

SentiNet: Detecting Localized Universal Attacks Against Deep Learning Systems

Edward Chou
Stanford University

Florian Tramèr
Stanford University

Giancarlo Pellegrino
CISPA Helmholtz Center for Information Security

Abstract—SentiNet is a novel detection framework for *localized universal attacks* on neural networks. These attacks restrict adversarial noise to contiguous portions of an image and are reusable with different images—constraints that prove useful for generating physically-realizable attacks. Unlike most other works on adversarial detection, SentiNet does not require training a model or preknowledge of an attack prior to detection. Our approach is appealing due to the large number of possible mechanisms and attack-vectors that an attack-specific defense would have to consider. By leveraging the neural network’s susceptibility to attacks and by using techniques from model interpretability and object detection as detection mechanisms, SentiNet turns a weakness of a model into a strength. We demonstrate the effectiveness of SentiNet on three different attacks—i.e., data poisoning attacks, trojaned networks, and adversarial patches (including physically realizable attacks)—and show that our defense is able to achieve very competitive performance metrics for all three threats. Finally, we show that SentiNet is robust against strong adaptive adversaries, who build adversarial patches that specifically target the components of SentiNet’s architecture.

I. INTRODUCTION

Deep neural networks are susceptible to a variety of attacks aimed at causing misclassifications [51], [21], [5]. As deep learning models are also often re-used (e.g., via transfer learning [4]), model vulnerabilities—whether inherent or purposefully inserted by a malicious party [34]—can easily affect a large number of systems. This has severe implications for the trustworthiness of deep learning models in security-critical decision-making situations. Defending against these attacks is challenging due to the wide variety of possible attack mechanisms and vectors, especially for models operating in the visual domain. In this work, we explore *localized* and *universal* attacks on visual classifiers and introduce SentiNet, a robust defense which detects adversarial inputs without requiring any specific model re-training or prior knowledge of the attack vector.

We focus on attacks that are *localized*, i.e., the adversarial region is constrained to a small contiguous portion of an image, and *universal*, i.e., attacks are image-agnostic. Inputs with these properties have proven useful for instantiating robust and physically realizable attacks that take the form of an adversarial object or sticker placed inside a visual scene [5], [34], [14], [15]. These classes of attacks typically use *unbounded* perturbations (i.e., without any specific ℓ_∞ or ℓ_2 constraint as in most digital attacks [51], [21]), to ensure that the attacks are robust to changes in viewpoint, lighting and other physical artifacts. Several such physical attacks have been demonstrated, with the goal of causing misclassifications

when applied to arbitrary images with different class labels [5], [34]. A drawback of localized attacks is that they are generally visible and detectable by the human eye, but there are many situations where attacks can be deployed in autonomous settings or carefully disguised [5].

A prospective defender must first consider that the model being protected may have been compromised prior to being deployed. An attack can originate from the source of the network provider, as in the case with data poisoning attacks [23], or can be intercepted and modified, as with trojaning attacks [34]. Even if a network is integrity protected, adversaries can still generate localized and universal attacks that will affect the model at test time, via adversarial examples [5]. Altogether, this creates an extremely difficult security setting where vulnerabilities are easily distributed, where adversaries target properties inherent to neural network systems that cannot be removed, and where attacks might be too diverse in appearance for a signature-based scheme.

Our goal is to create a defense against localized universal attacks that is attack-vector agnostic. To this end, we identify unifying and necessary features of successful localized universal attacks—including physically realizable attacks—and develop SentiNet, a novel technique that exploits these attack behaviors to detect them. We start from the observation that localized universal attacks are designed to be robust to a variety of artifacts while generalizing to a large distribution of inputs (e.g., the adversarial patch of [5] is designed to work when applied to *any* input image). Our first insight is that a localized universal attacks’ success relies on the use of “salient” features that strongly affect the model’s classification on many different inputs. We thus consider techniques from *model interpretability* and *object detection* to discover highly salient contiguous regions of an input image. As we show, these techniques uncover adversarial image regions, as well as benign ones that strongly affect classification. In a second step, we exploit the strong robustness and generalization properties of malicious regions to distinguish them from benign regions with high saliency. Specifically, we overlay extracted regions on a large number of held-out clean images and test how often this results in a misclassification. Malicious regions are much more likely than benign regions to generate misclassifications and are thus detected by SentiNet. As we show in our evaluation of SentiNet, mounting an attack that evades detection requires lowering an adversarial region’s saliency to a point where the region is no longer universal (i.e., it fails with high probability on random inputs)—even for a adaptive adversary with knowledge of SentiNet’s architecture. We also validate SentiNet’s effectiveness in a realistic physical setting, where it

successfully detects a printed adversarial patch [5] with high reliability.

a) Contributions: To summarize, this paper makes the following contributions:

- We propose SentiNet, a new architecture that protects a neural network by using the same model to detect localized universal attacks.
- To the best of our knowledge, SentiNet is the first architecture that does not rely on prior knowledge of the specific attack vector used to carry the attack, e.g., trojaned networks, poisoned networks, and adversarial patches—including physically realizable attacks.
- SentiNet uses a novel approach to detect a potential attack region using techniques developed for model visualization and object detection and feeds the attack deployed on multiple test images back to the network to perform attack classification.
- We evaluate SentiNet to protect pre-existing compromised and uncompromised networks against three known attack vectors, i.e., backdoors for poisoned networks, triggers for trojaned networks, and adversarial patches for uncompromised networks. We show that SentiNet can protect neural networks successfully, with an average true positive rate of 96.22% and an average true negative rate of 95.36%.
- We further evaluate SentiNet against a fully adaptive white-box adversary and present seven attacks against SentiNet’s core components. We show that SentiNet is resistant against strong adversaries by demonstrating the robustness of each individual component.

b) Paper Organization: In Section II, we present the architecture of deep learning systems and SentiNet’s threat model. Then, in Section III, we present SentiNet and its architecture. In Section IV, we evaluate SentiNet against localized universal attacks taken from the literature, as well as against physically printed adversarial patches. In Section V, we assess SentiNet against adaptive attackers trying to fool SentiNet’s internal components. Next, in Section VI, we discuss our results. Finally, in Section VII, we cover related works, and in Section VIII, we provide our conclusions.

II. BACKGROUND

A. Deep Learning Systems

Deep learning (DL) is a branch of machine learning which focuses on multi-layered artificial neural networks [33]. A neural network can be defined as a standard machine learning function f_m , which given an input x returns a prediction y and prediction-confidence $conf$; i.e. $(y, conf) = f_m(x)$. Convolutional Neural Networks (CNN) [32] are a specific architecture of neural network primarily targeted at computer vision tasks. Common CNN architectures include VGG-16 [49], ResNets [24] and Inception models [50].

DL systems are computer systems that rely on neural networks to perform specific tasks. At its essence, a DL system takes in an input, computes an output value, and makes a prediction based on the output. The analysis performed by a

DL system is often a classification task such as a face-based user authentication mechanisms, voice recognition, or voice-to-text system. Recently, DL systems have been proposed for autonomous vehicles and digital assistants [57].

B. Threat Model

In this work, we assume a scenario where a DL system uses a pre-trained deep CNN model to classify sensor data. Within this scenario, the goal of the adversary is to hijack the prediction of the model by providing a malicious image to the CNN model. In Section II-B1, we present the properties of the malicious inputs considered in this paper, and in Section II-B2, we present existing techniques to mount the attacks. Additionally, we assume an adversary that is aware of the defense mechanisms, and that can generate malicious images to bypass SentiNet. In Section II-B1, we present such an adversary.

1) Localized Universal Attacks: The goal of the adversary is to hijack the prediction of the model to gain control of the actions performed by the DL system. To achieve this goal, the adversary can craft a malicious object and place it in the input image, e.g., inside the visual scene of the sensors. The malicious objects considered in this paper are *localized*, i.e., the object is constrained to a small contiguous region of the image. The objects of this paper are also *universal*, i.e., the object is created once and reused many times with different input images. Figure 1 shows three examples of universal, localized malicious objects.

2) Attack Vectors: The adversary can construct and use malicious objects in different ways, that we review in this section. For example, the adversary can “alter” the behavior of the network to respond to a malicious object before its deployment in a DL system. Examples of these attacks are trojaning [28], [34] or poisoning attacks [23]. Alternatively, the adversary can also cause misclassifications to uncompromised models by crafting ad-hoc malicious object, e.g., adversarial patches [48], [31], [5], [14], [15], [3].

a) Compromised Models: One way to mount localized universal attacks is to compromise the network before deployment, by establishing a strong response between a class and a malicious object. Over the past few years, two attack vectors have emerged, i.e., data poisoning attacks and trojaning attacks. In a data poisoning attack, the adversary compromises the network at training time by inserting malicious inputs, i.e., benign images with malicious objects called *backdoors* (see Figure 1b), in the training set [23]. In a model trojaning attack, the adversary compromises the network by modifying the weights of selected neurons to respond to a specific *trojan trigger* [28], [34] (see Figure 1a).

b) Vulnerabilities of Uncompromised Models: Even if the networks are integrity protected, an adversary can hijack models’ predictions by exploiting the inherent instability of neural networks when processing maliciously-crafted inputs. Recent works have shown that adversaries can create localized universal malicious objects, e.g., printed patches [48], [5], [15], [14] or 3D objects [3] (see, e.g., Figure 1c), that can fool a model under real-world conditions such as lighting, sensor noise, and rotation.



Fig. 1: Examples of localized universal attacks. (a) Trojan trigger for trojaned VGG-16 model for face recognition [34]. (b) Backdoor for poisoned Faster-RCCN for road signs detection [23]. (c) Adversarial patch for uncompromised VGG-16 for ImageNet [5].

3) Adaptive Adversary: Over the past years, many ideas have been proposed to protect neural networks from attacks. While some new ideas have moderately increased the robustness of neural networks (e.g., strong adversarial training [36]), many do not adequately protect networks against adversaries aware of the specific defense mechanism being used (see, e.g., [8], [2], [53]). Accordingly, in this paper, we assume a strong white-box adversary that is fully aware of SentiNet, its architecture and mechanisms.

III. SENTINET

In this section, we present SentiNet. The goal of SentiNet is to identify adversarial inputs that will hijack the prediction of the neural network without assuming the knowledge of the attack vector beforehand, e.g., exploiting vulnerabilities of compromised and uncompromised networks. The core insight of SentiNet is to use the very behavior of adversarial misclassification to detect an attack.

The architecture of SentiNet is shown in Figure 2. First, SentiNet uses techniques from model interpretability and object detection to extract from an input scene x those regions that most highly influence the model prediction y (Section III-A). These regions likely contain the malicious object (if present) as well as benign salient regions. Then, SentiNet applies these extracted regions on a set of benign test inputs and observes the behavior of the model. Finally, SentiNet compares the synthetic behaviors with the known behavior of the model on benign inputs, to detect prediction hijacking (Section III-B).

A. Adversarial Object Localization

The first phase of our approach intends to localize on the given input the regions that might contain malicious objects. The idea is to identify the parts of the input x that contribute to the model prediction y . Because the attack is small and localized, we can hope to recover the true class of input x if we evaluate the model on a segmented input that contains no part of the attack. In the following, we look into the details of this phase. First, we present a segmentation-based approach to propose classes (see Figure 2.a). Then, starting from proposed classes and the given input, we generate a mask for x that may contain the malicious object (see Figure 2.b).

1) Class Proposal via Segmentation: The detection of the attack begins with the identification of a set of possible classes that may be predicted by the model f_m . The first of such classes is the actual prediction, i.e., $y = f_m(x)$. The other classes are identified by segmenting the input x and then evaluating the network on each segment. Algorithm 1 shows the algorithm to propose classes via input segmentation. Different approaches can be used to segment a given input x including sliding windows and network-based region proposals [45]. In our approach, we use the selective search image segmentation algorithm [55]. Selective search generates an exhaustive list of region proposals based on the patterns and edges found in natural scenes [55]. Then, we evaluate each proposed segment, i.e., $f(x_p)$, and return the k most confident predictions, where k is a configuration parameter of SentiNet. We exclude the primary class $y = f_m(x)$ from our choice of k classes. A general guideline towards selecting k is to set it to be slightly higher than the amount of classes that are present in the dataset per-image. In our case, Imagenet [13] has around 1.5 classes per image, and we set k to 2.

Algorithm 1: ClassProposal

```

in :  $f_m$  – model;
       $x$  – input of  $f_m$ ;
       $y$  – primary class, i.e.,  $y = f_m(x)$ ;
       $k$  – propositions
out :  $C$  - set of proposed classes and confidence ( $|C| = k$ )
1  $P = \text{SelectiveSearch}(x)$ ;
2  $C = \{(y_p, \text{conf}_p) : \forall x_p \in P, (y_p, \text{conf}_p) = f_m(x_p) \wedge y_p \neq y\}$ ;
3  $C = \text{TopConf}(C, k)$ ;
4 return  $C$ 

```

2) Mask Generation: Once the class proposal C is obtained, the second step of SentiNet consists of identifying the regions of x that most highly influence the predictions C . To find these regions, we resort to techniques to explain and interpret model predictions.

A particularly suitable approach for our goal is Grad-CAM [11], a model-interpretation technique that identifies contiguous spatial regions of an input without requiring modifications to the original model. At a high level, Grad-CAM uses gradients computed in the final layers of a network to calculate the saliency of input regions. For class c , Grad-CAM calculates the gradients of the model’s output y^c (the model’s *logit* score for class c) with respect to each of the

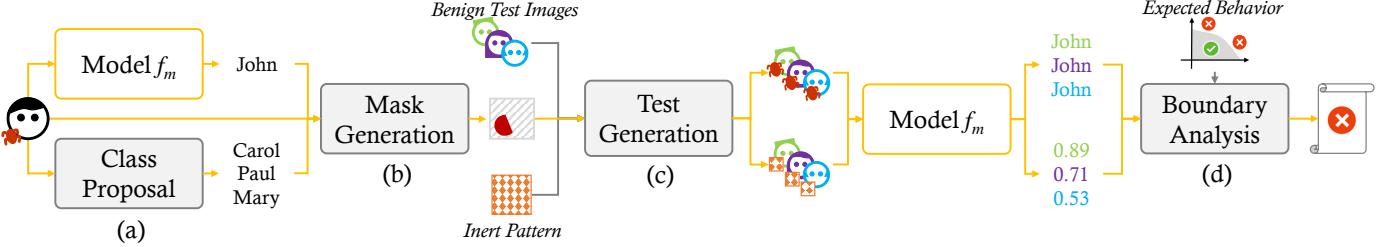


Fig. 2: Overview of the SentiNet architecture to protect a model f_m . The output and class proposals of an input are used to generate masks and image tests, which are then fed back into f_m to generate values for boundary analysis and attack classification.

k feature maps A^k of the model's final pooling layer to obtain $\frac{\delta y^c}{\delta A^k}$. The mean gradient value of each filter map, or “neuron importance weight”, is denoted $\alpha_c^k := \frac{1}{Z} \sum_i \sum_j \frac{\delta y^c}{\delta A^k}$. Finally, the feature maps A^k are weighted by their neuron importance and aggregated to obtain the final Grad-CAM output: $L_{Grad-CAM}^c := \text{ReLU}(\sum_k \alpha_c^k A^k)$. Here, $\text{ReLU}(x) = \max(x, 0)$ is the ReLU activation function [18] which retains only the positive gradient signals for class c . The output of Grad-CAM is a coarse heatmap of the positive importance of the image, usually at a lower resolution than the input image due to downsampling in the model's convolutional and pooling layers. Finally, masks are produced by binarizing the heatmap with a threshold of 15% of max intensity. We use this mask to segment salient regions for the next steps.

use these additional heatmaps to generate secondary masks to improve the original mask for the prediction y by subtracting common regions. This results in a set of masks that highlight only the localized attack and not the other salient regions in the image.

Algorithm 2: MaskGeneration

```

in :  $f_m$  – model;
       $x$  – input for  $f_m$ ;
       $y, conf$  – model prediction on  $x$ ;
       $C$  – proposed classes
out :  $M$  - masks for candidate regions with the malicious object
1  $mask_y = \text{MaskGradCAM}(f_m, x, y)$ ;
2  $M = \{(mask_y - \text{MaskGradCAM}(f_m, x, y_p), conf_p)$ 
   :  $(y_p, conf_p) \in C\}$ ;
3 return  $\{mask_y\} \cup M$ 
```

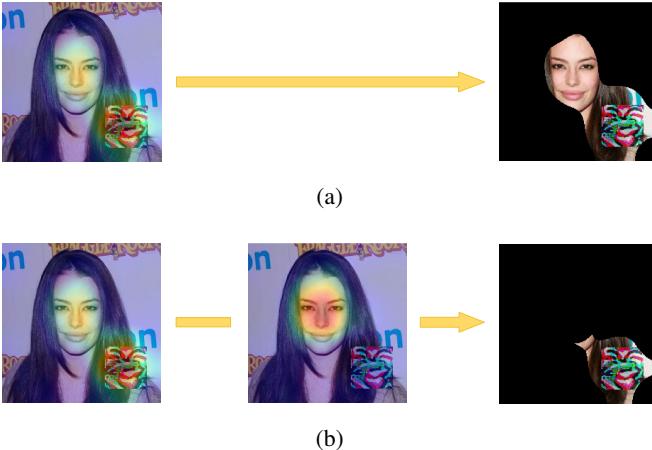


Fig. 3: Differential mask generation to remove ambiguous areas. (a) Example of Grad-CAM mask using prediction y covering benign areas. (b) Example of precise mask by removing masks of class proposals C .

We generate masks with Grad-CAM as shown in Algorithm 2. We start by extracting the mask using Grad-CAM for the input x and prediction y . As Grad-CAM can identify salient areas for benign classes, the resulting mask may span over both benign and malicious regions. An illustrative example is in Figure 3, where the Grad-CAM generated heatmap for a facial recognition network covers both a trojan trigger patch but also the original face. To improve the accuracy of the mask, we also extract a mask for each proposed class y_p . Then, we

B. Attack Detection

Once we identified regions M of the inputs x that may be containing malicious inputs, we test the model f_m to determine whether any of the regions can hijack the expected predictions of a set of benign test inputs.

1) Test Generation: Once an input region is localized, SentiNet observes the effects the region has on the model to determine whether the region is adversarial or benign. To do so, SentiNet overlays the suspected region on a set of benign test images X , which are often shipped together with deployed models. Test images X are fed back into the network, where the number of fooled examples are counted and used for adversarial images. Intuitively, the higher the number of mutated images can fool the model, the more likely the suspected region is an adversarial attack.

When the recovered region is small, this technique is effective at distinguishing adversarial and benign inputs, as small benign objects cannot typically overwhelm a networks prediction. However, one problem of this approach is that a region (whether adversarial or benign) that covers a larger fraction of the input image will likely cause misclassifications when overlaid onto most other images because they occlude the original object.

To measure the extent to which an overlaid region causes misclassifications simply by occluding the original object, rather than by virtue of highly-salient features, we perform a second test where we replace the content of the overlaid region with an inert pattern of low saliency (e.g., Gaussian

noise). We expect that adversarial regions will cause many misclassifications when overlaid on the test set, but have little effect on the network when replaced by an inert pattern before being overlaid. In contrast, we expect benign patterns to either cause few misclassifications, or to occlude objects and thus also disrupt the model when replaced by inert patterns. Algorithm 3 shows the algorithm we use to test extracted regions. For each region, we check how many overlaid test images fooled the network, and how confident the model is when classifying images overlaid with inert patterns.

Algorithm 3: Testing

```

in :  $f_m$  – model;
       $x$  – input for  $f_m$ ;
       $y$  – class of  $x$ ;
       $M$  – proposed masks;
       $X$  – benign test images;
out:  $Fooled$ ,  $AvgConf$ 
1  $R = \{x * mask : mask \in M\}$ ;
2  $IP = \text{InertPattern}(M)$ ;
3  $X_R = \text{Overlay}(X, R)$ ;
4  $X_{IP} = \text{Overlay}(X, IP)$ ;
5  $fooled_{y_R} = 0$ ,  $avgconf_{IP} = 0$ ;
6 for  $x_R, x_{IP} \in X_R, X_{IP}$  do
7    $(y_R, conf_R), (y_{IP}, conf_{IP}) = f(x_R), f(x_{IP})$ ;
8   if  $y_R == y$  then
9      $fooled_{y_R} += 1$ 
10   $avgconf_{IP} += conf_{IP}$ 
11  $avgconf_{IP} = \frac{avgconf_{IP}}{|X|}$ ;
12 return  $fooled_{y_R}$ ,  $avgconf_{IP}$ ;

```

2) *Decision Boundary for Detection*: With these two metrics (number of images fooled and average inert pattern confidence values) we can determine whether an input x is adversarial. A naive approach is to use thresholding based rules, but it is hard to determine how to set the thresholds and which metric holds more importance. Instead, we use metrics collected on clean examples to train a simple two-feature one-class classifier and classify outliers as adversarial.

We examine this problem by plotting metrics from an example task in a 2D plot in Figure 4, where the red triangular dots represent adversarial examples and the blue circular dots represent clean examples. We observe that the adversarial and clean points can be easily separated using a parabolic function, suggesting that a classifier approach such as linear regression or support vector machine could be used. However, this would operate under the false assumption that we have prior examples of adversarial inputs. Ideally, we want to create a technique that would allow us to identify an unseen adversarial input as an attack based on the attack-agnostic metrics.

We notice a general pattern where adversarial examples are usually clustered near the top-right of the plot. Because adversarial examples are designed to cause misclassifications when applied to other images and not overly obstruct the other important regions of an image, it makes sense that both the number of images fooled and the average noisy confidence metrics of an adversarial example would be high. We can use our set of benign test images to generate statistics of

the metrics of normal examples, which will then allow us to formulate when an input is abnormally adversarial.

We can use our collected metrics on clean examples to approximate a curve. By taking the points most likely to be the bounds of the statistics of our examples, we can approximate a curve where points lying outside our curve function can be classified as attacks. We collect our points by taking the points with the highest y -values for x -intervals, and then using a non-linear least squares function to approximate our curve. We then use our approximated curve to set classify attacks by calculating the distance between a curve and a point — using the Constrained Optimization by Linear Approximation (COBYLA) method [52]—and determining whether that distance is within a threshold estimated by the distances of clean examples lying outside the curve.

Algorithm 4: DecisionBoundary

```

in :  $B$  – sampled behavior of  $f_m$ 
out:  $f_{curve}$  – approximated curve function;
       $d$  – acceptable distance from  $f_{curve}$ 
1  $f_{curve} = \text{ApproximateCurve}(\text{OutPts}(B))$ ;
2  $avgd = 0$ ;
3 for  $(x, y) \in B$  do
4   if  $f_{curve}(x) > y$  then
5      $avgd += \text{COBYLA}((y, x), f_{curve})$ ;
6  $d = \frac{avgd}{|B|}$ ;
7 return  $f_{curve}, d$ ;

```

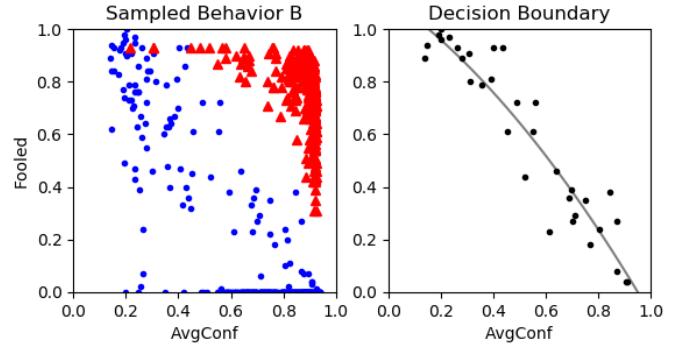


Fig. 4: Example of boundary detection for the trojaned experiments using 400 data points and random noise as inert pattern. On the left, the adversarial and benign metrics are plotted as red triangles and blue circles respectively; on the right, we plot the curve proposal from the sampled points, i.e., the benign test images X .

IV. EVALUATION

In this section, we evaluate SentiNet on a variety of previously proposed attacks, to highlight its versatility. In Section V, we then perform an extensive evaluation against *adaptive* adversaries with full knowledge of SentiNet’s inner workings—thereby demonstrating SentiNet’s robustness.

After presenting the experiment setup in Section IV-A, in Section IV-B, we evaluate the effectiveness of SentiNet in

protecting networks from three known attacks, i.e., adversarial patches, trojan triggers, and backdoors, with an average true positive rate of 96.22% and an average true negative rate of 95.36%. We further evaluate SentiNet in a realistic physical setting with a printed adversarial patch (see Section IV-C).

Finally, in Section IV-D, we look into the latency of SentiNet in terms of runtime analysis.

A. General Experiment Settings

We evaluated SentiNet when protecting three publicly available networks shared from prior works. Two of the selected networks are compromised and one is uncompromised. The compromised networks are a backdoored Faster-RCNN network for reading signs detection by Gu et al. [23] and a VGG-16 trojaned network for facial recognition by Liu et al. [34]. The uncompromised network is a VGG-16 network trained on the Imagenet dataset by Simonyan et al. [49]. Additionally, to operate, SentiNet requires a benign test image set X and an inert pattern s to generate the decision boundary as shown in Section III-B. We present the generation of each test set X for the selected networks in Section IV-B. Unless specified, we use random noise for our inert pattern s .

We measure the effectiveness and robustness of SentiNet in terms of accuracy and performance, collecting the TP/TN and FP/FN rates of SentiNet when processing benign and adversarial inputs. We present the creation of benign and adversarial images datasets of our experiments in Section IV-B. We measure efficiency by evaluating the execution of each step of SentiNet.

Finally, SentiNet uses Tensorflow 1.5 to generate the adversarial patches for the uncompromised network, BLVC-Caffe for the trojaned network, and Faster-RCNN Caffe [17] for the poisoned network. To parallelize the class proposal, SentiNet relies on the ROI pooling layer as implemented by the Fast-RCNN Caffe version. Finally, SentiNet uses the off-the-shelf implementations of Grad-CAM [46] and selective search [55].

B. Effectiveness

The first part of our evaluation assesses the effectiveness of SentiNet in protecting our selected networks against three attacks, i.e., trojan triggers [34] against trojaned networks, backdoors [23] against poisoned networks, and adversarial patches [5] against uncompromised models. For each attack, we measured the effectiveness of SentiNet in terms of the number of attacks detected. For the adversarial patches attack, we considered an additional variant where the attacker uses multiple patches at the same time. The summary of this evaluation is in Table I.

1) Trojaned Networks: A trojaned network is a model whose weights have been modified by an adversary to implant a response when processing inputs containing a so-called *trigger trojan* [34]. The trigger trojan is created from a set of specified neurons, and then fine-tunes the model's weights on the trigger to hijack the prediction [34]. For our evaluation, we selected the facial recognition model shared by Liu et al. [34] with a VGG-16 architecture [49] trained on the VGG-Face dataset [41].

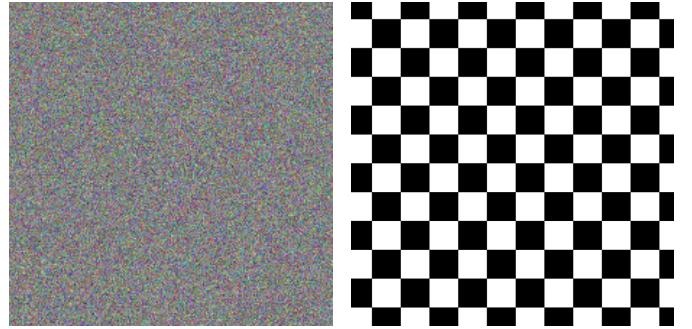


Fig. 5: Examples of inert patterns. The default pattern we use for s is random noise shown on the left. Another pattern we can potentially use is the checkered pattern on the right which the VGG-Face network also responds weakly to.

a) Datasets: For the evaluation, we created three datasets with benign, adversarial, and test images as follows. The benign images dataset contains 400 images randomly selected from the LFW dataset [27]. From the benign dataset, we derived the adversarial inputs dataset by placing the square trigger trojan shared by Liu et al. [34] to hijack the prediction of the VGG-16 network to the class “A.J. Buckley”. As the trigger trojan is created from a fixed region of the input, we placed them in the same position, i.e., the bottom-right corner of each image. An example of such a trigger trojan and adversarial input is shown in Figure 6a. Then, the test set X contains 100 randomly selected images from the VGG-16 dataset [49]. Finally, in this evaluation, we considered two types of inert noise, i.e., random noise and checker pattern (Examples of the two types of inert noise are in Figure 5).

b) Results: Of the 400 adversarial images, 368 of them hijack the prediction of the compromised model, i.e., the model incorrectly predicted “A.J. Buckley”. Of these 368 attacks, SentiNet can successfully detect almost all of them, i.e., 365 malicious inputs resulting in TP rates above 99%, regardless of the used inert noise. Then, the number of TN is also considerably high, with rates above 99%. In this case, the inert noise has a very marginal role in the detection. Of the 400 benign images, we have one FN when using the random inert noise and two FNs when using the checker inert noise.

To better understand the behavior of SentiNet, we have a closer look at the distribution of the benign and adversarial images with respect to the decision boundary used by SentiNet. The plot is shown in Figure 6a. As expected, most of the benign samples (in blue) fail to fool the model except for few outliers which produce low *avgConf* scores. On the contrary, the adversarial inputs (in red) fool the model a high number of times with a very high *avgConf* confidence scores. The decision boundary is calculated using the test set X as explained in Section III-B, and it is well separating the adversarial from benign regions.

2) Poisoned Networks: A poisoned network is a model created by an adversary via training, with the goal to implant a specific model response when processing inputs containing a *backdoor*. As opposed to trojaned networks, poisoned networks are compromised *during* the training phase instead of after. For our evaluation, we selected the poisoned network shared

TABLE I: Effectiveness of SentiNet protecting compromised and uncompromised networks.

Network and Task	Attack	Inert Noise	TP	TN	FP	FN
VGG-16 [34] for face recognition	Trojan trigger	Random	99.2%	99.8%	0.3%	0.8%
VGG-16 [34] for face recognition	Trojan trigger	Checker	99.2%	99.5%	0.5%	0.8%
Faster-RCNN [23] for road signs detection	Backdoor	Random	85.0%	86.9%	13.1%	14.8%
VGG-16 [49] for ImageNet	Adversarial patch	Random	98.5%	95.3%	4.8%	1.5%
VGG-16 [49] for ImageNet	2 × Adversarial patch	Random	99.2%	95.3%	4.8%	0.8%
VGG-16 [49] for ImageNet	Physical adversarial patch	Random	93.7%	90.2%	9.8%	6.3%

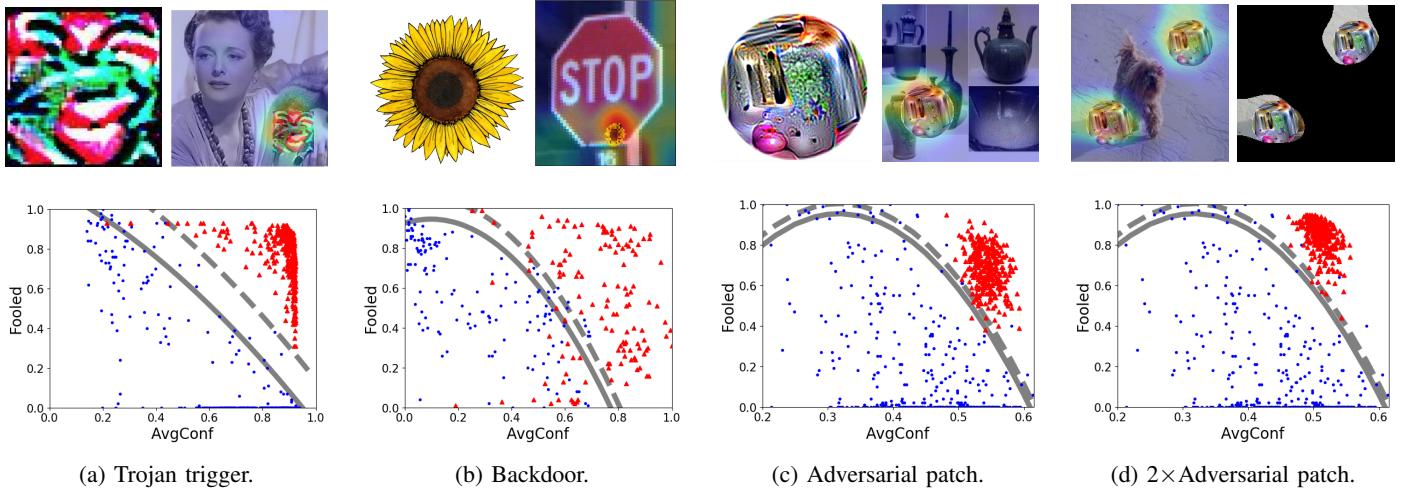


Fig. 6: Evaluation inputs and results. The first row shows examples of adversarial objects used by the attacker and the Grad-CAM output. The bottom row shows scattered plots of benign inputs (in blue) and adversarial inputs (in red) with respect to the decision boundaries (solid lines) and thresholds (dashed lines) used by SentiNet for the attack detection.

by Gu et al. [23], a Faster-RCNN model [45] to detect stop signs. The authors poisoned the training set so that the network will incorrectly classify stop signs with a yellow flower—the backdoor—as a warning sign. The backdoor and an example of adversarial input is shown in Figure 6b.

a) Datasets: For this evaluation, the benign images dataset contains 145 images of stop signs from the LISA dataset [38] by cropping out the images with their labeled bounding boxes. Then, we derived the adversarial images by placing the yellow flower backdoor shared by Gu et al. [23] at approximately below the “stop” text of each sign to create an “attack” dataset. The test set X contains 100 images selected from each class with equal probability.

b) Results: Out of the 145 adversarial inputs, 134 images successfully fool the Faster-RCNN model. SentiNet detected 114 images, with a TP rate of 85%. When using benign images, SentiNet incorrectly detected 19 images of 145 benign inputs, resulting in a 14.8% FNs. While SentiNet can achieve much higher accuracy and precision, we note that SentiNet’s accuracy in this experiment is comparable to the accuracy of proposed adversarial detection techniques (see, e.g., [6]).

Higher FP and FN rates of SentiNet can be better explained by having a look at the distribution of benign and adversarial images in Figure 6b. As opposed to trojaned networks, benign and adversarial images are not densely grouped. Instead, they are rather scattered over large areas, crossing the decision

boundary in two points, i.e., benign images above the boundary decision in the center of the plot and adversarial inputs below the boundary decision. Scattered points as shown in Figure 6b are likely due to coarser heatmaps generated by Grad-CAM when applied to the Faster-RCNN network. The Faster-RCNN architecture uses a 12×12 ROI pooling layer, whose layer is used by Grad-CAM to create the heatmap. The ROI pooling layer of the Faster-RCNN is smaller than the other networks used in our evaluation. For example, the VGG-16 trojaned network has a 16×16 ROI pooling layer. A smaller ROI pooling layer results in coarser grained heatmaps, whose masks are likely to include regions unrelated to the targeted class. As a result, test images with overlaid adversarial regions will include ambiguous features affecting both the probability of fooling the network and the confidence of the classification.

3) Uncompromised Networks: In this section, we evaluate SentiNet protecting an uncompromised network when processing adversarial patches. In our case, we use a VGG-16 [49] Imagenet-pretrained [13] network as our target network f_m .

a) Datasets: We randomly sampled 400 images from the Imagenet test set [13] to implement our attack. Then, we placed the patch at random positions on the 400 images to generate our dataset of adversarial images, occupying around 25% of the input images. We used the adversarial patch created by Brown et al. [5] which can fool the Imagenet-trained VGG-16 model to classify inputs as a “toaster”. The patch and an example of adversarial input is shown in Figure 6c. Also, in this evaluation, we considered a variant of the attack with

images containing multiple adversarial patches. Finally, our test set X consists of 100 randomly selected images from the Imagenet training set.

b) Results: Our evaluation showed that 338 images of the 400 adversarial images with a single patch fool the Imagenet-trained VGG-16. SentiNet detected almost all of them, i.e., 333 out of 338 with a TP rate above 98%. When using two patches, the adversary has a slightly higher advantage and can hijack the prediction 369 times over 400 attempts. Of these 369 attacks, SentiNet has a stronger response than single-patch attacks, detecting 368 attacks, with almost 100% TP rate.

In Figures 6c and 6d, we observe that the adversarial images (in red) points are skewed towards producing both higher *numFooled* and *avgConf* numbers. The classification rule generated by the decision boundary produces TN rates of ~95% as seen in Table I. Overall, both TP and FP compare favorably to other literature focused on adversarial attack detection.

Finally, when using two patches simultaneously, Grad-CAM correctly identifies the two disjoint regions that contribute to the prediction. Figure 6d shows both the heatmap and the mask generated by SentiNet. Additionally, we measured how often SentiNet can detect both patches by checking whether the generated masks are disjoint and cover substantial portions of both patches. We find that SentiNet discovers both patches 97.4% of the time, which we consider to be sufficiently accurate relative to the TP and TN values.

C. Physical Attacks

Localized adversarial attacks have the distinct advantage of being deployable in real-world settings as a physical attack via stickers or patches, as compared to adversarial noise. Several prior works [5], [48], [14], [15], [3] have demonstrated how adversarial noise can be effectively synthesized in the physical world to fool visual classifiers fed with video streams. In this section, we experimentally validate that SentiNet’s defensive capabilities perform well in a realistic attack scenario where a physically printed patch is displayed next to a common object, with the goal of robustly and reliably subverting a classifier’s predictions.

We captured a video of a banana displayed on its own or next to an adversarial patch [5] with a variety of positions and orientations (see Figure 7). The undefended VGG16 network classifies all 610 benign video frames correctly, and is always fooled by the patch when present in all other 541 frames. We evaluate SentiNet on these video frames using the same parameters as in our previous (digital) adversarial patch experiments—including the use of the randomly selected Imagenet test set and the checkerboard pattern for fuzzing. With SentiNet, the patch is correctly identified in 93.7% of the video frames, and the banana is correctly identified in 90.2% of benign frames.

Albeit not perfect, these results are promising: with SentiNet, the adversarial patch fails its goal of reliably subverting the classifiers on the vast majority of frames. In a deployment scenario where a classifier averages predictions over multiple frames (e.g., by yielding an object prediction every 10 frames,

via a majority vote over the preceding frames), SentiNet successfully yields correct classifications for the full benign video, while detecting and rejecting the adversarially perturbed video.

D. Runtime Analysis

Finally, we measured the latency of SentiNet when protecting a VGG-16 [49] architecture as a case study. All components—except for the selective search algorithm—are executed on a Tesla K-80 GPU. A single execution of SentiNet consists of a run of the selective search algorithm, the Grad-CAM, and a forward pass with a batch of test images. Using the off-the-shelf implementations, the runtime of selective search and Grad-CAM is 2 and 0.4 seconds respectively. The forward pass through the network takes about 2.5 seconds. However, we note that the forward pass runtime is greatly penalized by the overhead introduced by our PyCaffe implementation—a barebone forward pass of the VGG-16 is expected to take from 0.04 to 0.1 seconds [29]. With an expected worst-case execution runtime of 0.1 seconds, and that the forward pass runtime is independent of the batch size, the total latency introduced by SentiNet amounts to 2.5 seconds.

V. ADAPTIVE ATTACKS

Our previous analysis demonstrates SentiNet’s versatility in protecting neural networks from a variety of attacks. In this section, we evaluate the more challenging and realistic threat model of a fully adaptive white-box adversary [7] that is aware of the presence of SentiNet, of its architecture and its inner workings. Such an adversary can attempt to create adversarial objects that simultaneously fool the target network while also compromising the core components of SentiNet, i.e., the mask generation, the class proposal, and the attack detection. In Section V-A, we present attacks aimed at fooling the mask generation phase. Then, in Section V-B, we evaluate attacks against the class proposal. Finally, in Section V-C, we present attacks against the attack detection phase.

A. Attacking the Region Proposals

Our defense is reliant on successfully localizing the adversarial region in an image. In our current framework, this is done using the Grad-CAM algorithm, which generates a heatmap of the salient regions leading to a classification. If an attacker can disrupt the Grad-CAM mechanism and avoid successful detection and localization, the subsequent components of the pipeline will fail. We observe that the Grad-CAM mechanism uses network back-propagation to measure region importance. As this mechanism is differentiable, an adversary could generate targeted gradient perturbations to control the position and size of the heatmap. In this section, we consider three of these attacks: Grad-CAM perturbation, misdirection of the mask creation, and mask minimization. However, as the analysis of this section shows, while manipulating the heatmap is feasible in theory, in our defense context heatmap manipulation is ineffective in practice.

1) Perturbing Grad-CAM: Consider the adversarial image and its Grad-CAM heatmap in Figure 8a for the target class “toaster”. The heatmap in Figure 8a correctly identifies the area containing the patch. An adversary could try to

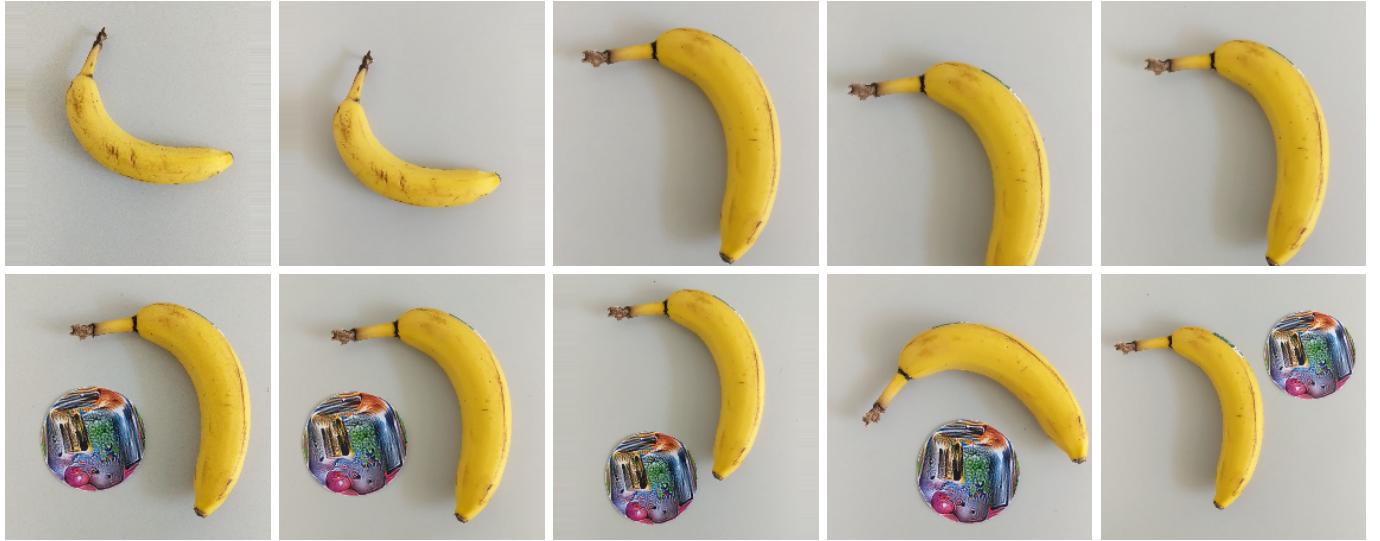


Fig. 7: 224x224 video frames without (top) and with (bottom) a physical adversarial patch used for our evaluation.

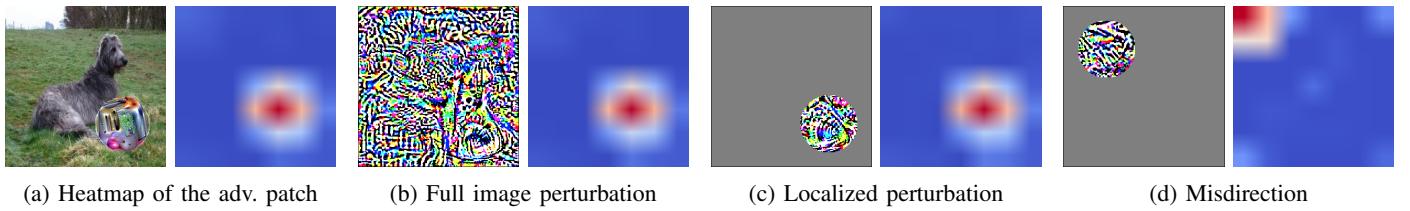


Fig. 8: Attacking region proposal. (a) The heatmap of the adversarial patch overlaid on an image of a dog. (b) Full-image perturbations can generate a visually identical heatmap. (c) Localized perturbation can generate the same heatmap of (a). (d) Localized perturbation fails to generate a similar heatmap.

generate a perturbation, i.e., an adversarial image, resulting in a visually identical heatmap. Such a perturbation can be created in practice as the Grad-CAM function $L_{GradCAM}^c = ReLU(\Sigma_k \alpha_c^k A^k)$ is differentiable, and the adversary can optimize an input on this function given a target class. For example, the adversary can use a standard Stochastic Gradient Descent Optimizer (SGD) on a VGG-16 network [49] to minimize a loss function calculated as the total difference between the current Grad-CAM output and the target Grad-CAM output, and iteratively add noise until the loss converges. An example of such a perturbation is shown in Figure 8b.

This attack shows that Grad-CAM outputs can be precisely manipulated through gradient optimization. However, such an attack requires to feed the network with a perturbation of the size of the input of the network being protected, which is not part of our threat model (Section II-B).

2) Heatmap Misdirection: In this attack, we consider an adversary who intends to create an input image that tricks SentiNet to detect the adversarial object in a different region where the adversarial object is located. Let us assume the adversary intends to convince SentiNet that the adversarial object is in the position as indicated by the heatmap of Figure 8a. As we demonstrated earlier, an adversary allowed to add perturbational noise to an entire image can generate a heatmap at the desired position. As we discussed before,

the adversary does not have full control of the whole image, rendering the attack infeasible. An attacker may try to generate a heatmap visually identical to the adversarial patch of Figure 8a by using a perturbation constrained to the same region. Figure 8c shows an example of such a perturbation obtained by modifying the loss function of the SGD to constrain the noise on the same region of interest. At this point, the adversary can try to generate a perturbation at a different location leaving the goal of the attack unchanged. An example of such an attempt is shown in Figure 8d. The perturbation is now on the top-left corner of the input image. However, the resulting heatmap is not shown in the desired position, i.e., bottom-right. Instead, the heatmap is positioned nearby the location of the perturbation, indicating that localized noise can only affect the corresponding Grad-CAM region.

3) Heatmap Minimization: An alternative strategy to fool SentiNet is to minimize the corresponding Grad-CAM region to the greatest extent possible to avoid detection. For example, the adversary can achieve that by modifying the loss function of SGD to optimize for minimal Grad-CAM output. The adversary can start from the adversarial patch image in Figure 9a and iteratively add perturbational noise to the region. Figure 9a, we show that as our loss converges, the Grad-CAM output is successfully minimized, avoiding detection of the patch.

Our analysis shows that heatmap minimization, i.e., fooling

SentiNet, is in tension with the attack success rate of the patch, i.e., fooling f_m . Figure 9a shows that as more noise is added to the patch, the success rate of the attack is reduced. This result suggests that Grad-CAM is capturing some inherent saliency of the region and cannot be minimized without reducing the attack effectiveness.

The tension between the two objectives could be solved by creating a perturbation that optimizes both for targeted misclassification and for heatmap minimization. Let us consider an adversary that attempts to jointly generate a patch for both criteria by optimizing both objectives during every iteration. Also, to better explore the role played by each objective, we introduce a weighting parameter $\alpha \in [0, 1]$ between the two objectives (i.e., the misclassification objective has weight α , and the heatmap minimization has weight $1 - \alpha$). To evaluate then attack, we generate 40 adversarial patches as described by Brown et al. [5] for a range of weighting values $\alpha \in [0, 1]$. For each patch, we select 100 images from the Imagenet test set [13] and apply the patch. In total, we generated 4,000 malicious images for each weighting ratio α . Then, we counted the patches that fool the model, the Grad-CAM¹, or both.

The results of our experiment are shown in Figure 9b. As patches work with slight variance, we averaged the attack result to give a better sense of how well a patch would perform. As can be seen in Figure 9b, there is an inverse relationship between the effectiveness of a patch in fooling f_m (in red) and the region proposal of SentiNet (dashed green), corroborating our previous findings. Additionally, we further plot the patches that successfully fulfill both criteria (in dashed purple), and find that the optimum value is where the ratios of successful misclassifications and hidden patches overlap, giving us patches that fulfill both criteria with an average success rate of 10%. This strongly suggests that minimizing the Grad-CAM output directly weakens the attack effectiveness and that it is difficult to optimize for both objectives jointly.

4) Results on Attacking Region Proposals: To summarize, in this section, we presented three attacks against the Grad-CAM algorithm. Our evaluation shows that, while the Grad-CAM output can be perturbed with localized perturbations, misdirecting the Grad-CAM heatmap seems an infeasible attack strategy. Also, our results show that minimizing the heatmap size dramatically reduces the effectiveness of the attack. Accordingly, we conclude that attacking the Grad-CAM algorithm may bring a very little advantage to an adversary.

B. Attacking the Class Proposal

Another approach to avoid the localization of the adversarial region is attacking the class proposal step. In this section, we discuss attacks exploiting the algorithms implemented in the class proposal step. In particular, we concentrate on two types of attacks where the adversary intends avoiding detection by generating masks without the adversarial region or weakening the detection by creating inefficient masks.

1) Mask Reduction with Specialized Patch Sub-regions: Instead of avoiding detection, the adversary may try to weaken the detection of the patch by reducing the size of the mask of

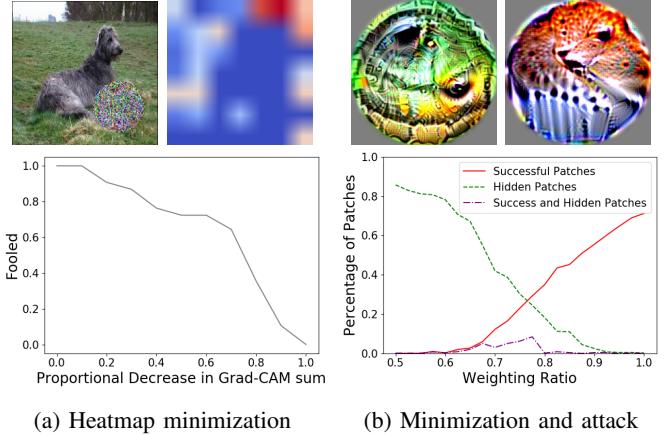


Fig. 9: Heatmap minimization attack. **(a)** Example of adversarial input minimizing the Grad-CAM output (top); Plot showing the tension between minimization and attack success. **(b)** Patches minimizing the heatmap and maximizing the attack success respectively (top); Plot of success of the patch vs. minimization of the heatmap.

the primary class. The goal of the class proposal is to identify additional classes in the input image to remove ambiguous areas (see Figure 3a-b). Here, the attacker may try tricking the class proposal into identifying classes in sub-regions of the patch. Such an attack results in a mask containing only a portion of the entire patch, thus weakening the response of the model at test time and the detection of the attack.

The creation of a localized universal patch exposing such behavior may be very challenging. Such a patch needs to have a region causing the activation of a class, say y' , and, at the same time, another region for the target class y . Also, to carry this attack, the patch should cause a change in the prediction of the model when the region for y' is missing. Building a localized universal patch with such a non-linear dependency between the two regions may be hard, if not unfeasible, and we hope other researchers will explore whether such a type of attack is possible.

2) Avoiding Mask Reduction by Over-Segmentation: Mask reduction removes from the primary mask areas that are ambiguous, resulting in more efficient masks. Instead of generating inefficient mask by removing malicious regions, the adversary may try to bypass the mask reduction and generate large, ineffective masks like the one shown in Figure 3a. To achieve such a goal, the adversary might attack the image segmentation algorithm, i.e., selective search [55], and trick the algorithm into returning many small segments outside of the malicious region. When processing small segments, the network may return predictions with low confidence which are ignored when generating the mask for the primary class (see TopConf(C, k) in Algorithm 1). As a result, the final mask will not be refined by removing the ambiguous areas thus weakening the response of the model at test time.

However, attacking the selective search algorithm may not be a feasible strategy. Our inspection of the selective search algorithm revealed that an adversary controlling a limited

¹We use a < 0.5 overlap ratio between the adversarial pixels and the Grad-CAM region.

region of the input image may not be able to influence the generation of a segment of arbitrary size and position. As a result, we believe that attacking the selective search algorithm may be unlikely.

3) Results on Attacking the Class Proposals: To summarize, in this section, we presented three attacks against the algorithms that propose a list of classes present in the image x . Our evaluation shows that the goal of avoiding the prediction of the primary class conflicts the goal to hijack the final prediction. Also, our analysis suggests that creating inefficient masks may be either remarkably challenging—if not infeasible—or even not possible. Accordingly, we conclude that attacking the class proposal step may bring little to no advantages to an adaptive adversary.

C. Attacking the Attack Classification

We now consider attacks aimed at fooling the decision procedure of SentiNet.

We now consider attacks aimed at fooling the decision procedure of SentiNet, where extracted regions or inert patterns are overlaid onto benign test images to measure their generalizability. One possible attack in the context of poisoned or trojaned networks has the adversary manipulate the model so that it recognizes the inert pattern as a member of a targeted class. This would let the attacker bypass our defense as adversarial patterns will remain adversarial when overlaid with the “inert” pattern. This attack does not apply to the setting where an adversary aims to evade an uncompromised network with adversarial patches. For the general case, we note that the choice of inert pattern can be made after the network has been trained, so one can test whether the chosen pattern affects the model. We also found that using patterns made up of various random patterns or noise (see Figure 5) produce good results, which further hinders a training-time adversary’s ability to target the specific pattern than will later be used at test-time. For example, in Table I, we can see that for the evaluation with the trojaned network, the TP and TN rates of the random noise pattern and checker pattern are within $\leq 0.25\%$.

VI. DISCUSSION

Our results show that our defense is able to record high accuracy metrics for detecting adversarial images in all three cases and is robust to strong adaptive adversaries. We now discuss in more depth the strengths and limitations of our approach, highlighting some unusual aspects of our design.

a) Attack Detection: We showed the effectiveness of SentiNet when protecting both compromised and uncompromised networks, without prior knowledge of the network vulnerability. Attack detection rates in four attacks are between 98.5% and 99.2%. In one attack, SentiNet scored 85.5% TP rate, that is comparable with proposed detection techniques [6].

b) Turning a Weakness into a Strength and Proportional Defense: One strength of SentiNet is that it relies on the fact models are compromised by an attack. Therefore, our detection framework is largely unaffected by the mechanism or deployment the attack uses, detecting attacks successfully as long as they fool the model. In fact, SentiNet is better at detecting attacks when the adversary is stronger. The properties

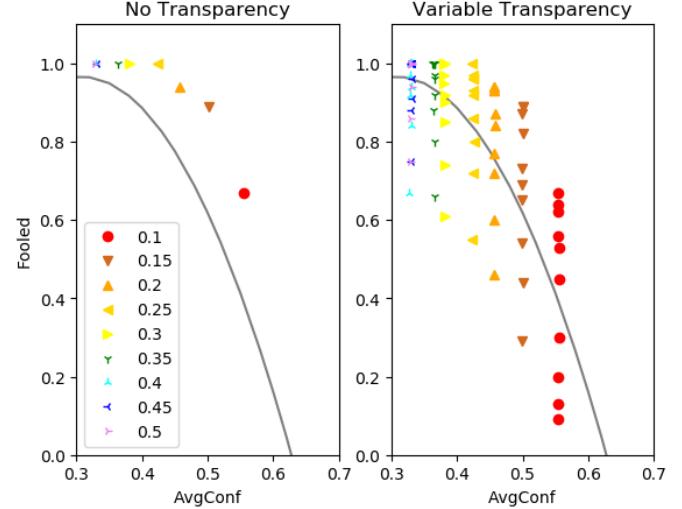


Fig. 10: Size analysis of adversarial patches. The legend denotes the ratio of the image to the input, and we can see that the *AvgConf* drops as the size increases. On the right, we plot the attack success rate after increasing the transparency values, and we can see that with large (> 0.35) patches the input drops below the decision boundary while still retaining a 90% attack success rate.

that characterize a strong attack make it easier for SentiNet detection as such an attack would easily result in outlier behavior outside the threshold of an approximated curve. In real-world conditions, attacks have to be even more robust as they need to tolerate different lighting and viewpoint variations. Real-world deployments of neural networks could potentially represent the most potent deployment scenario for SentiNet.

c) Detection of Unsuccessful Attacks: SentiNet can also be further extended with additional functionality. With the adversarial input detection and class proposal, SentiNet can also analyze the second or subsequent proposed classes, raising the possibility of using SentiNet to detect unsuccessful, attempted attacks. Such a behavior can be useful and help deter attackers from probing and testing our defense with experimental attacks.

d) Runtime Adversarial Object Suppression: Furthermore, the masking functionality can be used to still preserve functionality by reporting the output label with the inert pattern. Unlike other detection frameworks which simply identify when an attack has taken place, the calculated mask of SentiNet can easily be used to remove the localized universal attack and salvage as much of the rest of the data as possible.

e) Attack Size: The goal of SentiNet is to capture unreasonably salient attacks, designed to be small and unnoticeable. With this measure, SentiNet largely succeeds at detecting abnormal regions of images that deviate from patches of natural images. When adversaries can modify the majority of pixels in an image, they can override the prediction. As noted by Brown et al. [5], large images of an actual toaster will hijack the same prediction of an adversarial patch at a large enough size, raising an interesting question about what actually constitutes an “attack”. Based on this observation, we

note that the attack's *avgConf* drops as the size of the object increases, and by increasing the transparency of the object, the attack drops below the threshold while retaining very high attack success (See Figure 10). Similarly as observed by Brown et al. [5], drop of *avgConf* and high attack success is the result of obfuscating the test inputs with the large targeted class. We conclude that, while our defense correctly captures small patches, the detection of unreasonably large objects is very challenging for SentiNet.

f) Latency: The runtime of SentiNet is about 2.5s, which is acceptable for tasks like runtime facial recognition. However, it could be impractical for real-time scenarios including autonomous driving. The vast majority of the runtime of SentiNet (1.9s, i.e., 75% of the total) is taken by the selective search algorithm. Over the past years, the research community has proposed faster image segmentation approaches; however, none of the new ideas seem to offer the same trade-off between precision, performance, and security as provided by the selective search algorithm. For example, Ren et al. [45] and Redmon et al. [42], [43], [44] proposes using a neural network to segment images. These new approaches are remarkably fast, taking as little as 0.02 seconds per image (i.e., YOLOv3 [44]) to segment an image. While such a low runtime is very desirable for SentiNet, neural network segmentation algorithms introduce severe vulnerabilities in SentiNet. For example, in a recent work, Tramèr et al. [54] showed an interesting property of neural network image segmentation techniques, where an adversary can use perturbations to fully control the position and the size of the output segments. Alternatively, in scenarios where efficiency is a priority, a sliding-window approach can be a valid alternative. However, the sliding-window approach has a few drawbacks that make it inadequate for SentiNet. Specifically, it improves execution time only when using large windows, and large windows are more likely to contain multiple classes, affecting the capability to detect adversarial inputs of SentiNet. Overall, based on the current state of the art, we believe selective search is adequate to cope with relevant deployment scenarios of DL systems. Also, we hope that the encouraging results of SentiNet will inspire researchers to propose more efficient and secure segmentation techniques.

g) Other Classes of Attacks and Future Improvement: The goal of SentiNet is to protect networks against localized universal adversarial inputs, and our results show the viability and robustness of our approach. However, other types of attacks may be possible such as non-universal malicious objects, e.g., patches that work with specific images, or non-localized malicious objects, e.g., disjoint patches. These attacks may pose a challenge for SentiNet and their impact needs to be further studied.

A promising direction that could improve SentiNet to handle disjoint malicious objects is using other finer-grained visualization techniques, e.g., Grad-CAM++ [11]. In general, deep learning interpretability and visualization is a challenging problem and breakthroughs in this area can also allow us to further reason about whether such attacks will take place.

Handling non-universal patches may require to revisit the anomaly detection phase, which assumes that successful attacks hijack test inputs of different classes. The anomaly detection approach of SentiNet could be extended to take advantage of the richer data provided by the neuron outputs during the

inference process. Recent works have shown techniques to detect anomalous high dimensional data using one class neural networks (see, e.g., [19], [10]) which could enhance our current framework.

VII. RELATED WORK

We now review works closely related to this paper. First, we explore the domain of attacks against neural networks. Then, we expand on prior works on localized universal attacks. Finally, we review proposed approaches to detect attacks against neural networks.

a) Neural Network Attacks: The literature on attacks on neural networks is vast and still growing. Szegedy et al. [51] first demonstrated how adversarial noise can be used to fool neural network classifiers by adding small gradient perturbations to an image that is imperceptible to humans. Numerous works have built on this approach; some notable works include the Fast Gradient Sign Method [21], DeepFool [40], and Universal Adversarial Perturbations [39]. This area of research can be categorized as a cat-and-mouse game in recent years, where defenses are created for new attacks that bypass previous defenses [6] [9]. Additionally, attacks certainly are not limited to gradient-perturbation based techniques; data poisoning can be used to cause misintended model behaviors [47], and compromised hardware can also be used to insert trojans during the network inference procedure [12]. Akhtar et al. [1] provides a useful survey about the current state of the adversarial deep learning field.

b) Localized Universal Attacks: Multiple works have demonstrated attacks within a variety of classification settings and attacker capabilities. Adversarial patches [5] are possibly the most well-known localized universal attack. These attacks are generated by performing back-propagation on the target class to calculate gradient noise localized to a region of the image. A related attack—Localized and Visible Adversarial Noise [30]—operates under a similar principle with smaller but less robust attacks. Robust Physical-World Attacks on Deep Learning Models [14] demonstrates how adversarial perturbations can be disguised as graffiti stickers to fool traffic sign attacks. Similarly, Sharif et al. [48] use perturbations placed on glasses to fool facial classification models. Trojaned Neural Networks [34] perform back-propagation on specifically chosen neurons in the network rather than the target class. The generated triggers are used to "trojan" the model by performing slight fine-tuning to guide the trigger outputs towards a specified class, making sure that the triggers only cause misclassifications on trojaned models. BadNets [23] targets traffic sign detection models by inserting pre-chosen patterns into images with the target label, poisoning the data before the training process.

c) Adversarial Attack Detection: Detection techniques for attacks as a defensive measure have been proposed by many researchers. Safetynets [35] is designed to detect adversarial-noise based attacks and exploits the different activations adversarial perturbations produce to train a SVM classifier. Metzen et al. [25] use a similar approach by training a modified target classification network to detect adversarial perturbations. Feinman et al. [16] also trains a classifier to detect adversarial perturbational inputs based on the neural network features,

while Gong et al. [20] introduces a classifier trained to detect adversarially-perturbed images. Magnet [37] trains a classifier on manifolds of normal examples to detect adversarial perturbations without prior knowledge of the attack. There are also some works designed at creating defenses that do not require training. Grosse et al. [22] uses statistical techniques to distinguish adversarial-perturbations outputs, while Hendrycks et al. [26] uses PCA to visualize differences in perturbed images. A survey by Yuan et al. [56] covers further detection defenses. All these works are only aimed at defending against adversarial perturbations whereas SentiNet can defend a network against other types of attacks, i.e., data poisoning and trojaning attacks.

VIII. CONCLUSION

In this work, we introduce SentiNet, a framework for detecting localized universal attacks on Convolutional Neural Networks. Our method is notable because it only relies on the malicious behavior of an adversarial attack to perform classifications, without requiring prior knowledge of the attack vector. We demonstrate the versatility of SentiNet on three experiments with fundamentally different attack mechanisms: a data poisoning attack, a network trojaning attack, and adversarial patches—including physically realizable ones. We further evaluate the robustness of SentiNet against strong adaptive adversaries by individually testing each component of our defense. Our approach can be run in realtime in many scenarios, and is flexible and easy to deploy.

We hope SentiNet inspires further approaches towards creating attack-agnostic defenses. Tailoring a defense towards a specific attack means unknown attacks cannot be captured, and also makes the system highly vulnerable to strong adaptive adversaries. We believe a similar approach can be used to detect other attacks by leveraging the same core concepts of identifying an attack from a model’s weakness.

REFERENCES

- [1] N. Akhtar and A. Mian, “Threat of adversarial attacks on deep learning in computer vision: A survey,” *CoRR*, vol. abs/1801.00553, 2018. [Online]. Available: <http://arxiv.org/abs/1801.00553>
- [2] A. Athalye, N. Carlini, and D. Wagner, “Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples,” *arXiv preprint arXiv:1802.00420*, 2018.
- [3] A. Athalye and I. Sutskever, “Synthesizing robust adversarial examples,” *arXiv preprint arXiv:1707.07397*, 2017.
- [4] Y. Bengio, “Deep learning of representations for unsupervised and transfer learning,” in *Proceedings of ICML Workshop on Unsupervised and Transfer Learning*, 2012, pp. 17–36.
- [5] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer, “Adversarial patch,” *CoRR*, vol. abs/1712.09665, 2017. [Online]. Available: <http://arxiv.org/abs/1712.09665>
- [6] N. Carlini, “Evaluation and design of robust neural network defenses,” Ph.D. dissertation, EECS Department, University of California, Berkeley, Aug 2018. [Online]. Available: <http://www2.eecs.berkeley.edu/Pubs/TechRpts/2018/EECS-2018-118.html>
- [7] N. Carlini, A. Athalye, N. Papernot, W. Brendel, J. Rauber, D. Tsipras, I. Goodfellow, and A. Madry, “On evaluating adversarial robustness,” *arXiv preprint arXiv:1902.06705*, 2019.
- [8] N. Carlini and D. Wagner, “Adversarial examples are not easily detected: Bypassing ten detection methods,” in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*. ACM, 2017, pp. 3–14.
- [9] N. Carlini and D. A. Wagner, “Adversarial examples are not easily detected: Bypassing ten detection methods,” *CoRR*, vol. abs/1705.07263, 2017. [Online]. Available: <http://arxiv.org/abs/1705.07263>
- [10] R. Chalapathy, A. K. Menon, and S. Chawla, “Anomaly detection using one-class neural networks,” *CoRR*, vol. abs/1802.06360, 2018. [Online]. Available: <http://arxiv.org/abs/1802.06360>
- [11] A. Chattopadhyay, A. Sarkar, P. Howlader, and V. N. Balasubramanian, “Grad-cam++: Generalized gradient-based visual explanations for deep convolutional networks,” *CoRR*, vol. abs/1710.11063, 2017. [Online]. Available: <http://arxiv.org/abs/1710.11063>
- [12] J. Clements and Y. Lao, “Hardware trojan attacks on neural networks,” *CoRR*, vol. abs/1806.05768, 2018.
- [13] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, “ImageNet: A Large-Scale Hierarchical Image Database,” in *CVPR09*, 2009.
- [14] I. Evtimov, K. Eykholt, E. Fernandes, T. Kohno, B. Li, A. Prakash, A. Rahmati, and D. Song, “Robust physical-world attacks on machine learning models,” *CoRR*, vol. abs/1707.08945, 2017. [Online]. Available: <http://arxiv.org/abs/1707.08945>
- [15] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, F. Tramer, A. Prakash, T. Kohno, and D. Song, “Physical adversarial examples for object detectors,” *arXiv preprint arXiv:1807.07769*, 2018.
- [16] R. Feinman, R. R. Curtin, S. Shintre, and A. B. Gardner, “Detecting Adversarial Samples from Artifacts,” *ArXiv e-prints*, Mar. 2017.
- [17] R. B. Girshick, “Fast R-CNN,” *CoRR*, vol. abs/1504.08083, 2015. [Online]. Available: <http://arxiv.org/abs/1504.08083>
- [18] X. Glorot, A. Bordes, and Y. Bengio, “Deep sparse rectifier neural networks,” in *AISTATS*, 2011.
- [19] M. Goldstein and S. Uchida, “A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data,” *PLOS ONE*, vol. 11, no. 4, pp. 1–31, 04 2016. [Online]. Available: <https://doi.org/10.1371/journal.pone.0152173>
- [20] Z. Gong, W. Wang, and W. Ku, “Adversarial and clean data are not twins,” *CoRR*, vol. abs/1704.04960, 2017. [Online]. Available: <http://arxiv.org/abs/1704.04960>
- [21] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and Harnessing Adversarial Examples,” *ArXiv e-prints*, Dec. 2014.
- [22] K. Grosse, P. Manoharan, N. Papernot, M. Backes, and P. D. McDaniel, “On the (statistical) detection of adversarial examples,” *CoRR*, vol. abs/1702.06280, 2017. [Online]. Available: <http://arxiv.org/abs/1702.06280>
- [23] T. Gu, B. Dolan-Gavitt, and S. Garg, “Badnets: Identifying vulnerabilities in the machine learning model supply chain,” *CoRR*, vol. abs/1708.06733, 2017. [Online]. Available: <http://arxiv.org/abs/1708.06733>
- [24] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *CoRR*, vol. abs/1512.03385, 2015. [Online]. Available: <http://arxiv.org/abs/1512.03385>
- [25] J. Hendrik Metzen, T. Genewein, V. Fischer, and B. Bischoff, “On Detecting Adversarial Perturbations,” *ArXiv e-prints*, Feb. 2017.
- [26] D. Hendrycks and K. Gimpel, “Early Methods for Detecting Adversarial Images,” *ArXiv e-prints*, Aug. 2016.
- [27] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, “Labeled faces in the wild: A database for studying face recognition in unconstrained environments,” University of Massachusetts, Amherst, Tech. Rep. 07-49, October 2007.
- [28] Y. Ji, X. Zhang, S. Ji, X. Luo, and T. Wang, “Model-reuse attacks on deep learning systems,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 349–363.
- [29] J. Johnson, “Cnn benchmarks,” 2018. [Online]. Available: <https://github.com/jcjohnson/cnn-benchmarks>
- [30] D. Karmon, D. Zoran, and Y. Goldberg, “Lavan: Localized and visible adversarial noise,” *CoRR*, vol. abs/1801.02608, 2018. [Online]. Available: <http://arxiv.org/abs/1801.02608>
- [31] A. Kurakin, I. Goodfellow, and S. Bengio, “Adversarial examples in the physical world,” *arXiv preprint arXiv:1607.02533*, 2016.
- [32] Y. LeCun, Y. Bengio *et al.*, “Convolutional networks for images, speech,

- and time series,” *The handbook of brain theory and neural networks*, 1995.
- [33] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, 2015.
- [34] Y. Liu, S. Ma, Y. Aafer, W.-C. Lee, J. Zhai, W. Wang, and X. Zhang, “Trojaning attack on neural networks,” in *NDSS*, 2018.
- [35] J. Lu, T. Issaranon, and D. A. Forsyth, “Safetynet: Detecting and rejecting adversarial examples robustly,” *CoRR*, vol. abs/1704.00103, 2017. [Online]. Available: <http://arxiv.org/abs/1704.00103>
- [36] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, “Towards deep learning models resistant to adversarial attacks,” in *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=rJzIBfZAb>
- [37] D. Meng and H. Chen, “Magnet: a two-pronged defense against adversarial examples,” *CoRR*, vol. abs/1705.09064, 2017. [Online]. Available: <http://arxiv.org/abs/1705.09064>
- [38] A. Møgelmose, D. Liu, and M. M. Trivedi, “Traffic sign detection for u.s. roads: Remaining challenges and a case for tracking,” in *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, Oct 2014, pp. 1394–1399.
- [39] S. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, “Universal adversarial perturbations,” *CoRR*, vol. abs/1610.08401, 2016. [Online]. Available: <http://arxiv.org/abs/1610.08401>
- [40] S. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, “Deepfool: a simple and accurate method to fool deep neural networks,” *CoRR*, vol. abs/1511.04599, 2015. [Online]. Available: <http://arxiv.org/abs/1511.04599>
- [41] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep face recognition,” in *British Machine Vision Conference*, 2015.
- [42] J. Redmon, S. K. Divvala, R. B. Girshick, and A. Farhadi, “You only look once: Unified, real-time object detection,” *CoRR*, vol. abs/1506.02640, 2015. [Online]. Available: <http://arxiv.org/abs/1506.02640>
- [43] J. Redmon and A. Farhadi, “YOLO9000: better, faster, stronger,” *CoRR*, vol. abs/1612.08242, 2016. [Online]. Available: <http://arxiv.org/abs/1612.08242>
- [44] ———, “Yolov3: An incremental improvement,” *arXiv preprint arXiv:1804.02767*, 2018.
- [45] S. Ren, K. He, R. B. Girshick, and J. Sun, “Faster R-CNN: towards real-time object detection with region proposal networks,” *CoRR*, vol. abs/1506.01497, 2015. [Online]. Available: <http://arxiv.org/abs/1506.01497>
- [46] R. R. Selvaraju, A. Das, R. Vedantam, M. Cogswell, D. Parikh, and D. Batra, “Grad-cam: Why did you say that? visual explanations from deep networks via gradient-based localization,” *CoRR*, vol. abs/1610.02391, 2016. [Online]. Available: <http://arxiv.org/abs/1610.02391>
- [47] A. Shafahi, W. R. Huang, M. Najibi, O. Suciu, C. Studer, T. Dumitras, and T. Goldstein, “Poison frogs! targeted clean-label poisoning attacks on neural networks,” *CoRR*, vol. abs/1804.00792, 2018. [Online]. Available: <http://arxiv.org/abs/1804.00792>
- [48] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, “Accessitize to a crime: Real and stealthy attacks on state-of-the-art face recognition,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’16. New York, NY, USA: ACM, 2016, pp. 1528–1540. [Online]. Available: <http://doi.acm.org/10.1145/2976749.2978392>
- [49] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” *CoRR*, vol. abs/1409.1556, 2014. [Online]. Available: <http://arxiv.org/abs/1409.1556>
- [50] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. E. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, “Going deeper with convolutions,” *CoRR*, vol. abs/1409.4842, 2014. [Online]. Available: <http://arxiv.org/abs/1409.4842>
- [51] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. J. Goodfellow, and R. Fergus, “Intriguing properties of neural networks,” *CoRR*, vol. abs/1312.6199, 2013. [Online]. Available: <http://arxiv.org/abs/1312.6199>
- [52] A. R. C. K. S. P. L. Toint, “On the convergence of derivative-free methods for unconstrained optimization,” in *Approximation theory and optimization: tributes to MJD Powell*, 2007, pp. 83–108.
- [53] F. Tramer, N. Carlini, W. Brendel, and A. Madry, “On adaptive attacks to adversarial example defenses,” *arXiv preprint arXiv:2002.08347*, 2020.
- [54] F. Tramèr, P. Dupré, G. Rusak, G. Pellegrino, and D. Boneh, “Ad-versarial: Defeating perceptual ad-blocking,” *arXiv preprint arXiv:1811.03194*, 2018.
- [55] J. R. Uijlings, K. E. Sande, T. Gevers, and A. W. Smeulders, “Selective search for object recognition,” *Int. J. Comput. Vision*, vol. 104, no. 2, pp. 154–171, Sep. 2013. [Online]. Available: <http://dx.doi.org/10.1007/s11263-013-0620-5>
- [56] X. Yuan, P. He, Q. Zhu, R. R. Bhat, and X. Li, “Adversarial examples: Attacks and defenses for deep learning,” *CoRR*, vol. abs/1712.07107, 2017. [Online]. Available: <http://arxiv.org/abs/1712.07107>
- [57] R. Zhang, W. Li, and T. Mo, “Review of deep learning,” *CoRR*, vol. abs/1804.01653, 2018. [Online]. Available: <http://arxiv.org/abs/1804.01653>