

Why you shouldn't trust me: A survey on Adversarial Model Interpretation Manipulations.

Verena Heusser

verena.heusser@student.kit.edu

Karlsruhe Institute of Technology (KIT)

Karlsruhe, Germany

Abstract

The accuracy of machine learning models is no longer enough: we also want the often inherently complex models to be safe, robust, and interpretable by humans. As machine learning models enter critical areas in human lives such as the criminal justice system, medicine or financial systems, the inability for humans to understand these models is dangerous and problematic. Progress in the emerging research field of explainable artificial intelligence promises to be a remedy, where interpretation methods try to uncover *how* models work. However, while the number of studies using these methods is exploding, there are also a growing number of articles pointing out that the interpretive methods are still fundamentally flawed. This work provides an overview of the subfield of manipulating interpretable machine learning, with the goal of providing insight into concepts, existing research, and future directions. We want to raise awareness that interpretation methods, just like the underlying machine learning models, can be outwitted by adversaries and that there is often no way to detect adversarial attacks.

Keywords

Interpretability, Adversarial Machine Learning, Adversarial Model Interpretation Manipulations

ACM Reference Format:

Verena Heusser. 2020. Why you shouldn't trust me: A survey on Adversarial Model Interpretation Manipulations. In *Interpretability '20: ACM Symposium on Neural Model Explanations, December 16–20, 2020, Karlsruhe, DE*. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 Introduction

In recent years, deep learning models have demonstrated superior performance on a variety of tasks [10, 30, 32]. While performance is still increasing and more tasks are being handled, their performance comes at the cost of complexity: models often use millions to billions of parameters to achieve universal function approximation. This

⁰Code for replications and experiments will be made available on https://github.com/verenaHeusser/adversarial_interpretation_manipulation

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Explainability '20, December 16–20, 2020, Karlsruhe, DE

© 2020 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

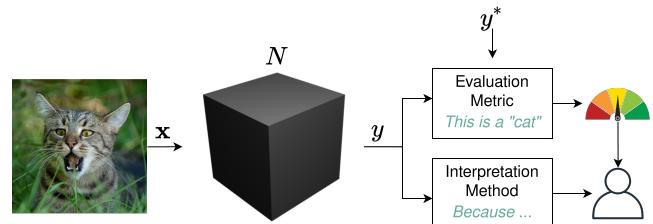


Figure 1: Prediction pipeline using a machine learning model, depicted as black box. Typically, evaluation metrics require the prediction y and the ground truth label y^* allowing for the assessment of the model's accuracy. Additionally answering the question *why*, i.e. making the model interpretable for a human, requires additional methods.

complexity means that they remain black boxes that cannot be interpreted even by experts.

Such a black box is able to predict fairly well for unseen yet similar data, answering the question of *what* is the most likely label for an input sample. However, most models will provide no answer to *why* or *how* the model chose this label for the instance and which features of the instance were crucial for making this prediction. For example, if a machine learning model is tasked with classifying images of cats (as in Figure 1), one would like to assume that the presence (or absence) of a cat in an image is indicative (contraindicative) of the classification of the image into the "cat" ("not cat") category.

Automated algorithms are already in use in critical areas, such as medicine, chemistry, the criminal justice system, the financial sector or the piloting of self-driving cars [11, 15, 46]. Thus, as machine learning models are moving out of the lab into the real-world, the inability of humans to understand these (black box) models seems even more problematic. Not knowing how a model makes predictions, and not being able to detect systematic biases in the model, prevents the vastly advancing technology of machine learning from being used in highly sensitive and safety-critical applications.

Suppose a deep neural network predicts the risk for cancer from a mammogram, which is an image of breast tissue. A doctor would only use the algorithm if there is a way to validate that (1) the algorithm is accurate (which can be measured in terms of the predictive accuracy), and (2) if the model is also using the correct indications in the data for predicting the risk of cancer. (1) is the standard approach for validating the performance of machine learning models, but in this example, one can clearly see why predictive accuracy

might not be enough in many areas. For approaching (2), i.e. uncovering *why* a model predicts a low / high risk of cancer, the research field of explainable artificial intelligence (XAI) offers a fast growing number of methods. Some research even suggests to allow 'peeking inside the black box' of deep learning models [1].

In addition to this insecurity on the model level, it is likely that machine learning systems in deployment will be attacked.

Not knowing about attacks and data arranged to exploit specific vulnerabilities has contributed to the field of XAI comprising topics of (1) *model interpretations*, (2) *adversarial attacks*, or manipulation methods and (3) the field of *adversarial manipulations of model interpretations*. All these subfields have the common goal to make models more robust and safe for deployment. (1) refers to the development of techniques that can be used to understand and explain the decision making process of a machine learning model or even the development of models that are inherently interpretable. (2) is the field of detecting vulnerabilities in models that cause these models to be deceived by altered input. (3) is the main topic of this paper, i.e. how to fool interpretation methods in order to detect vulnerabilities and malfunctions in interpretation methods. Ideally, an interpretation, or explanation method should indicate which features in the input to a model contribute to the prediction and also to what extent each feature contributes. The extent to which each feature contributes to a prediction is often called the *importance* score of a feature. Figure 2 shows such a feature importance map (Figure 2b) produced by the interpretation method LRP [9] applied to the neural network model Inception-v3 [43]. The input image is from the ImageNet dataset [33]. The output of the interpretation method is projected onto the original image for better human readability. This importance map suggests that specific portions of the original cat image are important for the neural network make the high-confidence prediction (see..) of the category 'tiger cat'.

While interpretation methods are already used for analysis of computer vision systems [9, 38, 49], text and sequence analysis [4, 7], and deep learning in security [45], there is still a lack in the understanding of model interpretation methods. In particular, it is unclear how the variety of proposed model interpretation methods are related and what common concepts can be used to evaluate and compare them. Many works are dedicated to establish a formal definition of what it means for a model to be interpretable, and how to select and evaluate methods for generating interpretations of machine learning models [26, 28]. However, a growing number of researchers also focus on breaking these interpretation methods, similar to research on adversarial attacks on machine learning models, which is deeply fueled by the vast deployment of models in the real world [5, 12, 13, 17, 18, 22–25, 39, 50].

Outline.

This article examines a topic at the intersection of explainable and adversarial machine learning research. The overview presented in this article examines the existing literature and contributions in the field of XAI focusing on methods to manipulate explanation methods. We try to offer a comprehensive taxonomy of these interpretation manipulation methods.

This paper is structured as follows. section 2 introduces common interpretation methods for machine learning models, and offers a taxonomy of the variety of techniques and a brief outline of

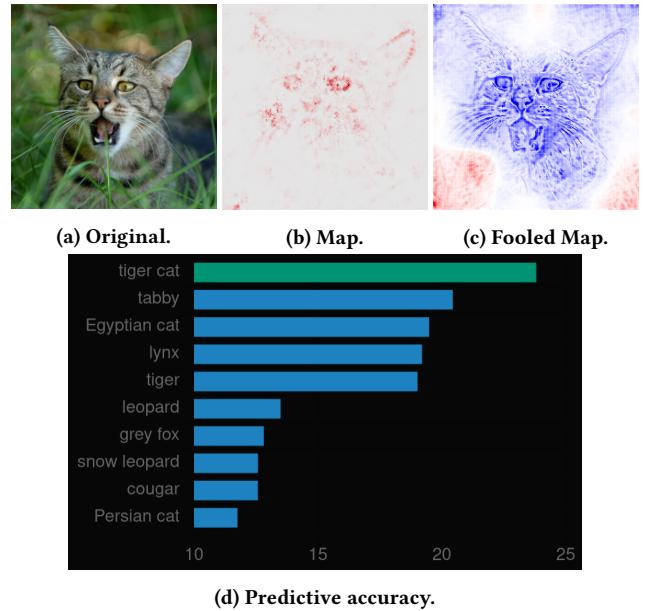


Figure 2: Visualization of the feature importance and fooled feature importance maps produced by the LRP interpreter applied to the image of a cat and an image classification model. The fooling method is the *location* fooling from [18]. Dark red here means a stronger significance of the feature.

popular interpretation methods. In section 3, the main topic of this paper, namely manipulation methods for deceiving interpretation techniques, is outlined. A taxonomy of methods is proposed and possible evaluation criteria are listed. section 5 proposes approaches to benchmark the robustness of interpretation techniques and section 4 provides a review of important studies in the field of manipulation methods. The implications of this research area on XAI are discussed in section 6.

2 Interpretation Methods

There exists a variety of definitions in the vastly expanding research field of XAI, and the concept of *interpretability* still has no formal commonly used technical meaning [26]. To build on the common ground of existing research, this work follows the terminology of Lipton et al. [26] and Arrieta et al. [8].

Broadly, interpretability focuses on *how* and *why* a machine learning model makes predictions. Simply put, interpretability is focused on getting some notion of an explanation for the decisions made by a machine learning model.

2.1 Terminology

The authors of [8] make a distinction between the related but different concepts of *interpretability* and *explainability*. Lipton [26] further breaks down interpretability into *transparency* and *post-hoc* interpretability. The notion of *explainability* from [8] can be related to Lipton's *transparency*, while Lipton's *post-hoc* interpretability is essentially *interpretability* as defined by Arrieta et al. [8].

Post-hoc Interpretability refers to the extent to which cause and effect can be observed in a model, which can be translated to uncovering *why* a model made prediction y to an input \mathbf{x} , or how input and output relate. Consider the example of image classification from Figure 1. Here, interpretability would mean that if a cat is present in the image (the cause), the model classifies it to the category 'cat' (the effect). Now imagine we find that the model takes the green meadow in the image as evidence to predict 'cat', and not the cat itself. This would imply a lack of interpretability, as the model learns to assign features to the concept 'cat' other than those related to 'cat' in the correct sense. This toy example emphasizes a common problem in image classification: [47] observe the over-reliance of models on image background, rather than on objects in the foreground.

Explainability or Transparency on the other hand spans methods to uncover *how* a model makes predictions, meaning to observe the inner workings of a model and thus to literally explain what is happening in terms of understanding of the mechanisms by which a model works. Thus, transparency refers to the model's inherent properties that can be known before the training process and that are helpful to understand the model.

While both concepts seem to be important for the general objective of explainable artificial intelligence, this paper focuses on post-hoc interpretability. There are essentially two ways to achieve interpretability: (1) to use inherently interpretable models or (2) to post-process a model in a fashion that allows to yield insights. The former is known as the development of *surrogate* models and more generally described as *model-agnostic* methods. Option (2) is known as *model-transparent* methods.

Local and Global Methods. A further categorization can be made based on the scope of interpretations: *Local* methods aim at providing interpretations that are true for a single data points and its neighbors. *Global* methods aim at gaining interpretations that are valid for most data points in a class [21, 29, 48]. The interpretation methods discussed within this paper mostly fall into the class of local explanation methods [9, 27, 31].

Feature Attribution Methods and Sample Attribution Methods. Interpretation methods aim at making complex and inherently uninterpretable black box models interpretable by creating human readable visualizations. A frequently used type of explanation methods are *feature attributions* mapping each input feature to a numeric score. This score should quantify the importance of the feature relative to the model output. The resulting attribution map is then visualized as a heatmap projected onto the input sample. This allows humans to interpret which input attributes are the most helpful for making the final prediction. Sample attribution methods on the other hand interpret the model performance in terms of the importance of training examples from the dataset.

We propose the following formal definition for interpretation method:

Definition 1: Interpretation Method.

We consider a neural network $N : \mathbb{R}^d \rightarrow \mathbb{R}^k$. For an arbitrary classification task, N classifies an input sample $\mathbf{x} \in \mathbb{R}^d$ in k

categories where the prediction $f_N(\mathbf{x}) = y \in \{1, \dots, K\}$ is given by $y = \text{argmax}_i f_N(\mathbf{x})_i$.

Given the neural network N , its input vector $\mathbf{x} \in \mathbb{R}^d$ and the neural network's prediction for input \mathbf{x} , $f_N(\mathbf{x}) = y$, an interpretation method I determines why label y has been chosen by N for input \mathbf{x} . The interpretation is given by an output vector $\mathbf{h}_k \in \mathbb{R}^d$ for a class k where each entry h_i is mostly a numeric value describing the relevance for the i -th input feature x_i of \mathbf{x} for the final score $f_N(\mathbf{x})$.

As \mathbf{h} has the same dimensions as the input \mathbf{x} it can be mapped to the input, overlaying \mathbf{x} as a heatmap, where the color value represents the importance of feature x_i towards the prediction $f_N(\mathbf{x})$. An example is given in Figure 2b. Higher values, implying a stronger relative importance for making the prediction $f_N(\mathbf{x})$, are depicted in dark red.

While all explanation methods try to obtain importance measures for the network prediction, they differ with respect to how these measures are obtained. [45] propose two major categories for interpretation strategies, namely *black-box*, in the following named *model-agnostic* methods and *white-box*, or interpretation methods. While black-box interpretations assume no knowledge about the underlying model, white-box methods only work by using the model parameters.

This terminology of discriminating between black-box and white-box methods may not be confused with the nature of the underlying models: Models still remain of black-box nature even though a white-box method may contribute to making the decision making process of such a model more insightful.

The following section details the two categories and will give examples of the state-of-the-art interpretation methods within each group.

2.2 Model-agnostic methods.

Model-agnostic interpretations assume no knowledge about the model thus treating it as a black box. The underlying model is approximated by learning its behavior with an interpretable model, e.g. a linear model. The interpretable model is also dubbed the 'surrogate' model. The common approach for learning the surrogate is to approximate the relationship between the input samples and the corresponding prediction by the model. As the model itself does not need to be known, these approaches can be used in scenarios where the model itself is not directly accessible. Model-agnostic interpretations are fairly popular and are used in a wide range of applications, ranging from finance and law to medicine and chemistry [15, 46].

A black-box interpretation offers the great advantage of being applicable to any model and offers simplicity because the interpretation is embedded in the model. However, this option of gaining interpretability might be costly for users that already have a high performing model. For this reason, growing need for methods exists that can be applied without retraining or modifying the underlying model. We will briefly describe two common model-agnostic approaches. Refer to the original papers for details.

Local Interpretable Model-agnostic Explanations (LIME).

LIME [31] perturbs the input and observes how the predictions of a black box model change. For the task of image classification, LIME

creates a set of perturbed instances by dividing the input image into interpretable components, which are technically contiguous superpixels, and runs each perturbed instance through the model to get the probability for how much the change in each superpixel influences the whole model prediction.

Figure 3 shows an example of LIME applied to the neural network model Inception-v3 [43]. Input image from the ImageNet dataset [33]. The superpixel in dog instances place is highlighted in green, which correctly indicates that this superpixel has a high influence on the prediction of the images correct class ('bernese mountain dog'). LIME also correctly indicates that the superpixel in the cat's place does not indicate the correct class label.

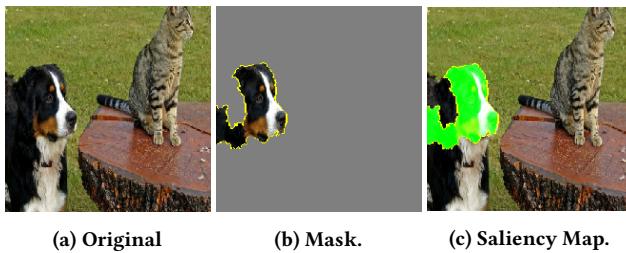


Figure 3: Visualization of the output of the LIME interpreter applied to an image and image classification model.

SHapley Additive exPlanations (SHAP). SHAP [27] builds on Shapley analysis, which is essentially about judging the importance of attributes. The model is trained on a number of subsets of all available features, and the feature importance scores are calculated by evaluating the effects that the omissions of the specific features have on the model prediction. An example is shown in Figure 4. Image regions highlighted in green are found to be important for predicting the correct label.

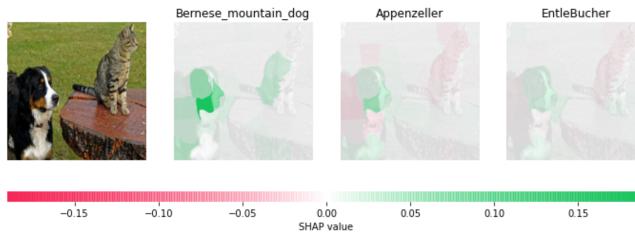


Figure 4: Visualization of the output of the SHAP interpreter applied to an image and image classification model.

2.3 Model-transparent methods.

The other group of interpretations are model-transparent, or white-box methods, where the underlying model is known with all its parameters. Thus, the interpretation can be directly computed by using the model instead of relying on an approximation of f_N as within the black-box methods. These methods typically rely on the relationship between an input sample, the underlying model's prediction and the associated activations of the models hidden

layers. Methods within this group are for example propagation-based and gradient-based approaches. The former propagate back the model's prediction back through the model. The latter make use of the information provided by the gradients of the loss function, which contain sensitive information about the prediction and the features. Using the backpropagation method, features in the input can be highlighted based on the amount of gradient they receive. This shows their contribution to the final score. A few example methods within this group are listed below.

Layer-wise Relevance Propagation (LRP). While many approaches in the group of model-transparent interpretations are designed only for image classification, or convolutional neural networks, this method [9] is an exception. LRP propagates relevance values backwards through the network and decomposes the score of a predicted class backwards through the network. It relies on a Taylor series close to the prediction point rather than partial derivatives at the prediction point itself. An example for a feature map produced by LRP can be found in Figure 2b.

DeepLIFT [37] is an improved version of LRP, where a reference point in the input feature space is defined. Relevance scores are propagated proportionally to the changes of neuronal activations from the reference.

SmoothGrad (SG) [40] averages over interpretations of noisy copies of an input sample thus reducing noise by visually diffusing the interpretation. The noise is drawn from i.i.d. from a normal distribution.

Methods developed for convolutional neural networks are for instance GradCAM [36] or SimleGrad TODOcite.

3 Manipulation Methods

As outlined in section 2, there are a variety of explanation methods readily available as frameworks and open source implementations. However, there is still little analysis on the robustness and reliability of such methods. While it is already common practice to test machine learning models against adversarial attacks in a number of domains [16, 20], the same is not yet the standard for interpretation methods. We argue that interpretation techniques should not be used in critical applications without basic testing of interpretation techniques against adversarial settings.

3.1 Adversarial Setting

Adversarial Attacks on Models. Adversarial examples, as first introduced by [44], are clever manipulations of an input by an adversary which aims at causing misclassification and fooling of applications. They are mostly used to fool or attack machine learning models. We formally define adversarial attacks by the following properties:

Definition 2: Model Manipulation Method

1. *Impercpetibility of Perturbation:* The adversarial example is similar to original data, i.e. the norm of the added perturbation δ to an input sample x thus must be small, i.e.

$$\|x + \delta\| = \|(x + \delta) - x\|_{\text{inf}} \leq \epsilon$$

2. *Prediction dissimilarity*: The prediction of the model is significantly different to the prediction on the non-adversarial example:

$$f_N(\mathbf{x} + \delta) \approx f_N(\mathbf{x})$$

Note, that within adversarial foolings of models, the perturbation is mostly applied to the input data, and not to the model itself.

Evidence from many studies shows that deep learning models can be easily tricked by adversarial examples. Albeit there are not yet as many studies, there also exists evidence that many interpretation methods are also fragile with respect to small changes to input data [2, 3, 35] as well as to the model itself [12, 18]. This fooling of interpretation methods is outlined below.

Adversarial Attacks on Model Interpreters. Contrary to adversarial attacks on machine learning models, the focus of this paper is on the attacks on interpretation techniques without changing the prediction of the model. An adversarial attack on a model interpretation is in the following also called a *manipulation* method. The goal is to apply perturbations to either an input sample or the model to change the output of an interpretation technique while leaving the model prediction unchanged. The last condition is important because adversarial interpreter manipulations aim to fool the interpretation method and essentially not the model itself. Fooling the model would only disclose the vulnerability of the model but would not allow to gain insight into the stability of the interpretation method. Again, the problem can be formally defined as:

Definition 3: Interpretation Manipulation Method.

A manipulation method \mathcal{F} is defined as a method for altering the output of an explanation method \mathcal{I} while leaving the model performance of the neural network N roughly unchanged. As manipulations can be applied on the input or the model level (see subsubsection 3.2.1), $\mathbf{x} + \delta$ denotes a perturbed input sample regarding the input level manipulation, while $N + \delta$ denotes a model with altered parameters, referring to the model level manipulation.

A manipulation method is successful in fooling an interpreter, if the following properties hold:

1. *Prediction similarity*: The model prediction stays approximately the same, i.e.

$$f_N(\mathbf{x} + \delta) \approx f_N(\mathbf{x}), \text{ or } f_{N+\delta}(\mathbf{x}) \approx f_N(\mathbf{x})$$

2. *Interpretation dissimilarity*: The explanation map $h(\mathbf{x} + \delta)$ is significantly different to the explanation map resulting from non adversarial models or inputs $h(\mathbf{x})$, i.e. $h(\mathbf{x} + \delta) \neq h(\mathbf{x})$

$$\arg \max_{\delta} = \mathcal{D}(\mathcal{I}(\mathbf{x}_i, \omega), \mathcal{I}(\mathbf{x}_i + \delta, \omega))$$

3. *Imperceptibility of Perturbation*: In case the attack is in the input domain of the model, the perturbation of input samples must be imperceptible by humans. According to [13], the norm of the added perturbation δ to an input sample \mathbf{x} thus must be small, i.e.

$$\|\mathbf{x} + \delta\| = \|(\mathbf{x} + \delta) - \mathbf{x}\|_{\inf} \leq \epsilon$$

These measures are to be seen as comparison between a baseline model N and a model that is applied in the adversarial setting (i.e. either N is not changed but applied to adversarially altered data $\mathbf{x} + \delta$, or N is adversarially trained thus becoming $N + \delta$).

[12] extend these properties to include the so called *model similarity*. This measure extends the *prediction accuracy* to span the accuracy difference in between the baseline model and the new model, and also the mismatch of data points where the predictions of both models differ.

After formally defining what successfully fooling an interpretation method means, we want to provide intuition in Figure 2. The interpretation method produces an interpretation, here in form of a saliency map projected onto the original image. If a successful manipulation is applied, the resulting saliency map of the same interpreter should be different to the original map. This effect is clearly visible, as Figure 2b is visually significantly different to the map produced by the same interpretation method but applied to an adversarial model (see Figure 2c).

3.2 Taxonomy of Interpretation Manipulation Methods

There are two important categories of Manipulation Methods that aim at attacking model interpretation methods. The first category is based on the level these manipulations operate on, i.e. input space level or model / parameter level. The second categorization is based on the target of the manipulations. While untargeted manipulations are mostly random perturbations, targeted manipulations aim to perturb the interpretation of specific input features.

3.2.1 Manipulation Levels

Adversarial Input Manipulation. The general approach is to perturb or alter input data while observing the effect of this perturbation on the model prediction. This concept is visualized in Figure 6. As found in [13], visually-imperceptible perturbations of an input image can make explanations worse for the same model and interpreter.

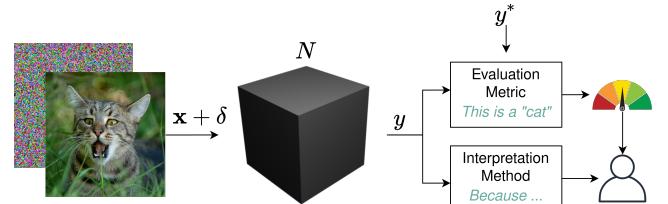


Figure 5: Depiction of an adversarial input manipulation. The model is fine-tuned with altered input samples, which are indicated by $\mathbf{x} + \delta$.

Adversarial Model Manipulation. Contrary to input manipulations, model manipulations do not operate on the input space but rather on the model parameter space itself. As first introduced by Heo et al. [18] in 2019, this line of research is comparably new. Adversarial model manipulations for fooling the interpreter are obtained by fine-tuning the model on the same data but with an adapted objective function. [18] propose the adapted loss function for the task of image classification of

$$\mathcal{L} = \mathcal{L}_{CE}(\mathcal{D}; \omega) + \lambda \cdot \mathcal{L}(\mathcal{D}; \omega; \omega_0)$$

where \mathcal{L}_{CE} is the standard cross-entropy classification loss. Adversarial model manipulation is depicted in Figure 6 where the altered model is indicated by $N + \delta$.

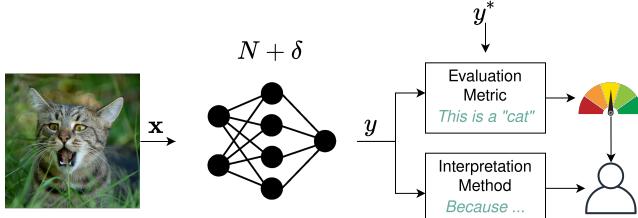


Figure 6: Depiction of an adversarial model manipulation. The model is fine-tuned with the same distribution of input data and a fooling loss, thus yielding the biased model $N + \delta$.

3.2.2 Manipulation Targets

In addition to the categorization of manipulation methods based on the manipulation level, the methods can further be categorized based on the target of their perturbation. The first possibility is *untargeted* perturbation, the second is *targeted* perturbation. Both these styles can be applied on either model and input level.

Untargeted Manipulations. The majority of manipulations is untargeted, meaning that the applied perturbations are mostly random and not designed to change the prediction for a specific portion of an input sample.

Targeted Manipulations. On the contrary, targeted manipulations aim at specifically changing the explanation of certain features of an input instance. Such a specific feature might be an object in the input image in the context of image classification. [18] for instance introduce a fooling scheme in which the interpretations of the target classes elephant and school bus are swapped. Manipulations on the level of the model are mostly targeted, as the explanation methods are being fooled by adapting the model parameters.

3.3 Evaluation Criteria

Besides the necessary properties of a successful interpretation manipulation method, other evaluation criteria are important to access the successfulness of a fooling method and to enable the comparison between different fooling methods. These criteria are informally defined in the following.

Effectiveness. The manipulation scheme is inexpensive to conduct. Input manipulations are by definition inexpensive, as the perturbation can be applied to single input samples. Model manipulations are more expensive as they require the model parameters to be adapted. However, an adversarial model can be obtained by fine-tuning the model with an adapted objective function. This fine-tuning also has the advantage that the model is adapted to include a systematic bias and can thus be applied to fool explanation methods without further adapting the model or input samples after the fine-tuning step. Furthermore, this systematic bias is hidden in the model, and is hard to uncover. Input manipulations can only fool the model when the inputs are always manipulated.

Transferability. The manipulation does not only fool one type of interpretation method, but it's effect transfers to other interpretation techniques.

Generalisation. Generalization of an attack refers to the transfer of fooling to other test samples. This is noteworthy since a manipulation method might only perturb the decision boundary locally around the training points, i.e. only influencing training instances and their neighbors. However, it is desired that the explanations of unseen samples are affected as well. Furthermore, not only unseen samples interpretations, but also samples that are far away in the feature space, should be affected,

TODO

Most of the explanation methods outlined in sec. section 2 have been shown to be vulnerable to adversarial perturbations. Manipulation methods often show that there exist small feature changes resulting in a change of the explanation methods output while the output of the model itself does not change. Most approaches aim at providing a relevance measure of the input features.

Creation of a fooled model by fine-tuning the model with a fooling loss.

As outlined in section section 3, there exists a plethora of interpretations methods differing in the assumption about the model character and also with respect to how interpretations are obtained. Thus, reliable evaluation methods are required allowing for a choice of an appropriate and robust interpretation method. Ultimately, the accordance to these evaluations should naturally allow for choosing an appropriate and robust interpretation method. Evaluations of the quality of an explanation method are separated into qualitative and quantitative evaluations.

Qualitative Evaluation. Inspection and random sampling are commonly used techniques to obtain an intuition about the effect of manipulations. As interpretations are attributed to input features, the resulting relevance values l can be easily mapped to the input vector x . Visual inspection of these evaluations for specific samples is informative, but does not allow for general statistics and validation of manipulation effects. Thus, quantitative evaluations are required. [2] consider two kinds of visualizing saliency maps:

- **Absolute Value (ABS).** Saliency maps visualized this way show only the absolute values of the normalizem maps.
- **Diverging.** The diverging visualization indicates positive and negative importance in different colors.

Quantitative Evaluation. As the goal of interpreter manipulations is to fool an interpreter, thus altering the output of an interpreter, it is straightforward to compare interpretations and data samples before and after perturbation [17].

As interpreter manipulations shall alter the output of an interpretation methods while keeping the prediction of a model unchanged, the following metrics

- **Fooling Success Rate (FSR).** [18] introduce the concept of the Fooling Success Rate (FSR). The FSR captures the relationship between the model's predictive accuracy and the correctness of the interpretation averaged over multiple test

samples. The ‘correctness’ of the interpretation is the difference between the original interpretation methods output and the output of the same interpretation method when applied to either an adversarial input sample or adversarial model. The FSR counts samples for the model’s prediction did not change but for which the interpretation method’s output changed as a successfully fooled example. Thus, the higher the FSR, the more often the fooling is successful in fooling the interpretation method.

- **Area Over Prediction Curve (AOPC).** AOPC [34] is a principled way of quantitatively evaluating that the interpretations found by interpretation methods are valid, i.e. based on the features that the model truly uses for making the prediction. [18] use this measure to ensure that their adversarial model training does not fool the model (i.e. the predictive accuracy of the model is unchanged), but does fool the interpretation method.

As the goal of interpreter manipulations is to fool an interpreter, thus altering the output of an interpreter, it is straightforward to compare interpretations and data samples before and after perturbation [17]. There are metrics that are applied to identify changes in salient features for any task:

- **Spearman’s rank order correlation.** As interpretation methods rank the features based on their importance, the rank correlation [41] is a natural measure for comparing interpretations.
- **Intersection of the top- k features.** For some tasks, only the top- k features are relevant, such that a comparison between these top- k features is insightful.

Contrary, the following metrics are used only in computer vision tasks. They have been used in literature to quantify similarities between natural images and remove duplicates. Therefore, they are used in XAI research to compare the changes between saliency maps before and after manipulation for computer vision tasks.

- **Structural Similarity Index (SSIM).** SSIM values are relative similarity measure in the range $[0, 1]$, where larger values indicate higher similarity.
- **Pearson Correlation Coefficient (PCC).** PCC is also a relative similarity measure returning values in the range $[0, 1]$. Larger values indicate higher similarity.
- **Pearson Correlation of the Histogram of Gradients (HOG).** Used by [2] to indicate the intensity of change between two images.
- **Mean Squared Error (MSE).** As an absolute error measure, values close to zero indicate high similarity.

Note that these are only examples without demand for completeness. For further information see [2]. Normalizing these measures to yield values in $[0, 1]$ with a sum of one is good practice. Note that defining similarities that are similar to human vision is still an active area of research.

4 Interpreter Manipulation Method Examples

After introducing the terminology of model interpreters and manipulation methods in the previous chapters, this chapter gives detailed information about recent manipulation methods. This section also

provides insight into major findings in the field of manipulating model interpretations. First, input level manipulations are discussed, followed by model level manipulations.

4.1 Input Level Manipulations

Fooling both Model and Interpreter.

[42] design adversarial attacks that fool the machine learning model as well as the model interpretation. They design targeted and untargeted input patches superimposed onto original images and then feed into an image classification network and the interpretation method GradCAM.

The authors conclude that GradCAM does not reliably highlight the true cause of the prediction decision made by the model. Top-1 predicted label

The authors compare targeted and untargeted patches as well as uniform patches and randomly disturbed ones.

Model-agnostic Interpreters can be gamed.

[39] propose a framework for fooling the model-agnostic interpreters LIME and SHAP. Their method successfully hides the biases of models trained on adversarial examples by... The authors take a statistical approach model-agnostic interpretation methods. They examined the data produced by LIME and SHAP and showed that the perturbed samples are out-of-distribution samples compared to the distribution of the regular training data.

Figure 7 shows that the data samples generated by LIME are distributed differently than the original, non-perturbed data samples.

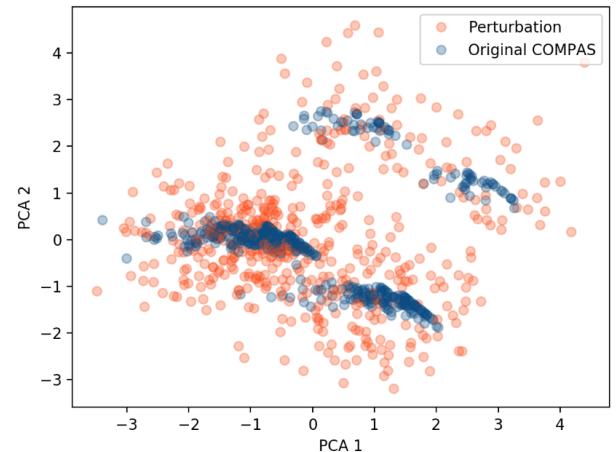


Figure 7: Principal Component Analysis (PCA) on the original data (orange) of the COMPAS dataset and the samples perturbed by LIME (blue). Note that the differences are obvious even in the space reduced to two dimensions.

Saliency Maps are vulnerable to Adversarial Attacks. [17] showed that importance scores produced by the popular interpretation methods Simple Grad, DeepLIFT and TODO.

4.2 Model Level Manipulations

The studies on model manipulation outlined so far have shown that *input perturbations* can make interpretations worse for the same model and interpreter. The articles in this section show that *perturbed model parameters* can also make explanations worse for the same input and interpreter.

Adversarial Model Fine-Tuning Fools Multiple Interpreters.

[18] were the first to introduce adversarial model manipulations for fooling interpretation methods. The authors adapted the fine-tuning stage of image classification models by using an altered fooling loss function. This loss function is a combination of the standard cross entropy loss function (to maintain the prediction performance) and an additional adversarial term. The adversarial term is used to encourage the interpretation method to give bad interpretations. The results show that the interpretation results are significantly altered while the classification accuracy is maintained. This indicates, that the model is robust to the attack, while the interpretation technique is very sensitive. Two categories of fooling methods are introduced:

- **Passive Fooling**, describing the adaption of the adversarial loss term to fool the interpretation method into highlighting uninformative pixels in the input image. Example results from the paper are in Figure 8. The baseline column shows that the interpretation method applied to the original image highlights pixels within the elephant as highly important for the network prediction. After fine-tuning the model with the adversarial loss, the effect of fooling the interpretation method is visible: Other, rather uninformative pixels are highlighted (see labeled columns two to four in the figure).
- **Active Fooling** is a method with the aim of causing the interpreter to highlight a completely different object in the image, i.e. to make the interpreter actively create false interpretations. This is realized by rewriting the loss function to minimize TODO.

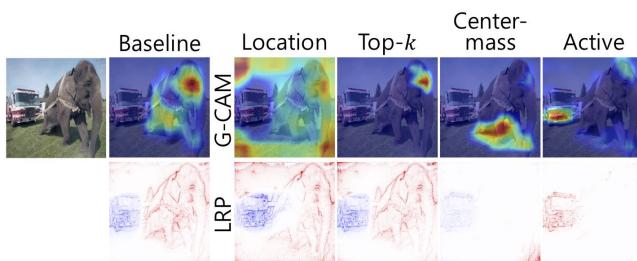


Figure 8

The authors also conduct an analysis to prove that the interpretations are valid. This is done by using the AOPC metric [34]. They find that all interpreters are fooled to a certain degree, and that the foolings furthermore generalize to other interpreters and especially to the whole validation set. It is worth noting that the proposed attack could not easily fool SmoothGrad, indicating that this is a better, or at least more robust interpretation method.

The authors find that SmoothGrad is less susceptible to model manipulation, while all other interpreters ()

The main point the authors are trying to make is that machine models can be systematically manipulated to contain unfair biases. They prove that such biases can be explicitly encoded into the loss function during the training stage, which yields an adversarial classifier that will generalize the learned bias to unseen test samples. This is dangerous, as the bias cannot be uncovered unless one has access to the full training pipeline. As interpretation methods claim to uncover the features a model uses for its decision.

After fine-tuning the model with the regular classification loss combined with an adversarial loss, they investigated if the interpreter results change as a function of model parameters. Two types of fooling methods were introduced, namely *active* and *passive* fooling.

[12] examine the relation of interpretation methods and the concept of fairness. They propose to learn a modified model with concealed unfairness. This is done by fine-tuning a classification model with a loss function extended by an explanation loss.

Their approach differs methodologically to [18] as follows: [18] adapt the standard cross entropy loss function by taking the gradient of the correct label element from the logits layer, while [12] use the gradient of the cross-entropy loss. Taking the gradient of the cross-entropy loss conveys more information about other classes, which may contribute to an improved generalization across different interpretation methods and first of all across different test samples.

While their approach takes the gradient of the one correct label element from the logits layer just before the softmax output, we take the gradient of the cross-entropy loss.

They define adversarial models that focus only on sensitive features which are not informative for the ground truth decision.

5 Benchmarking Interpretations

Checking the robustness, scope and hence the quality of model interpreters has become an indispensable step in explainable machine learning. Evaluating explanation and interpretation methods is difficult as ground truth is mostly lacking. In most applications, it is not known which input features are most important.

[2] propose a framework for sanity checking saliency map based interpretation methods. For this, a number of randomization tests are introduced along with some visualization techniques and metrics to compare interpretation outputs. The authors find that most methods fail their tests, and warn of the danger of visual assessment. Specifically, they warn that humans tend to choose visually significant appearing images that lack sensitivity to the data distribution and generation as well as to the model. However, their findings are so far limited to the domain of computer vision models and tasks. Implementing their randomization tests for other real-world datasets, such as COMPAS [6] or the adult income dataset [14] would be an interesting next step.

Additionally, in order to account for adversarial model manipulations, Heo et al. [18] propose to expand the criteria for checking the robustness of interpreters further.

6 Discussion

1

This paper summarizes the current approaches to manipulating model interpretation methods. On the one hand, the findings suggest that our models are not fully aligned with how human information processing works. If machine learning interpretation models would decide by the criteria we humans employ for tasks such as image classification, there would be no fooling of interpretation models by input or model manipulations. On the other hand, it was shown that advances in machine learning models has led to models that rely too much on the data they are trained on (the i.i.d. assumption), thus showing a high susceptibility to o.o.d. properties or properties that are highly correlated with labels in the dataset but are not distinctive in the real world (such as image backgrounds). Models and interpreters can still be misled in a large and systematic manner.

While there exists a number of review papers on XAI and its various subfields, this report is to the best of our knowledge the first one to comprehensively review manipulation methods for interpreters.

A growing number of studies gives evidence for model how interpretation methods can be gamed. Among these are the studies outlined in section 4. Other studies also raise concerns about if standard deep learning practices are valid, such as the work on fooling the broadly used attention mechanism [19].

We believe that identifying risks and adversaries helps to open up research on more robust interpretation methods.

6.1 Conclusion

Finally, it must be noted that the suitability of a method depends on its application domain.

Much critique has been applied to methods aiming at interpreting complex and potentially non-interpretable models in the domain of computer vision. Some researchers argue it is not worthwhile to study non interpretable systems while dismissing that using inherently interpretable models in the first place might be the better approach.

Adversarial attacks show that machine learning systems are still fundamentally fragile: They may be successful in a number of tasks, but fail to adapt to o.o.d. scenarios, i.e. when being applied to unfamiliar territory.

The findings about manipulating interpretations do not suggest that interpretations are completely meaningless, just as adversarial attacks on predictions models do not imply that machine learning models are useless. However, they suggest that there still are fundamental flaws in the way neural networks operate and that much caution and supervision could be applied if they are to be deployed in the real world.

This paper follows the footsteps of [26], trying to caution against blindly putting faith into post-hoc explanation methods. Moreover, we propose that checking the robustness of interpretation methods not only with respect to adversarial input manipulations but also with respect to adversarial model manipulation should be a necessary proof of concept.

¹All figures in this article are produced by the author unless noted otherwise.

6.2 Future Work

We see several possible future directions of future work. Firstly, for approaching the discrepancy of in-lab and real-life applications of, more focus might be laid in the development better performance metrics for both measuring the performance of machine learning models as well as their interpreters. More specifically, it might be fruitful to further investigate the correlation between ood samples and the performance of an interpretation method. So far, most of these findings are limited to specific experimental settings.

There is also no work proposing a benchmarking for ...

What is currently sparse is the comparison between different interpretation techniques and the relation of interpretation fragility to the model class, interpretation method and the task type and dataset structure.

The output of the interpretation method is projected onto the original image for better human readability → dangerous to trust this

References

- [1] Amina Adadi and Mohammed Berrada. 2018. Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI). *IEEE Access* 6 (2018), 52138–52160.
- [2] Julius Adebayo, Justin Gilmer, Michael Muelly, Ian Goodfellow, Moritz Hardt, and Been Kim. 2018. Sanity checks for saliency maps. *Advances in neural information processing systems* 31 (2018), 9505–9515.
- [3] David Alvarez Melis and Tommi Jaakkola. 2018. Towards robust interpretability with self-explaining neural networks. *Advances in Neural Information Processing Systems* 31 (2018), 7775–7784.
- [4] Marco Ancona, Enea Ceolini, Cengiz Öztïreli, and Markus Gross. 2017. Towards better understanding of gradient-based attribution methods for deep neural networks. *arXiv preprint arXiv:1711.06104* (2017).
- [5] Christopher Anders, Plamen Pasliev, Ann-Kathrin Dombrowski, Klaus-Robert Müller, and Pan Kessel. 2020. Fairwashing explanations with off-manifold deterrent. In *International Conference on Machine Learning*. PMLR, 314–323.
- [6] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. Machine Bias Risk Assessments in Criminal Sentencing. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- [7] Leila Arras, Franziska Horn, Grégoire Montavon, Klaus-Robert Müller, and Wojciech Samek. 2017. "What is relevant in a text document?": An interpretable machine learning approach. *PloS one* 12, 8 (2017), e0181142.
- [8] Alejandro Barredo Arrieta, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, et al. 2020. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion* 58 (2020), 82–115.
- [9] Sebastian Bach, Alexander Binder, Grégoire Montavon, Frederick Klauschen, Klaus-Robert Müller, and Wojciech Samek. 2015. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. *PloS one* 10, 7 (2015), e0130140.
- [10] Titus J Brinker, Achim Hekler, Alexander H Enk, Carola Berking, Sebastian Haferkamp, Axel Hauschild, Michael Weichenthal, Joachim Klode, Dirk Schadendorf, Tim Holland-Letz, et al. 2019. Deep neural networks are superior to dermatologists in melanoma image classification. *European Journal of Cancer* 119 (2019), 11–17.
- [11] Alexandra Chouldechova. 2017. Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. *Big data* 5, 2 (2017), 153–163.
- [12] Boty Dimanov, Umang Bhatt, Mateja Jamnik, and Adrian Weller. 2020. You Shouldn't Trust Me: Learning Models Which Conceal Unfairness From Multiple Explanation Methods.. In *SafeAI@ AAAI*, 63–73.
- [13] Ann-Kathrin Dombrowski, Maximilian Alber, Christopher Anders, Marcel Ackermann, Klaus-Robert Müller, and Pan Kessel. 2019. Explanations can be manipulated and geometry is to blame. In *Advances in Neural Information Processing Systems*. 13589–13600.
- [14] Dheeru Dua and Casey Graff. 2017. UCI Machine Learning Repository. <http://archive.ics.uci.edu/ml>
- [15] Radwa Elshawi, Mouaz H Al-Mallah, and Sherif Sakr. 2019. On the interpretability of machine learning-based model for predicting hypertension. *BMC medical informatics and decision making* 19, 1 (2019), 146.
- [16] Hang Gao and Tim Oates. 2019. Universal Adversarial Perturbation for Text Classification. *arXiv preprint arXiv:1910.04618* (2019).

- [17] Amirata Ghorbani, Abubakar Abid, and James Zou. 2019. Interpretation of neural networks is fragile. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 33. 3681–3688.
- [18] Juyeon Heo, Sunghwan Joo, and Taesup Moon. 2019. Fooling Neural Network Interpretations via Adversarial Model Manipulation. *CoRR* abs/1902.02041 (2019). arXiv:1902.02041 <http://arxiv.org/abs/1902.02041>
- [19] Sarthak Jain and Byron C Wallace. 2019. Attention is not explanation. *arXiv preprint arXiv:1902.10186* (2019).
- [20] Corey Kereluk, Bob L Sturm, and Jan Larsen. 2015. Deep learning and music adversaries. *IEEE Transactions on Multimedia* 17, 11 (2015), 2059–2071.
- [21] Been Kim, Martin Wattenberg, Justin Gilmer, Carrie Cai, James Wexler, Fernanda Viégas, et al. 2018. Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (tcav). In *International conference on machine learning*. PMLR, 2668–2677.
- [22] Pieter-Jan Kindermans, Sara Hooker, Julius Adebayo, Maximilian Alber, Kristof T Schütt, Sven Dähne, Dumitru Erhan, and Been Kim. 2017. The (un)reliability of saliency methods. *arXiv preprint arXiv:1711.00867* (2017).
- [23] Aditya Kuppa and Nhien-An Le-Khac. 2020. Black Box Attacks on Explainable Artificial Intelligence (XAI) methods in Cyber Security. In *2020 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 1–8.
- [24] Himabindu Lakkaraju and Osbert Bastani. 2020. "How do I fool you?" Manipulating User Trust via Misleading Black Box Explanations. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. 79–85.
- [25] Erwan Le Merrer and Gilles Trédan. 2020. Remote explainability faces the bouncer problem. *Nature Machine Intelligence* 2, 9 (2020), 529–539.
- [26] Zachary C Lipton. 2018. The mythos of model interpretability. *Queue* 16, 3 (2018), 31–57.
- [27] Scott M Lundberg and Su-In Lee. 2017. A unified approach to interpreting model predictions. In *Advances in neural information processing systems*. 4765–4774.
- [28] W James Murdoch, Chandan Singh, Karl Kumbier, Reza Abbasi-Asl, and Bin Yu. 2019. Definitions, methods, and applications in interpretable machine learning. *Proceedings of the National Academy of Sciences* 116, 44 (2019), 22071–22080.
- [29] Anh Nguyen, Jeff Clune, Yoshua Bengio, Alexey Dosovitskiy, and Jason Yosinski. 2017. Plug & play generative networks: Conditional iterative generation of images in latent space. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 4467–4477.
- [30] Thai-Son Nguyen, Sebastian Stuerker, and Alex Waibel. 2020. Super-Human Performance in Online Low-latency Recognition of Conversational Speech. *arXiv preprint arXiv:2010.03449* (2020).
- [31] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 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*. 1135–1144.
- [32] Robin Ruede, Verena Heusser, Lukas Frank, Alina Roitberg, Monica Haurilet, and Rainer Stiefelhagen. 2020. Multi-Task Learning for Calorie Prediction on a Novel Large-Scale Recipe Dataset Enriched with Nutritional Information. *arXiv preprint arXiv:2011.01082* (2020).
- [33] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei. 2015. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision (IJCV)* 115, 3 (2015), 211–252. <https://doi.org/10.1007/s11263-015-0816-y>
- [34] Wojciech Samek, Alexander Binder, Grégoire Montavon, Sebastian Lapuschkin, and Klaus-Robert Müller. 2016. Evaluating the visualization of what a deep neural network has learned. *IEEE transactions on neural networks and learning systems* 28, 11 (2016), 2660–2673.
- [35] Wojciech Samek, Grégoire Montavon, Andrea Vedaldi, Lars Kai Hansen, and Klaus-Robert Müller. 2019. *Explainable AI: interpreting, explaining and visualizing deep learning*. Vol. 11700. Springer Nature.
- [36] Ramprasaath R Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. 2017. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *Proceedings of the IEEE international conference on computer vision*. 618–626.
- [37] Avanti Shrikumar, Peyton Greenside, and Anshul Kundaje. 2017. Learning important features through propagating activation differences. *arXiv preprint arXiv:1704.02685* (2017).
- [38] Karen Simonyan, Andrea Vedaldi, and Andrew Zisserman. 2013. Deep inside convolutional networks: Visualising image classification models and saliency maps. *arXiv preprint arXiv:1312.6034* (2013).
- [39] Dylan Slack, Sophie Hilgard, Emily Jia, Sameer Singh, and Himabindu Lakkaraju. 2020. Fooling LIME and SHAP: Adversarial Attacks on Post hoc Explanation Methods. In *AAAI/ACM Conference on AI, Ethics, and Society (AIES)*.
- [40] Daniel Smilkov, Nikhil Thorat, Been Kim, Fernanda Viégas, and Martin Wattenberg. 2017. Smoothgrad: removing noise by adding noise. *arXiv preprint arXiv:1706.03825* (2017).
- [41] Charles Spearman. 1961. The proof and measurement of association between two things. (1961).
- [42] Akshayvarun Subramanya, Vipin Pillai, and Hamed Pirsiavash. 2019. Fooling network interpretation in image classification. In *Proceedings of the IEEE International Conference on Computer Vision*. 2020–2029.
- [43] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jon Shlens, and Zbigniew Wojna. 2016. Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2818–2826.
- [44] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2014. Intriguing properties of neural networks. In *International Conference on Learning Representations*. <http://arxiv.org/abs/1312.6199>
- [45] Alexander Warnecke, Daniel Arp, Christian Wressnegger, and Konrad Rieck. 2020. Evaluating explanation methods for deep learning in security. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 158–174.
- [46] Leanne S Whitmore, Ante George, and Corey M Hudson. 2016. Mapping chemical performance on molecular structures using locally interpretable explanations. *arXiv preprint arXiv:1611.07443* (2016).
- [47] Kai Xiao, Logan Engstrom, Andrew Ilyas, and Aleksander Madry. 2020. Noise or signal: The role of image backgrounds in object recognition. *arXiv preprint arXiv:2006.09994* (2020).
- [48] Jason Yosinski, Jeff Clune, Anh Nguyen, Thomas Fuchs, and Hod Lipson. 2015. Understanding neural networks through deep visualization. *arXiv preprint arXiv:1506.06579* (2015).
- [49] Matthew D Zeiler and Rob Fergus. 2014. Visualizing and understanding convolutional networks. In *European conference on computer vision*. Springer, 818–833.
- [50] Xinyang Zhang, Ningfei Wang, Hua Shen, Shouling Ji, Xiapu Luo, and Ting Wang. 2020. Interpretable deep learning under fire. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*.