important

to one model than to another model. For example, dog pixels more important to f_o than to f_s . We define model contrast score (MCS) as the difference in concept attributions between a model that considers a concept more important (f_1) than another model (f_2):

$$MCS = G_c(f_1, X_{corr}) - G_c(f_2, X_{corr}).$$

We expect MCS to be the largest when $f_1 = f_o$, $f_2 = f_s$, $X_{corr} \subset X_{o,s}$, and c corresponds to objects in the BAM dataset. This measures how differently objects are attributed between f_o and f_s — between when they are targets of classification (more important) and when they are CF (hence less important). We also compute a series of MCS scores by training f_1 using one of $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 0.9\}$, and f_2 using $X_{o,s}^{1.0}$. This gives us a spectrum of contrast scores where the dog CF is important to a different degree.

4.3 Input dependence rate (IDR)

While MCS compares attributions between models, one may also be interested in how a method performs on a single model. Section 3.4 introduced relative feature importance between inputs—a CF (with $k = 1.0$) is less important to a model (trained with that CF) than regions covered by that CF. Based on this knowledge, we can compare attributions of two inputs with and without CF, and expect g_c of the CF region to be smaller when CF is present. We define input dependence rate (IDR) as the percentage of correctly classified inputs where CF is attributed less than the original regions covered by CF. Formally,

$$IDR = \frac{1}{|X_{cf}|} \sum_{(x_{cf}, x_{-cf}) \in (X_{cf}, X_{-cf})} \mathbb{1}(g_c(f, x_{cf}) < g_c(f, x_{-cf})),$$

where x_{cf} and x_{-cf} are inputs with and without CF. Since we only require c to be an input region, we can still compute g_c of that region even if CF is absent. In the BAM framework, we have $X_{cf} = X_{o,s}$, $X_{-cf} = X_{\emptyset,s}$, and $f = f_s$. A high IDR means that an attribution method is more likely to correctly attribute CF. Intuitively, $1 - IDR$ is the false positive rate: out of 100 inputs, how many of their explanations assign higher attributions to less important features, thereby misleading human interpretation.

4.4 Input independence rate (IIR)

While IDR considers two inputs that should be attributed differently, input independence rate (IIR) expects similar attributions between two inputs that lead to the same model output (logit scores for all classes). Given any model f and any input x , we propose an optimization-based approach to compute a set of connected pixels δ , such that $f(x) \approx f(x + \delta)$. Because

x and $x + \delta$ have similar outputs, we call x and $x + \delta$ functionally similar. This δ , in fact, can have a large norm due to the excessive invariance of neural networks found in Jacobsen et al. (2018); Engstrom et al. (2019). Specifically, we use gradient descent to optimize the following objective:

$$\arg \min_{\delta} \|f(x + \delta) - f(x)\|_2 - \eta_1 \|\delta\|_2 + \mathcal{R},$$

where $-\eta_1 \|\delta\|_2$ avoids the trivial solution of $\delta = 0$. \mathcal{R} is a regularization term that encourages δ to look natural (see details in Appendix). This optimization is applicable to any models where gradients are accessible. When δ aligns well with a human-friendly concept, a false positive explanation that highly attributes δ could be dangerously misleading, as the output is the same with or without δ . Hence, we initialize δ from pixels of a dog, and only modify those pixels within a small L_2 distance of initialization. Figure 9 shows an example post-optimization with δ still looking like a dog. For this particular example, we have $\|f(x + \delta) - f(x)\|_2 = 0.2$, which is magnitudes smaller than $\|f(x)\|_2 = 31.9$. We verify that such a δ exists for any given input.

Next, we compute g_c for pairs of x and $x + \delta$, where x is drawn from the original scene images ($X_{\emptyset,s}$). When δ is absent, g_c is computed over the region where δ would have been. We expect g_c to only change within a visually imperceptible threshold t , above which humans would notice the difference in attribution when δ is added. We define IIR as the percentage of images where the difference in g_c with and without δ is less than t :

$$IIR = \frac{1}{|X_{corr}|} \sum_{x \in X_{corr}} \mathbb{1}\left(\frac{|g_c(f, x + \delta) - g_c(f, x)|}{g_c(f, x)} < t\right).$$

Here f is trained on $X_{\emptyset,s}$, but it can be any model. Intuitively, $1 - IIR$ is the false positive rate: out of 100 inputs, how many of their explanations would draw attention to δ which has no functionality, thereby misleading human interpretation. We note that t depends on human subjects and is application specific.

5 Evaluation with/without BAM

With the BAM dataset and BAM models from Section 3 and BAM metrics from Section 4, we evaluate feature-based attribution methods including GradCAM (GC) (Selvaraju et al., 2016), Vanilla Gradient (VG) (Simonyan et al., 2013; Erhan et al., 2009; Baehrens et al., 2010), SmoothGrad (SG) (Smilkov et al., 2017), Integrated Gradient (IG) (Sundararajan et al., 2017), and Guided Backpropagation (GB) (Springenberg et al., 2014). We also consider Gradient x Input (GxI), as many methods use GxI to visualize attributions. Our saliency map visualization follows the same procedure

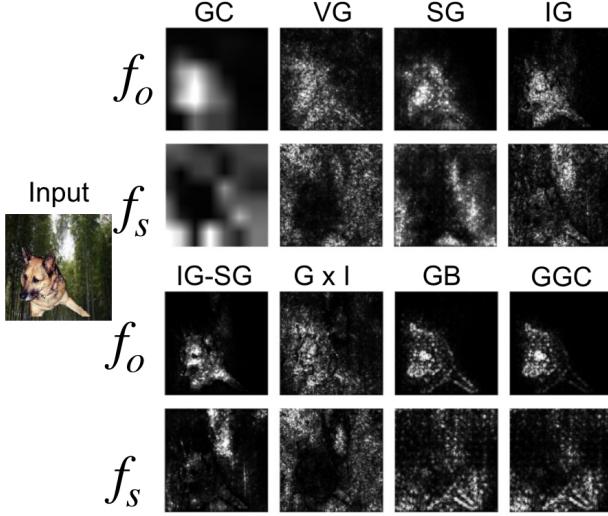


Figure 3: An example of saliency map visualizations for f_o and f_s . From qualitative examination alone, it is hard to rank method performance.

as Smilkov et al. (2017), except that we only use positive pixel attributions, as our work focuses on false *positives*. We also use *MCS* to evaluate a concept-based attribution method (TCAV).

In summary, our results suggest that 1) certain methods (such as GB) tend to assign similar attributions despite changes in underlying feature importance, 2) GC and VG are the least likely to produce false positive explanations, and 3) our metrics are indeed complementary—VG, for example, has high *IDR* and *IIR* but low *MCS*. Therefore, applications should choose attribution methods based on the metrics they care about the most (e.g., higher contrast between explanations, fewer false positive explanations, or robust explanations in the presence of functionless changes in the input).

5.1 Attributions between models with MCS

MCS offers two sets of evaluations—between two models trained using different labels and between a set of models trained with CFs of different commonality k . The rankings from the two sets of evaluations are similar: TCAV and GC have the best *MCS*, outperforming all the other methods.

***MCS* with coarse-grained CF.** One image from the BAM dataset and its saliency maps computed on f_o and f_s are shown in Figure 3. With qualitative examination alone, it is hard to see which method is better than others. We compute *MCS* between f_o and f_s over 10k images from $X_{o,s}$. The quantitative results are shown in Figure 4. TCAV has the highest *MCS*, immediately followed by GC. By applying smoothing to VG, SG improves *MCS*, outperforming the rest methods. We confirm that *MCS* is robust to the scale and

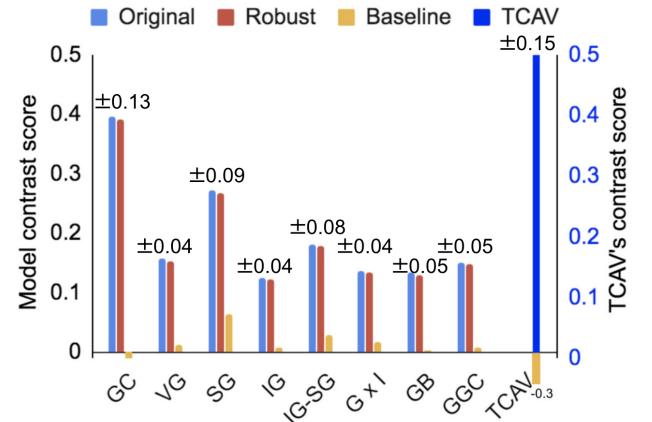


Figure 4: *MCS* between f_o and f_s . Blue bars are measurements from the original BAM dataset. Red bars show robustness of this measure. Yellow bars are baselines. Numbers on top are standard deviations. Higher *MCS* is better.

location of objects (red bars). The baseline (yellow bars) is calculated using random I_c . This means how much attributions of randomly chosen features differ between f_o and f_s (see details in Appendix). *MCS* for TCAV is computed by taking the difference in object TCAV scores between f_o and f_s .

***MCS* with fine-grained CFs** We also compute a series of *MCS* between a classifier trained on $X_{o,s}^{1,0}$ and a set of classifiers trained on $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 1.0\}$, as described in Section 3.3. As the commonality k of dog CF increases from left to right in Figure 6 (top), TCAV and GC closely follow the trend of accuracy drop upon CF removal (dashed black line). Visual assessment of GC in Figure 5 supports this observation: the first row shows that GC’s dog attribution decreases as k increases. All methods except TCAV and GC change at a much smaller scale. In particular, GB evolves minimally with the edges of the dog always being visible (second to last row of Figure 5), similar to the findings in Adebayo et al. (2018); Nie et al. (2018). Figure 6 (bottom) additionally shows the Pearson correlation coefficients between each method’s *MCS* and the accuracy drop upon CF removal. TCAV achieves the highest correlation closely followed by GC.

5.2 Attributions between inputs with IDR

Now we assess attribution difference between inputs to f_s with and without CF. From visualization alone (Figure 7), it is again hard to rank the saliency methods. The quantitative measurement of *IDR* in Figure 8 shows that GC and VG have the most correctly attributed CF—the least amount of false positive explanations. We note that VG is the original gradient method; many

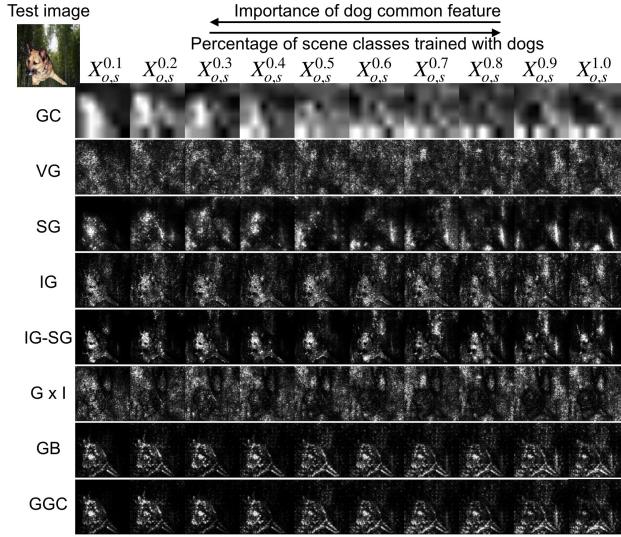


Figure 5: An example of saliency map visualizations for models trained with CFs of different k . k increases from left to right. A larger contrast among each row is better. (Full size figure in Appendix.)

other methods require additional steps after computing VG. This means that the cheapest method offers nearly the best performance (also suggested by Adebayo et al. (2018)). The baseline of IDR is around 50% (measured using random I_c). In applications where low false positive rate is critical, GC and VG are better choices than other methods. IDR is not applicable to TCAV, as TCAV is a global method.

5.3 Attributions between functionally similar inputs with IIR

Finally, we present the *IIR* results (which could have been measured on any model given any inputs). Most of the methods, with the exception of GC and VG, incorrectly assign much higher attributions to δ for over 80% of the examples (Figure 10). This alarming result is confirmed by visual assessments in Figure 9—the dog is clearly highlighted by IG, IG-SG, GB, and GGC. The finding that GB tends to highlight edges is consistent with Adebayo et al. (2018); Nie et al. (2018). Since δ is highly visible in the input image but does not affect prediction, attributions that directly depend on the input, such as GxI and IG, are likely to be affected by δ . This observation calls into question the common practice of multiplying explanations by the input image for visualization.

$t = 10\%$ is used as the threshold to compute *IIR* (Section 4.4). We visually determined that when g_c changes by more than 10%, we could clearly see the attribution difference of the δ region in some methods. The choice of t can be further calibrated by human subjects. As a reminder, *IIR* with $t = 10\%$ is the percentage of inputs

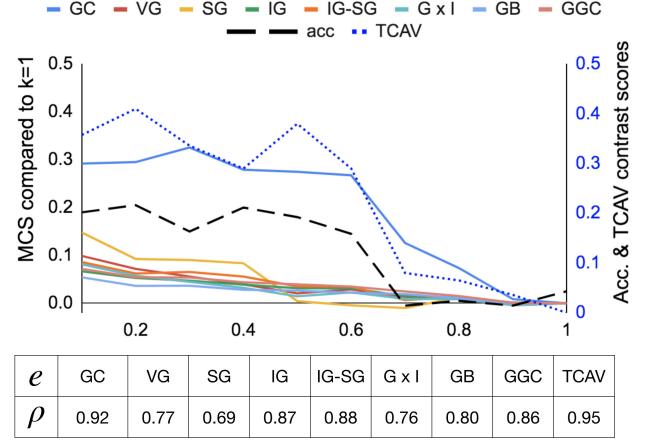


Figure 6: [Top] MCS between $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 1.0\}$ and $X_{o,s}^{1.0}$ as k increases. The dashed black line is the accuracy drop when CF is removed during testing. The dotted blue line is the series of MCS for TCAV. [Bottom] Pearson correlation coefficients (ρ) between each method’s MCS and the accuracy drop. A higher correlation is better.

where adding δ does not change the attribution of the region by more than 10%. We use $\eta_1 = 0.01$ when computing this δ , but the optimization is robust to the choice of η_1 . *IIR* is not applicable to TCAV, as TCAV is a global method.

6 Discussion

We evaluate methods based on how well difference in attributions aligns with relative feature importance. Perturbation-based evaluations, on the other hand, remove highly attributed features and infer method performance by the resulting accuracy drop. Below we discuss the differences between our approach and perturbation tests, and how our evaluation results might generalize to real datasets.

Assumptions about feature importance. Perturbation-based evaluations first run attribution methods on an input and rank features by the resulting attributions. A fixed percentage of highly ranked features are then removed, and method that leads to the highest accuracy drop is the best. Perturbation-based evaluations assume that there exist a unique set of important features whose removal would cause an accuracy drop. However, the set of important features may not be unique. The BAM framework, on the other hand, does not make assumptions about importance of individual features.

Computational efficiency. Perturbation tests are computationally expensive. For instance, the cost of retraining in Hooker et al. (2018) is linear to the number

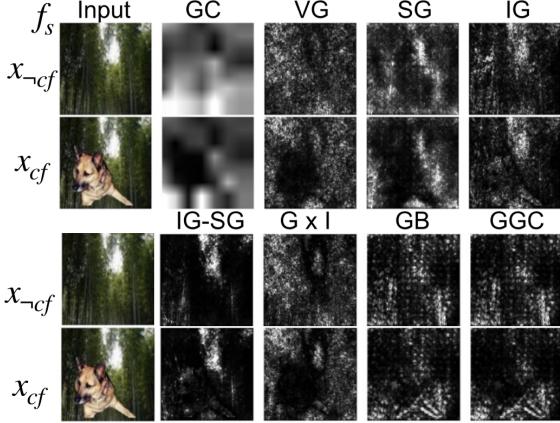


Figure 7: Saliency maps with and without CF on f_s . The dog CF is less important than the scene region being replaced.

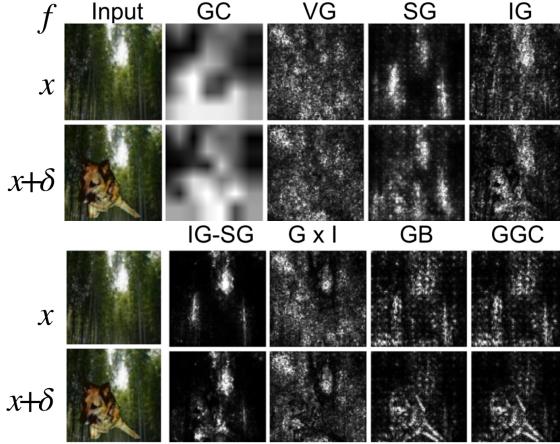


Figure 9: Saliency maps for x and $x + \delta$ on any f . x and $x + \delta$ are functionally similar.

of methods being examined. Tests that do not retrain the model after modifying the input such as Fong and Vedaldi (2017); Ancona et al. (2018); Hooker et al. (2018) still incurs a cost that is linear to the number of perturbation steps. Our test requires training a fixed number of models only once, and does not use small (and therefore costly) perturbation steps.

Do evaluation results on the BAM dataset generalize to real dataset? One might wonder how our evaluation results on the BAM dataset translates to natural images. While there is no guarantee that methods performing well on the BAM dataset will assign correct attributions to real images, BAM could be seen as a simpler and easier test to more complex scenarios. If an attribution method fails an easier test, it is also likely to fail harder tests. Furthermore, the metrics we evaluate, such as assigning lower attribution to less important features (hence avoiding false positives), reflect good properties of attribution methods

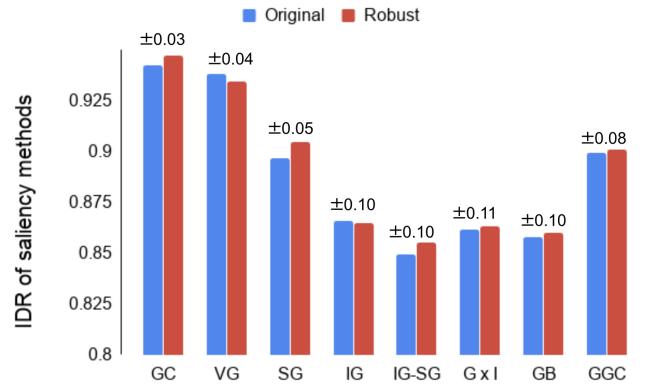


Figure 8: *IDR* results for $(X_{cf}, X_{\neg cf})$. Higher *IDR* is better. Red bars are robustness test of the metric. Numbers on top are standard deviations over 10 trials of 100 image pairs each. Baseline is 50%.

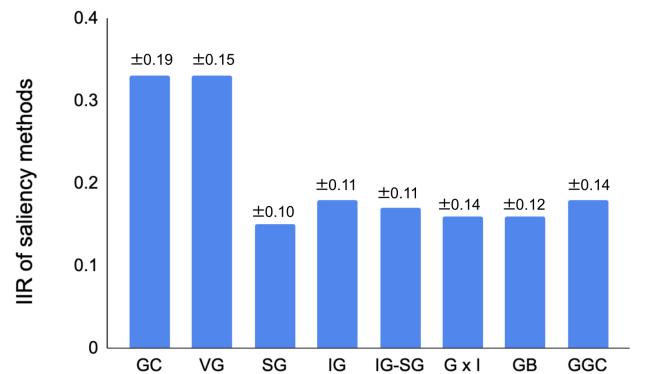


Figure 10: *IIR* results with $t = 10\%$. Higher *IIR* is better. Numbers on top are standard deviations over 10 trials of 100 image pairs each.

regardless of the underlying dataset.

7 Conclusions

There is little point in providing false explanations—evaluating explanations is as important as developing attribution methods. In this work, we take a step towards quantitative evaluation of attribution methods using relative feature importance between different models and inputs. We create and open source a semi-natural image dataset (BAM dataset), a set of models trained with known relative feature importance (BAM models), and three complementary metrics (BAM metrics) for evaluating attribution methods. Our work is only a starting point; one can also develop other measures of performance using our framework. We hope that developing ways to quantitatively evaluate attribution methods helps us choose the best metric and method for the application at hand.

References

- Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., et al. (2016). Tensorflow: A system for large-scale machine learning. In *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)*, pages 265–283.
- Adebayo, J., Gilmer, J., Muelly, M., Goodfellow, I. J., Hardt, M., and Kim, B. (2018). Sanity checks for saliency maps. In *NeurIPS*.
- Alvarez-Melis, D. and Jaakkola, T. S. (2018). Towards robust interpretability with self-explaining neural networks. In *NeurIPS*.
- Ancona, M. B., Ceolini, E., Oztireli, C., and Gross, M. H. (2018). Towards better understanding of gradient-based attribution methods for deep neural networks. In *ICLR*.
- Baehrens, D., Schroeter, T., Harmeling, S., Kawanabe, M., Hansen, K., and Müller, K.-R. (2010). How to explain individual classification decisions. *Journal of Machine Learning Research*, 11:1803–1831.
- Doshi-Velez, F. and Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*.
- Engstrom, L., Ilyas, A., Santurkar, S., Tsipras, D., Tran, B., and Madry, A. (2019). Learning perceptually-aligned representations via adversarial robustness. *arXiv preprint arXiv:1906.00945*.
- Erhan, D., Bengio, Y., Courville, A. C., and Vincent, P. (2009). Visualizing higher-layer features of a deep network.
- Fong, R. and Vedaldi, A. (2017). Interpretable explanations of black boxes by meaningful perturbation.
- Ghorbani, A., Abid, A., and Zou, J. Y. (2018). Interpretation of neural networks is fragile. *CoRR*, abs/1710.10547.
- He, K., Zhang, X., Ren, S., and Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778.
- Heo, J., Joo, S., and Moon, T. (2019). Fooling neural network interpretations via adversarial model manipulation. *arXiv preprint arXiv:1902.02041*.
- Hooker, S., Erhan, D., Kindermans, P., and Kim, B. (2018). Evaluating feature importance estimates. *CoRR*, abs/1806.10758.
- Jacobsen, J.-H., Behrmann, J., Zemel, R., and Bethge, M. (2018). Excessive invariance causes adversarial vulnerability. *arXiv preprint arXiv:1811.00401*.
- Kim, B., Wattenberg, M., Gilmer, J., Cai, C. J., Wexler, J., Viégas, F. B., and Sayres, R. (2018). Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (tcav). In *ICML*.
- Lage, I., Ross, A., Gershman, S. J., Kim, B., and Doshi-Velez, F. (2018). Human-in-the-loop interpretability prior. In *Advances in Neural Information Processing Systems*, pages 10159–10168.
- Lakkaraju, H., Bach, S. H., and Leskovec, J. (2016). Interpretable decision sets: A joint framework for description and prediction. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, pages 1675–1684. ACM.
- Lin, T., Maire, M., Belongie, S. J., Bourdev, L. D., Girshick, R. B., Hays, J., Perona, P., Ramanan, D., Dollár, P., and Zitnick, C. L. (2014). Microsoft COCO: common objects in context. *CoRR*, abs/1405.0312.
- Narayanan, M., Chen, E., He, J., Kim, B., Gershman, S., and Doshi-Velez, F. (2018). How do humans understand explanations from machine learning systems? an evaluation of the human-interpretability of explanation. *arXiv preprint arXiv:1802.00682*.
- Nie, W., Zhang, Y., and Patel, A. (2018). A theoretical explanation for perplexing behaviors of backpropagation-based visualizations. In *ICML*.
- Poursabzi-Sangdeh, F., Goldstein, D. G., Hofman, J. M., Vaughan, J. W., and Wallach, H. (2018). Manipulating and measuring model interpretability. *arXiv preprint arXiv:1802.07810*.
- Ribeiro, M. T., Singh, S., and Guestrin, C. (2016). Why should i trust you?: Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, pages 1135–1144. ACM.
- Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Bernstein, M. S., Fei-Fei, L., Berg, A. C., and Khosla, A. (2015). Imagenet large scale visual recognition challenge. *Springer US*.
- Samek, W., Binder, A., Montavon, G., Lapuschkin, S., and Müller, K.-R. (2017). Evaluating the visualization of what a deep neural network has learned. *IEEE Transactions on Neural Networks and Learning Systems*, 28:2660–2673.
- Selvaraju, R. R., Das, A., Vedantam, R., Cogswell, M., Parikh, D., and Batra, D. (2016). Grad-cam: Why did you say that? *CoRR*, abs/1611.07450.
- Simonyan, K., Vedaldi, A., and Zisserman, A. (2013). Deep inside convolutional networks: Visualising image classification models and saliency maps. *CoRR*, abs/1312.6034.

- Smilkov, D., Thorat, N., Kim, B., Viégas, F. B., and Wattenberg, M. (2017). Smoothgrad: removing noise by adding noise. *CoRR*, abs/1706.03825.
- Springenberg, J. T., Dosovitskiy, A., Brox, T., and Riedmiller, M. (2014). Striving for simplicity: The all convolutional net. *arXiv preprint arXiv:1412.6806*.
- Sundararajan, M., Taly, A., and Yan, Q. (2017). Ax- iomatic attribution for deep networks. In *ICML*.
- Zeiler, M. D. and Fergus, R. (2014). Visualizing and understanding convolutional networks. In *Euro- pean conference on computer vision*, pages 818–833. Springer.
- Zhou, B., Lapedriza, A., Khosla, A., Oliva, A., and Torralba, A. (2017). Places: A 10 million image database for scene recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.

Appendix

A Details in creating δ for input independence

The additional regularization terms in the loss function for creating δ for input independence test is as follows:

$$\mathcal{R} = \eta_2 [(x + \delta - p_h)^+ + (p_l - x - \delta)^+] + \eta_3 \sum \delta \odot (J - I_c)$$

$\eta_2 [(x + \delta - p_h)^+ + (p_l - x - \delta)^+]$ penalizes pixel values in $x + \delta$ that fall outside the valid pixel range $[p_l, p_h]$ (e.g., $[0, 255]$). The additional term $\eta_3 \sum \delta \odot (J - I_c)$ minimizes updates to regions outside of the δ region represented by mask I_c (J is a matrix of ones). The overall loss function is:

$$L = \|f(x + \delta) - f(x)\|_2 - \eta_1 \|\delta\|_2 + \mathcal{R}$$

The update rule for δ is:

$$\delta_{t+1} = \delta_t - \lambda \frac{\partial L}{\partial \delta}$$

where λ is the step size (defaults to 500). δ_0 is initialized from a dog image to obtain solutions that are semantically meaningful.

B Discussions on δ versus common feature

Note that there is a subtle difference between δ generated from the optimization procedure above versus the common feature (CF) obtained from training. Intuitively, to find δ , we are moving an input in the direction perpendicular to $\nabla_x f(x)$, but the gradient itself is fixed because the model is fixed. When training a model with CF, $\nabla_x f(x)$ becomes small with respect to the CF. This explains why we expect minimal attribution change when δ is added to the input during input independence testing, but expect small attribution to dog CF during input dependence testing.

C Other measures for input independence

An alternative measure of input independence is the average attribution difference when δ is added to the input:

$$\frac{1}{|X_{corr}|} \sum_{x \in X_{corr}} \left| \frac{g_c(f, x + \delta) - g_c(f, x)}{g_c(f, x)} \right|$$

Figure 11 shows the average perturbation over 100 images for each saliency method. Lower attribution difference is better. The ranking is roughly the same as the *IIR* metric.

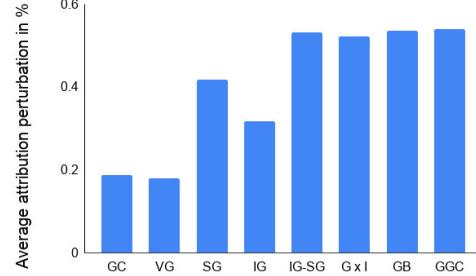


Figure 11: Average g_c between x and $x + \delta$ over 100 inputs.

D DNN Architecture and training

All BAM models are ResNet50 He et al. (2016) models. Training starts from an ImageNet pre-trained checkpoint Russakovsky et al. (2015) (available at <https://github.com/tensorflow/models/tree/master/official/resnet>) and all layers are fine-tuned on the BAM dataset. 90% of randomly chosen members of the BAM dataset are used to train, the rest are used for testing. All models are implemented using TensorFlow Abadi et al. (2016) and trained on a single Nvidia Tesla V100 GPU.

E Details of interpretability methods compared

We consider neural network models with an input $x \in \mathbb{R}^d$ and a function $f(x) : \mathbb{R}^d \mapsto \mathbb{R}^m$. A saliency method $e(f, x) : \mathbb{R}^d \mapsto \mathbb{R}^d$ outputs a saliency map highlighting regions relevant to prediction. Below is an overview of the eight saliency methods evaluated in our work.

GradCAM (GC) Selvaraju et al. (2016) computes the gradient of the class logit with respect to the feature map of the last convolutional layer of a DNN. Guided GradCAM (GGC) is GC combined with Guided Back-prop through an element-wise product.

Vanilla Gradient (VG) Simonyan et al. (2013); Erhan et al. (2009); Baehrens et al. (2010) computes the gradient of the target class k at logit layer l with respect to each input pixel: $e(f, x) = \frac{\partial f_k^l}{\partial x}$, reflecting how much the logit layer output would change when the input changes in a small neighborhood.

SmoothGrad (SG) Smilkov et al. (2017) reduces visual noise by averaging the explanations over a set of noisy images in the neighborhood of the original input image: $\frac{1}{|N|} \sum_{i=0}^N e(f, x + z_i)$, where $z_i \sim \mathcal{N}(\mu, \sigma^2)$.

Integrated Gradient (IG) Sundararajan et al. (2017) computes the sum of gradients for a scaled set of images along the path between a baseline image (x') and the original input image: $e(f, x) =$

$(x - x') \times \int_0^1 \frac{\partial f(x' + \alpha(x - x'))}{\partial x} d\alpha$. Smoothing from SG can be applied to IG to produce IG-SG.

Gradient x Input (G x I) computes an element-wise product between VG and the original input image. Ancona et al. (2018) showed that for a ReLU network with zero baseline and no bias.

Guided Backpropagation (GB) Springenberg et al. (2014) builds on top of the DeConvNet explanation method Zeiler and Fergus (2014) and attributes input importance through backpropagating neuron activations from the logit layer to the input layer.

We accompany visualization of a subset of saliency methods by averaging over channels and capping the extremes to the 99th percentile as done by Sundararajan et al. (2017); Smilkov et al. (2017) before normalizing each attribution to between [0, 1].

F Details of computing TCAV scores

We compute the TCAV scores of the dog concept for different models (e.g. f_o and f_s for absolute contrast). To learn the dog CAV, we take 100 images from $X_{o,s}$ where the object is a dog as positive examples and 100 images from $X_{\emptyset,s}$ as negative examples for the dog concept. We perform two-sided t-test of the TCAV scores, and reject scores where p -value > 0.01. We compute TCAV scores for each of the block layer and the logit layer of ResNet50. The final TCAV score is the average of the layers that passed statistical testing.

G Details of model contrast score baseline

For model contrast score, we generate a random mask I_c to calculate baseline differences. For TCAV, we obtain two TCAV scores for two models (f_o and f_s), and show the difference between the two, both for TCAV scores for the dog CAVs and random CAVs.

H Full size figures

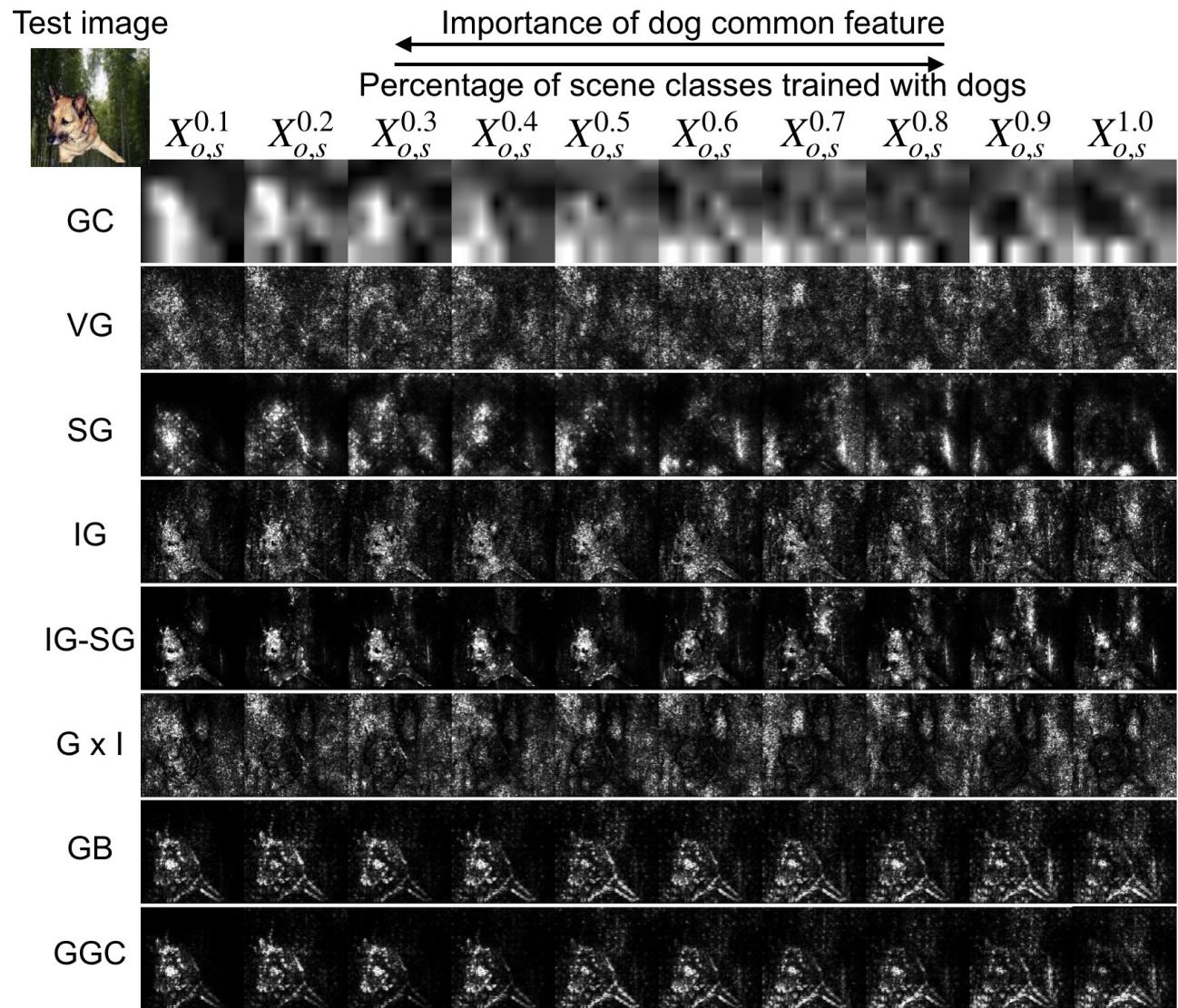


Figure 12: Full figure of an example of saliency map visualizations for models trained with CFs of different k . k increases from left to right. A larger contrast among each row is better.

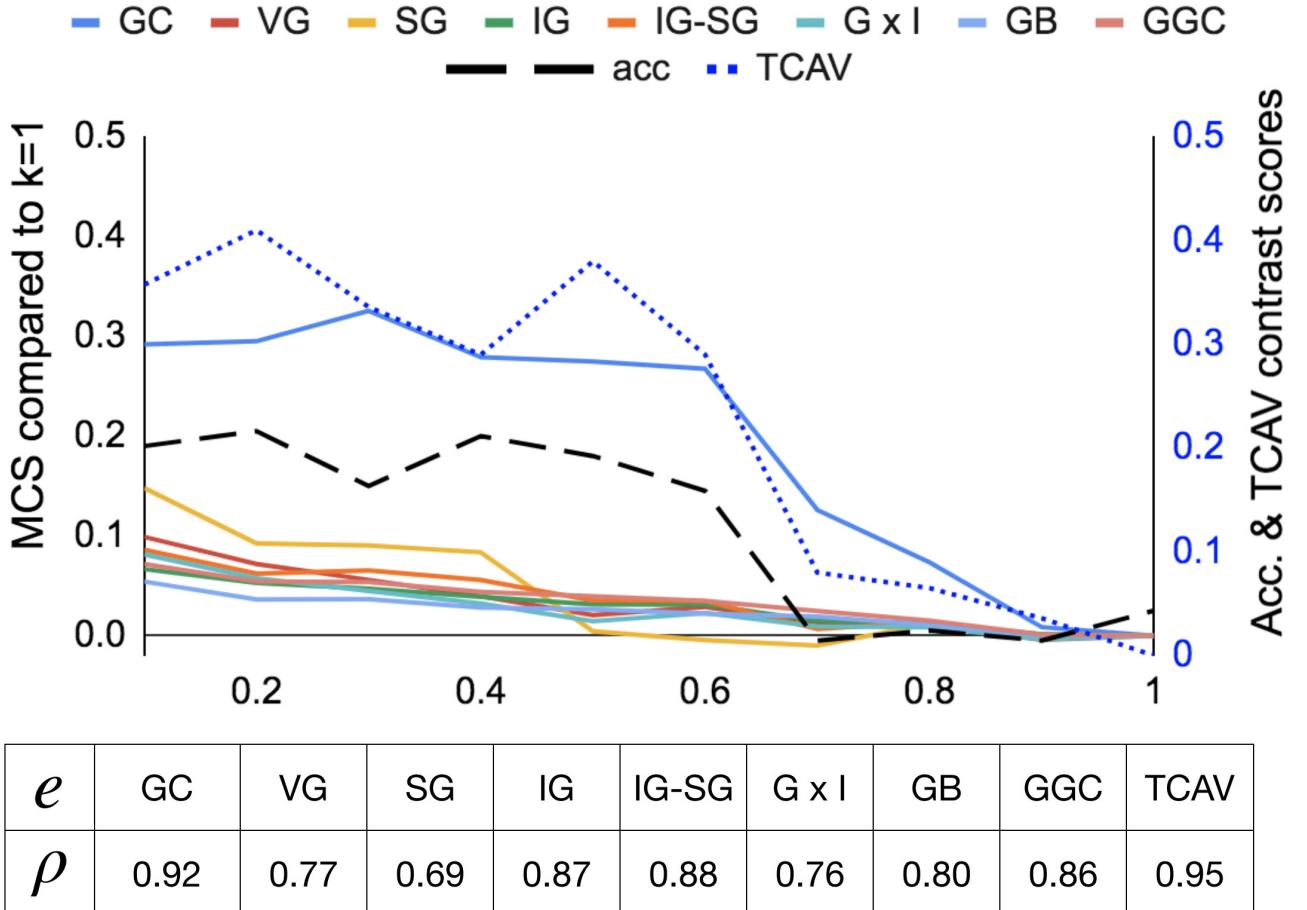


Figure 13: [Top] MCS between $\{X_{o,s}^k\}$ for $k \in \{0.1, \dots, 1.0\}$ and $X_{o,s}^{1,0}$ as k increases. The dashed black line is the accuracy drop when CF is removed during testing. The dotted blue line is the series of MCS for TCAV. [Bottom] Pearson correlation coefficients (ρ) between each method's MCS and the accuracy drop. A higher correlation is better.

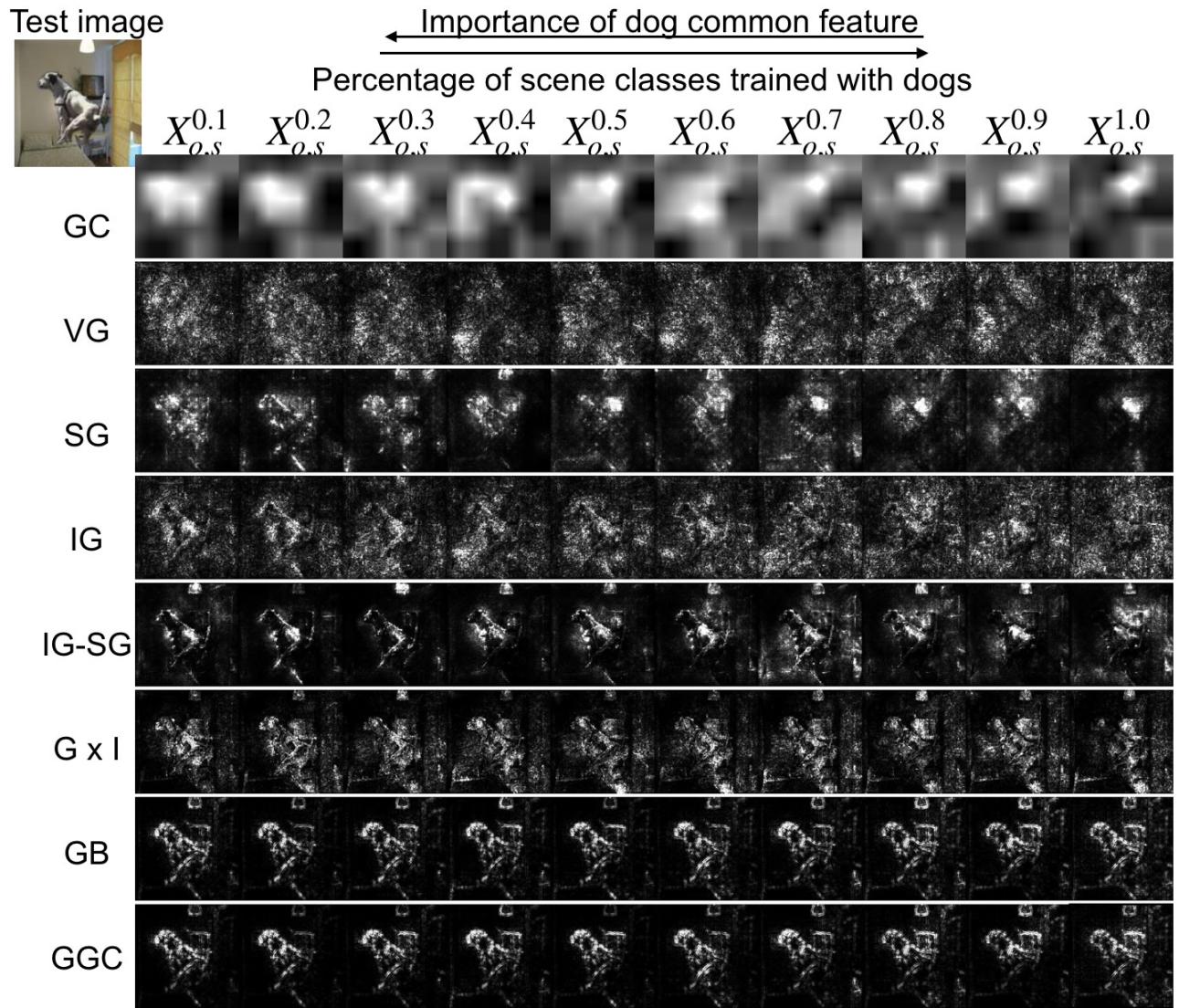


Figure 14: Additional example saliency maps from relative model contrast testing.

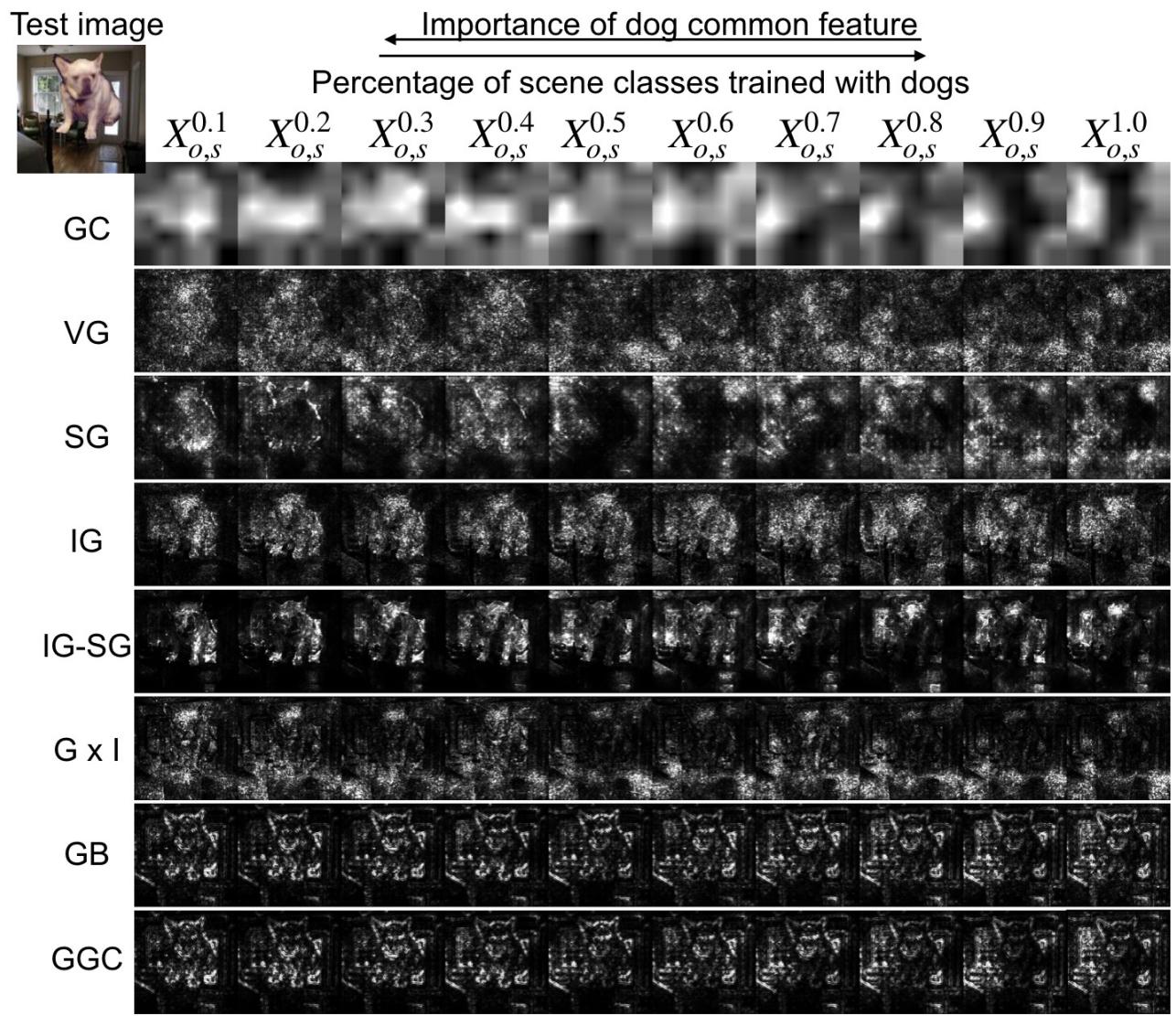


Figure 15: Additional example saliency maps from relative model contrast testing.

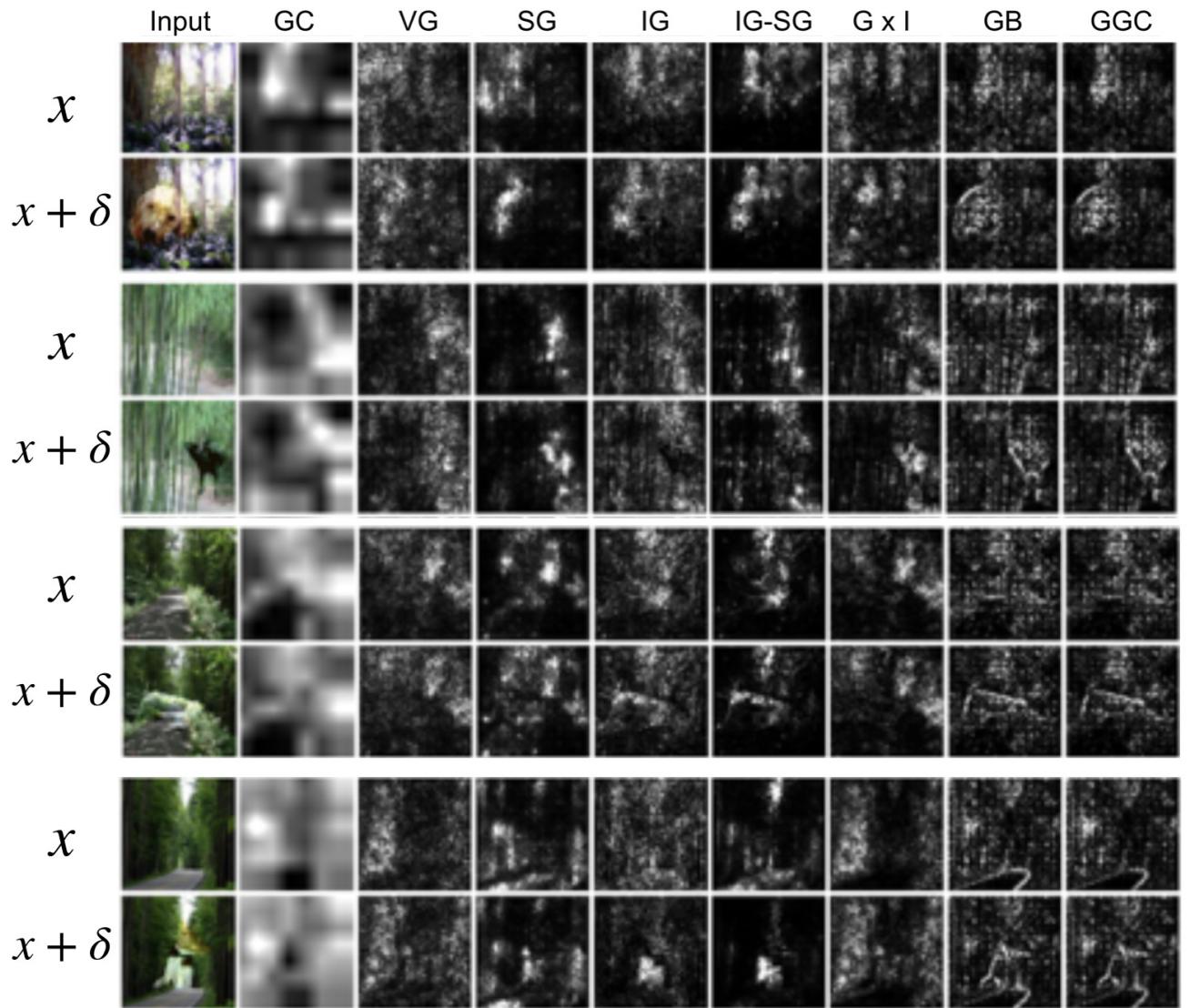


Figure 16: Additional example saliency maps from input independence testing.