

Adversarial Examples in Modern Machine Learning: A Review

Rey Reza Wiyatno Anqi Xu Ousmane Dia Archy de Berker

Element AI
Montréal, Canada

{rey.reza, ax, ousmane, archy}@elementai.com

Abstract

Recent research has found that many families of machine learning models are vulnerable to adversarial examples: inputs that are specifically designed to cause the target model to produce erroneous outputs. In this survey, we focus on machine learning models in the visual domain, where methods for generating and detecting such examples have been most extensively studied. We explore a variety of adversarial attack methods that apply to image-space content, real world adversarial attacks, adversarial defenses, and the transferability property of adversarial examples. We also discuss strengths and weaknesses of various methods of adversarial attack and defense. Our aim is to provide an extensive coverage of the field, furnishing the reader with an intuitive understanding of the mechanics of adversarial attack and defense mechanisms and enlarging the community of researchers studying this fundamental set of problems.

Table of Contents

1	Introduction	4
1.1	What can we learn from adversarial examples?	4
1.2	Why this work?	5
2	Common Terms and Notations	7
2.1	Common Terms	7
2.2	Notations	8
3	Adversarial Examples	9
4	Adversarial Attacks	10
4.1	L-BFGS Attack	12
4.2	Fast Gradient Sign Method	12
4.3	Basic Iterative Method	13
4.4	Iterative Least-Likely Class Method	13
4.5	R+FGSM	14
4.6	Adversarial Manipulation of Deep Representations	14
4.7	DeepFool	15
4.8	Jacobian-based Saliency Map Attacks	16
4.9	Substitute Blackbox Attack	19
4.10	Hot/Cold Attack	20
4.11	Carlini & Wagner Attacks	21
4.12	Universal Adversarial Perturbation	22
4.13	Data-Free UAP	24
4.14	VAE Attacks	25
4.15	Adversarial Transformation Networks	26
4.16	Dense Adversary Generation	27
4.17	Zeroth Order Optimization	28
4.18	One-Pixel Attack	30
4.19	Houdini	32
4.20	Momentum Iterative Fast Gradient Sign Method	33
4.21	AdvGAN	34
4.22	Boundary Attack	35
4.23	Natural Adversarial Attack	38
4.24	Spatially Transformed Adversarial Attack	39
4.25	Expectation Over Transformation	41
4.26	Backward Pass Differentiable Approximation	42
4.27	Simultaneous Perturbation Stochastic Approximation Attack	42
4.28	Decoupled Direction and Norm Attack	43
4.29	CAMOU	44
5	Towards Real World Adversarial Attacks	46
5.1	Printed Adversarial Examples	46
5.2	Adversarial Eyeglasses	46
5.3	Adversarial Stop Signs	47
5.4	Adversarial 3D Printed Turtle	48
5.5	Adversarial Patch	49
5.6	ShapeShifter	50
5.7	Non-physical Adversaries in the Real World	51

6	Defenses against Adversarial Attacks	52
6.1	Increasing Robustness of Machine Learning Models	54
6.1.1	Adversarial Training	54
6.1.2	Deep Contractive Network	54
6.1.3	Defensive Distillation	55
6.1.4	MagNet	56
6.1.5	PGD Adversarial Training	57
6.1.6	Ensemble Adversarial Training	58
6.1.7	Random Resizing and Padding as a Defense	58
6.1.8	Stochastic Activation Pruning	59
6.1.9	Total Variance Minimization and Quilting	60
6.1.10	Thermometer Encoding	61
6.1.11	PixelDefend	62
6.1.12	Defense-GAN	63
6.1.13	WRM: A Distributionally Robust Optimization with Adversarial Training	63
6.1.14	High-Level Representation Guided Denoiser	64
6.1.15	Adversarial Logit Pairing	65
6.1.16	Fortified Networks	66
6.1.17	Feature Denoising Block	67
6.1.18	Analysis by Synthesis	68
6.1.19	Web-Scale Nearest-Neighbor Search	68
6.1.20	ME-Net	69
6.2	Detecting Adversarial Attacks	71
6.2.1	Early Methods: PCA, Softmax, and Reconstruction of Adversarial Images	71
6.2.2	Adversary Detector Networks	72
6.2.3	Kernel Density and Bayesian Uncertainty Estimates	73
6.2.4	Feature Squeezing	74
6.2.5	Reverse Cross-Entropy	75
7	Transferability of Adversarial Examples	77
7.1	What is transferability?	77
7.2	Where does transferability come from?	77
7.3	What affects transferability?	77
8	Conclusion and Future Work	79

1 Introduction

Machine learning algorithms have critical roles in an increasing number of domains. Technologies such as autonomous vehicles and language translation systems use machine learning at their core. Since the early success of Convolutional Neural Networks (CNNs) on the ImageNet Large Scale Visual Recognition Competition (ILSVRC) [1, 2, 3], deep learning [4, 5] has been successfully applied to numerous tasks including image classification [3, 6, 7], segmentation [8, 9], object tracking [10, 11, 12], object detection [13, 14, 15], speech recognition [16, 17, 18], language translation [19, 20, 21], and many more.

Despite the success of modern machine learning techniques in performing various complex tasks, security in machine learning has received far less academic attention. Robustness, both to accident and to malevolent agents, is clearly a crucial determinant of the success of machine learning systems in the real world. For example, Amodei et al. [22] catalogue a variety of possible negative impacts from poorly secured systems, particularly emphasizing issues around sensitive applications such as medical and transportation systems. Although these authors focused on the safety of reinforcement learning algorithms in particular, many of the addressed concerns can directly apply to wide range of machine learning models.

In this review, we focus on the application of adversarial examples to supervised learning problems. We leave it to future authors to cover unsupervised learning, reinforcement learning, or other classes of problems. We also restrict our discussion to classification tasks, as opposed to regression, although many of the methods discussed below may generalize to other problem contexts.

1.1 What can we learn from adversarial examples?

The concept of an adversarial example long predates work in machine learning. Humans are famously vulnerable to perceptual illusions, which have been fruitfully used to explore the mechanisms and representations underlying human cognition. Such illusions are frequently used to elucidate the implicit priors present in human perception. For instance, the Müller-Lyer illusion [23], in which a line bracketed by two outwards-facing arrows appears longer than one bracketed by outwards facing ones is thought to reveal a “cubeness” prior learned by people who live in highly-rectangular environments [24]. Color and brightness constancy - our ability to perceive colors and brightness as unchanging despite variance in illumination - are richly explored in illusions such as Adelson’s checkerboard illusion and Lotto’s coloured cube. Such illusions can even probe the inter-individual variance in visual priors: the recently popular “dress colour” meme is thought to rely upon peoples’ differing expectations of illuminating light, with people used to blue-tinted illumination seeing the dress as gold/white, and those assuming warm illumination seeing it as blue/black [25].

Such illusions elucidate not only cognitive phenomena, but details of the underlying neural circuitry (for a thorough review, see Eagleman [26]). For example, the phenomenon of Inter Ocular transfer has provided a classic paradigm for identifying the locus of illusory effects. Based upon whether an illusory effect transfers from one eye to another, the substrate can be localized to pre-cortical circuitry (no transfer between eyes) or cortical ones, pathways after the mingling of information between the eyes [27, 28]. Similarly, adaptation-based illusions - where the appearance of an image changes over a period of prolonged viewing - have been used to predict the tuning curves of orientation-tuned neurons in visual cortex [27], the organization of colour representation in the lateral geniculate nucleus [29], and the sensitivity of the three colour-coding cell types in the retina [30]. So effective were these techniques that they earned the nickname “the psychologists’ microelectrode” - a precise, non-invasive way to characterize the internal workings of a blackbox system.

Szegedy et al. [31] found that deep neural networks are also vulnerable to “illusions”. These “adversarial examples” are created by the addition of “hidden messages” to an image, causing a machine learning model to grossly misclassify the perturbed image. Unlike perceptual illusions in humans, which are handcrafted, such examples are algorithmically generated to fool machine learning models. Figure 1 shows the now famous adversarial example generated using a method called the Fast Gradient Sign Method (FGSM) [32] (see Section 4.2). Judging from these evidences, there is indeed a huge generalisation gap between humans and deep neural networks [33].

The parallel between perceptual illusions in humans and adversarial examples in machines extends beyond the superficial in several important ways. One explanation for the effectiveness of adversarial examples is

that they push the input data off the manifold of natural inputs. This is precisely the same mechanism by which perceptual illusions in humans are generated, often exploiting mechanisms that generally improve the fidelity of perception but result in erroneous percepts when input data differs from natural inputs. As such, both approaches help to illustrate which features of the input domain are important for the performance of the system. Secondly, just as perceptual illusions have been used to interrogate the neural organization of perception, adversarial examples can help us understand the computations performed by neural networks. Early explanations focused upon the linearity of deep models [32], but more recent work focuses upon the entropy of the logit outputs [34]. Thirdly, recent evidence suggests a much stronger correspondence, namely that the same examples that fool neural networks also fool humans in time-limited settings [35]. As observed in that paper, this opens up the interesting possibility that techniques for adversarial defense might draw inspiration from the biological mechanisms that render humans invulnerable to such examples under normal viewing conditions.

Although the recent interest in adversarial attacks is chiefly concerned with their application to deep learning models, the field itself precedes the era of deep learning. For example, Huang et al. [36] established a taxonomy of adversarial attacks that has inspired many other works in adversarial machine learning, and also described a case study on adversarial attacks upon SpamBayes [37], a machine learning model for email spam filtering. Other works have also showed empirically that various machine learning models such as logistic regression, decision trees [38], k-Nearest Neighbor (kNN) [39], and Support Vector Machines (SVM) [40] are also vulnerable to adversarial examples [32, 41].

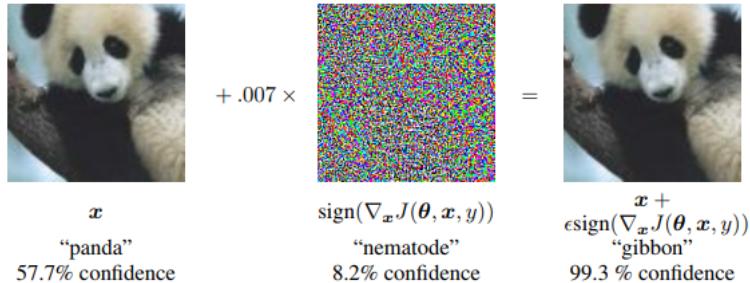


Figure 1: Adversarial example generated using the Fast Gradient Sign Method (FGSM) (taken from Goodfellow et al. [32]). GoogleNet [42] classified the original image shown on the left correctly as panda, but misclassified the image on the right as gibbon with high confidence. Note that the perturbation in the middle has been amplified for visualization purposes only.

1.2 Why this work?

Since the findings of Szegedy et al. [31], the arms race between adversarial attacks and defenses has accelerated. For example, defensive distillation [43] (see Section 6.1.3), then the state of the art defense against adversarial examples, was defeated within a year by an attack method proposed by Carlini and Wagner [44] (see Section 4.11). Similarly, defense using adversarial training [32] (see Section 6.1.1) once thought to be robust to whitebox attacks [45], was swiftly shown to rely upon a phenomenon called gradient masking [41, 46, 47] which can be circumvented by certain types of attacks. Most recently, a variety of defenses proposed by various different groups [48, 49, 50, 51, 52, 53, 54] that were accepted to the Sixth International Conference on Learning Representations (ICLR) 2018 have been shown to rely on gradient masking, and thus circumventable, shortly after the acceptance decision [55]. This further emphasizes how difficult it is to solve the adversarial examples problem in machine learning.

In this paper, we discuss various adversarial attack and defense strategies. Note that although adversarial examples exist in various domains such as computer security [56], speech recognition [57, 58, 59], and text [60], this paper focuses on adversarial examples in the computer vision domain where adversarial examples have been most extensively studied. We particularly focus upon perceptually imperceptible and inconspicuously

visible adversarial examples, which have the clearest potential for malicious use in the real world. Although other works have attempted to provide literature review on adversarial examples [61, 62], our work provides in-depth explanations of the motivation and mechanism of a wide array of attack and defense algorithms, along with a complete taxonomy and ontology of adversarial attacks and defenses, and a discussion of the strengths and weaknesses of different methods.

This paper is organized as follows. We begin by defining a list of common terms in adversarial machine learning and describing the notation used in this paper, in Section 2.1 and 2.2, respectively. Section 3 provides a general introduction to adversarial examples. The taxonomy, ontology, and discussion of adversarial attack and defense methods are defined in Section 4 and 6, respectively. We discuss several adversarial attacks in the real world in Section 5, and the transferability property of adversarial examples in Section 7. Finally, we conclude and suggest interesting lines of future research in Section 8.

2 Common Terms and Notations

2.1 Common Terms

We provide definitions of several terms that are commonly used in the field of adversarial machine learning in Table 1.

Table 1: Common terms in adversarial machine learning.

Common Terms	Definition
Adversarial example	Input to a machine learning model that is intentionally designed to cause a model to make mistake in its predictions despite resembling a valid input to a human.
Adversarial perturbation	Difference between a non-adversarial example and its adversarial counterpart.
Adversarial attacks	Methods to generate adversarial examples.
Adversarial defenses	Methods to defend against adversarial examples.
Adversarial robustness	The property of resisting misclassification of adversarial examples.
Adversarial detection	Methods to detect adversarial examples.
Whitebox attack	Attack scenario where an attacker has complete access to the target model, including the model's architecture and parameters.
Blackbox attack	Attack scenario where an attacker can only observe the outputs of the targeted model.
Transferability	A property of adversarial examples: examples specifically generated to fool a model can also be used to fool other models.
Universal attack	Attack scenario where an attacker devises a single transform such as image perturbation that adversarially confuses the model for all or most input values (input-agnostic).
Targeted attack	Attack scenario where an attacker wants the adversaries to be mispredicted in a specific way.
Non-targeted attack	Attack scenario where an attacker does not care about the outcome as long as the example is mispredicted.
Adversarial training [32]	Adversarial defense technique to train a model by including adversarial examples into the training set. Note that this differs from the notion of adversarial training used in Generative Adversarial Networks (GANs) [63].
Gradient masking [46, 47]	Defense mechanisms which prevent a model revealing meaningful gradients, <i>masking</i> or hiding the gradients of the outputs with respect to the inputs.
Shattered gradients [55]	When the gradients of a model are hard to compute exactly due to non-differentiable operations.
Stochastic gradients [55]	When the gradients of a model are obstructed due to some stochastic or random operations.
Obfuscated gradients [55]	A form of gradient masking which encompasses shattered gradients, stochastic gradients, vanishing, and exploding gradients.
Vanishing gradients	When the gradients of a model are converging to zero.
Exploding gradients	When the gradients of a model are diverging to infinity.

2.2 Notations

In order to make this paper easier to follow, we use the notations defined in Table 2 throughout this paper unless otherwise stated.

Table 2: Notations used in this survey.

Notation	Description
X	A set of input data (e.g., training set).
x	An instance of input data (usually a vector, a matrix, or a tensor).
x'	A modified instance of x , typically adversarial.
r	The additive perturbation from x to x' , i.e., $r = x' - x$.
y	The true class label for the input instance x .
t	An adversarial target class label for x' .
$f(x; \theta)$	Output of a machine learning model f parameterized by θ (e.g., a neural network). For a classifier, $f(x; \theta)$ specifically refers to the softmax predictions vector. Note that θ is often omitted for notation simplicity. Also, we use the parenthesized subscript $f(x; \theta)_{(c)}$ to denote the c -th element of the softmax vector, i.e., the predicted likelihood for class c .
$\hat{y}(x)$	Predicted label of a classifier model, i.e., $\hat{y}(x) = \arg \max_c f(x)_{(c)}$
$Z(x)$	Predicted logits vector of x from a softmax classifier model.
$\mathcal{L}(x, y)$	Loss function used to train a machine learning model. Note that we use $\mathcal{L}(x, y)$ instead of $\mathcal{L}(f(x; \theta), y)$ to simplify the notation.
$\nabla_x \mathcal{L}(x, y)$	Derivative of the loss function $\mathcal{L}(x, y)$ with respect to x .

3 Adversarial Examples

Adversarial examples are typically defined as inputs x' , where the differences between x' and non-adversarial inputs x are minimal under a distance metric $d(\cdot)$ (e.g., $d(\cdot)$ can be the L_p distance), whilst fooling the target model f . Generally, adversarial examples seek to satisfy

$$d(x', x) < \epsilon \text{ such that } \hat{y}(x') \neq \hat{y}(x), \quad (1)$$

where ϵ is a small constant that bounds the magnitude of the perturbations, and $\hat{y}(\cdot)$ denotes the predicted label of a classifier model (i.e., $\hat{y}(x) = \arg \max_c f(x)_{(c)}$). Note that we use $\hat{y}(x)$ to denote $\arg \max_c f(x)_{(c)}$ throughout this paper. However, some works have proposed perturbations that are visible but inconspicuous [64, 65, 66], so the similarity constraint between x and x' can be relaxed. Throughout this paper, we call these as “imperceptible” and “inconspicuous” (i.e., may be visible but not suspicious) adversarial examples, respectively.

Adversarial attacks are often categorized as either whitebox or blackbox. In whitebox attacks, the attacker is assumed to have information about the target model such as the architecture, parameters, training procedure, or the training data. On the other hand, blackbox attacks involve only access to the output of a target model, and not its internals. Blackbox attacks are more realistic assumption in the real world since an attacker rarely enjoys knowledge of the internals of the victim. However, evaluating models against whitebox attacks is important to measure the performance of the model in the worst-case scenarios. Adversarial attacks can be further categorized as targeted or non-targeted attacks. In a targeted attack, the adversarial example is designed to elicit a specific classification - like classifying all faces as belonging to George Clooney - whilst non-targeted attack only seek to generate an incorrect classification, regardless of class.

Adversarial examples exhibit an interesting phenomenon called the transferability property [31, 32, 67, 68]. This property states that adversarial examples generated to fool a specific model can often be used to fool other models. This phenomenon will be discussed in Section 7.

Why are machine learning models vulnerable to these examples? Several works have argued that adversarial examples are effective because they lie in the low probability region of the data manifold [31, 67]. Goodfellow et al. [32] pointed that deep neural networks are vulnerable to adversarial examples due to the local linearity property of these models, especially when using activation functions like the Rectified Linear Units (ReLU) [69] or Maxout [70]. Goodfellow et al. [32] observed that although deep neural networks use non-linear activation functions, one often trains such networks to only operate in the linear regions of the activation functions to avoid things like the vanishing gradient problem [71, 72, 73]. Furthermore, Goodfellow et al. [32] considered the fact that FGSM [32] (see Section 4.2) was designed based on the linear assumption works effectively to fool deep neural networks to support their argument that neural networks behave like a linear classifier. Arpit et al. [74] analyzed the capacity of neural networks to memorize training data and found that models with high degree of memorization are more vulnerable to adversarial examples. Jo and Bengio [75] argued that convolutional neural networks tend to learn the statistical regularities in the dataset rather than the high level abstract concepts. This may be related to the transferability property; since adversarial examples are transferable between models that are trained on the *same dataset*, these different models may have learned the same statistics and hence fall into the same traps. Similarly, Ilyas et al. [76] suggested that adversarial examples exist as a byproduct of exploiting *non-robust* features that exist in a dataset. Up to now, the reasons why machine learning models are vulnerable to adversarial examples are still an open research area.

4 Adversarial Attacks

In this section, we survey the adversarial attacks that exist today. Figure 2 and Table 3 illustrate the ontology and taxonomy of adversarial attack techniques discussed in this paper, respectively.

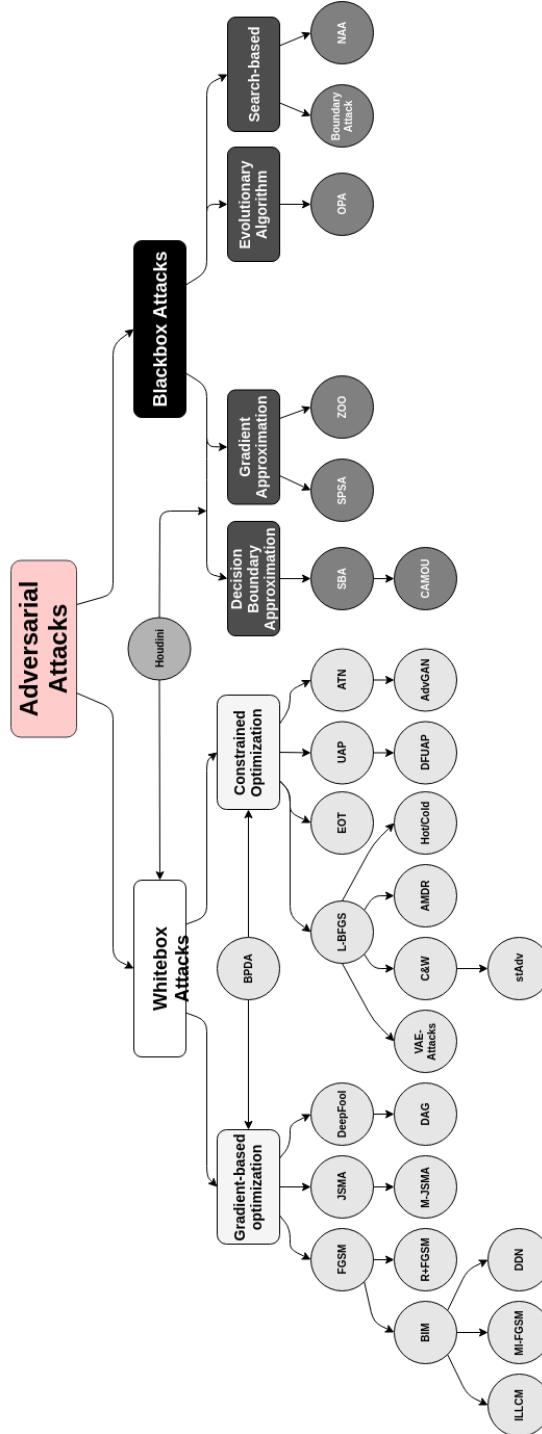


Figure 2: Ontology of adversarial attacks covered in this paper.

Table 3: Taxonomy of adversarial attacks covered in this paper.

Adversarial Attack(s)	Transparency	Specificity	Remarks
L-BFGS [31]	W	T, NT	Early attack on neural networks using constrained optimization method
FGSM [32]	W	T, NT	A fast single-step gradient ascent attack
BIM [45, 77]	W	T, NT	Iterative variants of FGSM
ILLCM [45, 77]	W	T	Extension of BIM to attack models with many output classes
R+FGSM [47]	W	T, NT	FGSM [32] with random initialization, can circumvent gradient masking
AMDR [78]	W	T, NT	Similar to L-BFGS but targetting feature space
DeepFool [79]	W	NT	Efficient method to find minimal perturbation that causes misclassification
JSMA [80]	W	T, NT	Some variants of JSMA can fool defensive distillation
SBA [41]	B	T, NT	Can fool defensive distillation [43], MagNet [81], gradient masking defenses
Hot/Cold [82]	W	T	Simultaneously moving towards “hot” class and away from “cold” class
C&W [44]	W	T, NT	Can fool defensive distillation [43], MagNet [81] and various detector networks
UAP [83]	W	NT	Generate input-agnostic perturbations
DFUAP [84]	W	NT	Generate input-agnostic perturbations without knowing any inputs
VAE Attacks [85]	W	T, NT	Can fool VAE [86] and potentially defenses relying on generative models
ATN [87]	W	T, NT	Generate adversarial examples using neural networks
DAG [88]	W	T, NT	Can fool semantic segmentation & object detection Models
ZOO [89]	B	T, NT	Can fool defensive distillation [43] and non-differentiable models
OPA [90]	B	T, NT	Uses genetic algorithm, can generate adversary by just modifying one pixel
Houdini [91]	W, B	T, NT	Method for attacking models directly through its non-differentiable metric
MI-FGSM [92]	W	T, NT	BIM + momentum, faster to converge and better transferability
AdvGAN [93]	W	T, NT	Generate adversarial examples using GAN [63]
Boundary Attack [94]	B	T, NT	Can fool defensive distillation [43] and non-differentiable models
NAA [60]	B	NT	Can generate adversaries for non-sensory inputs such as text
stAdv [95]	W	T, NT	Unique perceptual similarity objective
EOT [96]	W	T, NT	Good for creating physical adversaries and fooling randomization defenses
BPDA [55]	W	T, NT	Can fool various gradient masking defenses
SPSA [97]	B	T, NT	Can fool various gradient masking defenses
DDN [98]	W	T, NT	Better convergence compared to other constrained optimization methods
CAMOU [99]	B	NT	Attack in simulation using SBA [41], can be used to attack detection model

W: Whitebox
 B: Blackbox
 T: Targeted
 NT: Non-targeted

4.1 L-BFGS Attack

The L-BFGS attack [31] is an early method designed to fool models such as deep neural networks for image recognition tasks. Its end goal is to find a perceptually-minimal input perturbation $\arg \min_r \|r\|_2$, i.e., $r = x' - x$, within bounds of the input space, that is adversarial, i.e., $\hat{y}(x') \neq y$. Szegedy et al. [31] used the Limited Memory Broyden-Fletcher-Goldfarb-Shanno (L-BFGS) algorithm [100] to transform this difficult optimization problem into a box-constrained formulation where the goal is to find x' that minimizes

$$c\|r\|_2 + \mathcal{L}(x', t) \text{ such that } x' \in [0, 1], \quad (2)$$

where elements of x are normalized to $[0, 1]$, $\mathcal{L}(x', t)$ is the true loss function of the targeted model (e.g., categorical cross-entropy), and t is the target misclassification label. Since this objective does not guarantee that x' will be adversarial for any specific value of $c > 0$, the above optimization process is iterated for increasingly large values of c via line search until an adversary is found. Optionally, the resulting c value can be further optimized using the bisection method (a.k.a. binary search) between the range of the final line search segment.

This attack was successfully applied to misclassify many image instances on both AlexNet [3] and QuocNet [101], which were state-of-the-art classification models at the time. Thanks to its L_2 Euclidean distance constraint, L-BFGS produces adversaries that are perceptually similar to the original input x . Moreover, a key advantage of modeling adversarial examples generation process as a general optimization problem is that it allows for flexibility in folding additional criteria into the objective function. For instance, one may choose to use perceptual similarity metrics other than the L_2 distance, depending on requirements of a given application domain. We will see concrete examples of such criteria in subsequent sections.

4.2 Fast Gradient Sign Method

The Fast Gradient Sign Method (FGSM) [32] is designed to quickly find a perturbation direction for a given input such that the training loss function of the target model will increase, reducing classification confidence and increasing the likelihood of inter-class confusion. While there is no guarantee that increasing the training loss by a given amount will result in misclassification, this is nevertheless a sensible direction to take since the loss value for a misclassified instance is by definition larger than otherwise.

FGSM works by calculating the gradient of the loss function with respect to the input, and creating a small perturbation by multiplying a small chosen constant ϵ by the sign vector of the gradient:

$$x' = x + \epsilon \cdot \text{sign}(\nabla_x \mathcal{L}(x, y)), \quad (3)$$

where $\nabla_x \mathcal{L}(x, y)$ is the first derivative of the loss function with respect to the input x . In the case of deep neural networks, this can be calculated through the backpropagation algorithm [102]. In practice, the generated adversarial examples must be within the bounds of the input space (e.g., $[0, 255]$ pixel intensities for an 8-bit image), which is enforced by value-clipping.

The authors proposed to bound the input perturbation r under the L_∞ supremum metric (i.e., $\|r\|_\infty \leq \epsilon$) to encourage perceptual similarity between x and x' . Under this ∞ -norm constraint, the sign of the gradient vector maximizes the magnitude of the input perturbation, which consequently also amplifies the adversarial change in the model's output. A variant of FGSM that uses the actual gradient vector rather than its sign vector was later introduced as the Fast Gradient Value (FGV) method [82].

A sample adversarial example and perturbation generated by FGSM can be seen in Fig. 1. Note that this attack can be applied to any machine learning model where $\nabla_x \mathcal{L}(x, y)$ can be calculated. Compared to the numerically-optimized L-BFGS attack, FGSM computes gradients analytically and thus finds solutions much faster. On the other hand, FGSM does not explicitly optimize for the adversary x' to have a minimal perceptual difference, instead using a small ϵ to weakly bound the perturbation r . Optionally, once an adversarial example is found at a given ϵ value, one can use an iterative strategy similar to the L-BFGS attack's line search of c to further enhance perceptual similarity, although the resulting r may still not have minimal perceptual difference since perturbations are only searched along the sign vector of the gradient.

Huang et al. [103] have also shown that FGSM can be used to attack reinforcement learning models [104] where the policies are parameterized using neural networks such as the Trust Region Policy Optimization (TRPO) [105], Asynchronous Advantage Actor-Critic (A3C) [106], and Deep Q-Network (DQN) [107]. By applying the FGSM to modify images from various Atari games (e.g., Pong, Chopper Command, Seaquest, Space Invaders) [108], the agent can be fooled into taking sub-optimal actions.

4.3 Basic Iterative Method

The Basic Iterative Method (BIM) [45, 77] is one of many extensions of FGSM [32] (see Section 4.2), and is sometimes referred to as Iterative FGSM or I-FGSM. BIM applies FGSM multiple times within a supremum-norm bound on the total input perturbation, $\|r\|_\infty \leq \epsilon$. The adversarial examples generated by BIM are defined as

$$x'_{i+1} = Clip_\epsilon \left\{ x'_i + \alpha \cdot \text{sign}(\nabla_x \mathcal{L}(x'_i, y)) \right\} \text{ for } i = 0 \text{ to } n, \text{ and } x'_0 = x \quad (4)$$

where n is the total number of iterations and $0 < \alpha < \epsilon$ is the per-iteration step size. The clipping operator $Clip\{\cdot\}$ constrains each input feature (e.g., pixel) at coordinate (u, v, w) to be within an ϵ -neighborhood of the original instance x , as well as within the feasible input space (e.g., $[0, 255]$ for 8-bit intensity values):

$$Clip_\epsilon \{x'_{i,(u,v,w)}\} = \min \left\{ 255, x_{(u,v,w)} + \epsilon, \max \left\{ 0, x_{(u,v,w)} - \epsilon, x'_{i,(u,v,w)} \right\} \right\} \quad (5)$$

BIM was the first method shown to be effective with printed paper examples (see Section 5). Beyond classification models, BIM has also been used to attack semantic segmentation models [109], such as the FCN [8].

4.4 Iterative Least-Likely Class Method

The authors of BIM also proposed a targeted variant of the attack called the Iterative Least-Likely Class Method (ILLCM), where the goal is to generate an adversarial example which is misclassified as a specific target class t [45, 77]. In fact, ILLCM targets the class with the *least likelihood* of being chosen by the original classifier, i.e., $t = \arg \min f(x)$. The corresponding iterative update is given as:

$$x'_{i+1} = Clip_\epsilon \left\{ x'_i - \alpha \cdot \text{sign}(\nabla_x \mathcal{L}(x'_i, t)) \right\} \text{ for } i = 0 \text{ to } n, \text{ and } x'_0 = x. \quad (6)$$

This update is nearly identical to Equation 4, except that the predicted class in the cross-entropy loss is changed from the true label y to an adversarial target $t \neq y$, and the sign of the gradient update is reversed. Thus, whilst the non-targeted BIM and FGSM attacks *increase* the original classifier’s training loss, effectively “undoing training” and encouraging inter-class confusion, the targeted ILLCM *reduces* classification loss of an *adversarial training* pair (x, t) to misguide the model into having excessive confidence towards the target class t .

Why target the least likely class, $t = \arg \min f(x)$? Doing so maximizes misclassification robustness, preventing the model finding trivial adversarial examples for which the true classes are very similar. This is particularly relevant when working with large datasets such as ImageNet [1, 2], which contain many similar-looking classes. For instance, ImageNet includes examples of both Siberian Huskies and Alaskan Malamutes (both wolflike dogs). Non-targeted attacks risk finding trivial adversarial examples which cause confusion between the two, which is both easy to achieve and relatively benign. In contrast, ILLCM aims to maximize the negative impact of an attack through dramatic misclassification (e.g., dog → airplane), while minimizing input perturbations.

4.5 R+FGSM

The randomized single-step attack, or R+FGSM [47], adds a small random perturbation to the input before applying the adversarial perturbation generated by FGSM. This helps avoid the defensive strategy of gradient masking [41, 46, 47], which is illustrated in Fig. 3.

Tramèr et al. [47] discussed how adversarially training [32] (see Section 6.1.1) a model on FGSM [32] adversaries can effectively lead to gradient masking. Tramèr et al. [47] showed that there are many orthogonal adversarial directions, and that local loss gradients do not necessarily translate to the direction where the global loss of a model will be maximum. This led to some complacency in the machine learning community, in the mistaken belief that adversarially trained models are robust to unseen adversarial examples.

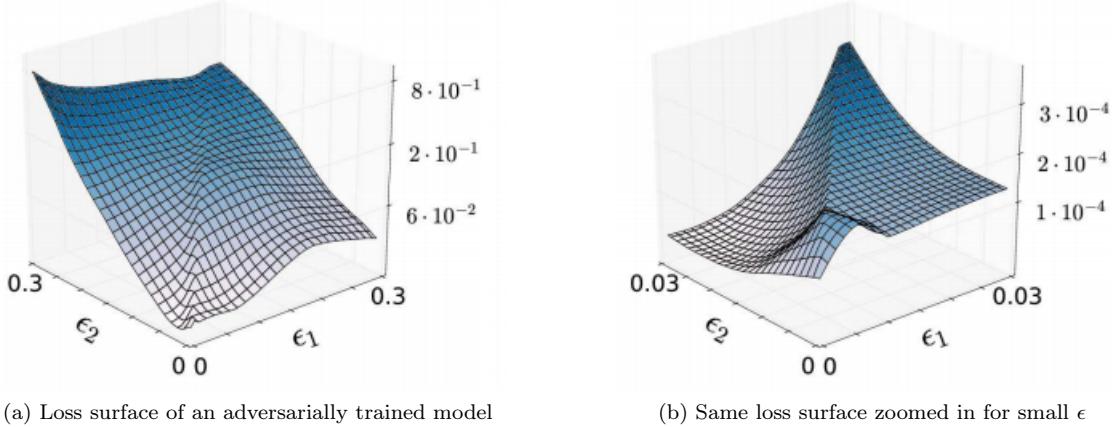


Figure 3: Illustration of a specific instance of gradient masking for an adversarially trained model (taken from Tramèr et al. [47]). Starting with values for model parameters ϵ_1 and ϵ_2 near the center of Fig. 3b, the gradient locally points towards smaller values for both parameters, while we see that on a wider scale the loss can be maximized (within an adversarial attack process) for larger values of ϵ_1 and ϵ_2 .

In order to escape from this particular case of gradient masking, R+FGSM first modifies the input into x^\dagger by pushing it towards a random direction (which is sampled as the sign of an unit multi-variate Gaussian), and then calculates the derivative of the loss with respect to x^\dagger :

$$x' = x^\dagger + (\epsilon - \alpha) \cdot \text{sign}(\nabla_{x^\dagger} \mathcal{L}(x^\dagger, y)), \text{ where } x^\dagger = x + \alpha \cdot \text{sign}(\mathcal{N}(0, 1)). \quad (7)$$

Here, α is a positive constant hyperparameter such that $0 < \alpha < \epsilon$. While the adversarial gradient now contributes less perturbation magnitude than in FGSM (i.e., $(\epsilon - \alpha)$ instead of ϵ), the random pre-perturbation increases the chance of finding an attack direction that escapes gradient masking.

Tramèr et al. [47] found that R+FGSM has a higher attack success rate compared to FGSM on adversarially trained Inception ResNet v2 [110] and Inception v3 models [111]. Furthermore R+FGSM was also found to be stronger compared to 2-steps BIM [45, 77] (see Section 4.3) on adversarially trained Inception v3 model, which suggests that random sampling provides better directions than using the local gradients. This strengthens the suspicion of gradient masking as random guesses should not produce better adversarial directions than using the actual gradients.

4.6 Adversarial Manipulation of Deep Representations

The approaches discussed so far optimize for properties of the output softmax or logits. Sabour et al. [78] proposed an altered formulation of the L-BFGS attack [31] that instead generates examples which resemble the target class in terms of their hidden layer activations. Adversarial Manipulation of Deep Representations

(AMDR) thus optimizes for similarity between a perturbed source image and a target image with different class label in the *intermediary* layers of a network, rather than the *output* layers.

Formally, AMDR requires a target neural network classifier f , a source image x , and a target image of a different class, x_t , where $f(x_t) \neq f(x)$. Given the above, the goal is to find an adversarial example x' that looks like x , yet whose internal representations resembles those of x_t . The resulting optimization objective is thus:

$$\arg \min_{x'} \|f_l(x') - f_l(x_t)\|_2^2 \quad \text{such that } \|x' - x\|_\infty < \epsilon, \quad (8)$$

where $f_l(\cdot)$ denotes the output of f at the l -th layer, i.e., the internal representations of the input, and ϵ denotes the bound for the L_∞ norm. Contrary to the L-BFGS attack, this method does not require a target label, but rather needs a target image x_t and a chosen feature layer l .

As shown by Sabour et al. [78], the AMDR attack successfully finds adversaries when evaluated against CaffeNet [112], AlexNet [3], GoogleNet [42], and a VGG variant [113] on ImageNet [1, 2] and Places205 [114] datasets. The authors also qualitatively evaluated the internal representations by inverting them back into an image using the technique proposed by [115] and found that the inverted images resembled the target images.

4.7 DeepFool

The DeepFool algorithm [79] estimates the distance of an input instance x to the closest decision boundary of a multi-class classifier. This result can be used both as a measure of the robustness of the model to attacks, and as a minimal adversarial perturbation direction. As motivation, the authors note that for a binary linear classifier, the distance to the decision boundary (which is simply a line) can be analytically computed using the point-to-line distance formula. This readily generalizes to a multi-class linear classifier, where the desired measure can be computed as the distance to the *nearest* of the decision boundary lines among the classes c .

Generalizing further to non-linear multi-class neural networks, DeepFool iteratively perturbs the input x by linearizing the model's per-class decision boundaries around the current set-point x'_i (starting from $x'_0 = x$), identifies the class j with the closest linearized decision boundary, and moves x'_i to this estimated boundary point. As shown in Algorithm 1, this process is repeated till $f(x'_i)$ becomes misclassified.¹ Recall that $f(x)_{(c)}$ denotes the c -th element of the softmax prediction vector $f(x)$, while \odot denotes element-wise multiplication.

The size of the resulting perturbation can be interpreted as a measure of the model's robustness to adversarial attacks. DeepFool can compute this measure using a variety of different L_p distance metrics including $p = 2$ Euclidean norm and $p = \infty$ supremum norm. In practice, once an adversarial perturbation r is found, the adversarial example is nudged further beyond the decision boundary to guarantee misclassification, e.g., $x' = x + 1.02r$.

DeepFool has been successful in attacking various models such as LeNet [116], Network in Network [117], CaffeNet [112], and GoogLeNet [42]. Furthermore, [79] found that DeepFool generates adversaries that have 5 times smaller perturbations compared to those resulting from FGSM [32] (see Section 4.2) on MNIST and CIFAR10 models, and 10 times smaller perturbations for ImageNet models. DeepFool was also found to produce adversaries with slightly smaller perturbations compared to the L-BFGS attack [31] (see Section 4.1) while being much faster (e.g., more than 30x speedup) to compute.

¹In the original formulation [79], the iterative algorithm terminates when $\hat{y}(x'_i) \neq \hat{y}(x)$, while our variant terminates on $\hat{y}(x'_i) \neq y$. These are identical when the classifier's prediction $\hat{y}(x)$ of a given input x correctly reflects the ground truth label y . Otherwise, x does not need to be perturbed if the original model already misclassifies it, and perturbing it to the nearest decision boundary might actually *correct* the misclassification.

Algorithm 1 DeepFool Algorithm for Multi-Class Classifier [79]

Input: input x , ground truth label y , number of classes N , classifier f , desired norm p , let $q = \frac{p}{p-1}$

Output: adversarial perturbation r

Initialize: $x'_0 \leftarrow x$, $r \leftarrow \{0, 0, \dots\}$, $i \leftarrow 0$

while $\hat{y}(x'_i) == \hat{y}(x)$ **do**

- for** $c = 0$ **to** N **do**
- if** $c \neq y$ **then**
- $w'_c \leftarrow \nabla_{x'_i} f(x'_i)_{(c)} - \nabla_{x'_i} f(x'_i)_{(y)}$
- $f'_c \leftarrow f(x'_i)_{(c)} - f(x'_i)_{(y)}$
- end if**
- end for**
- $j \leftarrow \arg \min_{c \neq y} \frac{|f'_c|}{\|w'_c\|_q}$
- $r_i \leftarrow \frac{|f'_j|}{\|w'_j\|_q^q} \cdot \text{sign}(w'_j) \odot |w'_h|^{q-1}$
- $x'_{i+1} \leftarrow x'_i + r_i$
- $i \leftarrow i + 1$

end while

Return: $r = \sum_i r_i$

4.8 Jacobian-based Saliency Map Attacks

The notion of the saliency map was originally conceived for visualizing how deep neural networks make predictions [118]. The saliency map rates each input feature (e.g., each pixel in an image) by its influence upon the network’s class prediction. Jacobian-based Saliency Map Attacks (JSMA) [80] exploit this information by perturbing a small set of input features to cause misclassification. This is in contrast to attacks like the FGSM [32] (see Section 4.2) that modify most, if not all, input features. As such, JSMA attacks tend to find sparse perturbations.

Given the predicted softmax probabilities vector $f(x)$ from a neural network classifier, one formulation of the saliency map S^+ is

$$S^+(x_{(i)}, t) = \begin{cases} 0 & \text{if } \nabla_{x_{(i)}} f(x)_{(t)} < 0 \text{ or } \sum_{c \neq t} \nabla_{x_{(i)}} f(x)_{(c)} > 0 \\ -\nabla_{x_{(i)}} f(x)_{(t)} \cdot \sum_{c \neq t} \nabla_{x_{(i)}} f(x)_{(c)} & \text{otherwise,} \end{cases} \quad (9)$$

where $x_{(i)}$ denotes the i -th element of x , and t is a specified label of interest, e.g., the target for visualization or attack. Intuitively, the S^+ saliency map uses components of the gradient $\nabla_{x_{(i)}} f(x)$ to quantify the degree to which each input feature $x_{(i)}$ *positively* correlates with a target class of interest t , while on average *negatively* correlating with all other classes $c \neq t$. If either condition is violated for a given feature $x_{(i)}$, then $S(x_{(i)}, t)$ is set to zero, effectively ignoring features which are not preferentially associated with the target class. The features with the largest saliency measure can then be increased to amplify the model’s predicted confidence for a target class t , whilst attenuating confidences for all other classes.

This process can easily be inverted to provide a negative saliency map, S^- , describing which features should be reduced to increase a target class probability. This formulation requires inverting the inequalities for the two low-saliency conditions:

$$S^-(x_{(i)}, t) = \begin{cases} 0 & \text{if } \nabla_{x_{(i)}} f(x)_{(t)} > 0 \text{ or } \sum_{c \neq t} \nabla_{x_{(i)}} f(x)_{(c)} < 0 \\ -\nabla_{x_{(i)}} f(x)_{(t)} \cdot \sum_{c \neq t} \nabla_{x_{(i)}} f(x)_{(c)} & \text{otherwise.} \end{cases} \quad (10)$$

Papernot et al. [80] notes that both saliency measures S^+ and S^- are overly strict when applied to individual input features (e.g., single image pixels), since it is likely that the sum of gradient contributions

Algorithm 2 Jacobian-based Saliency Map Attack by Increasing Pixel Intensities [80]

Input: n -dimensional input x normalized to $[0, 1]$, target class t , classifier f , maximum number of iterations I_{max} , perturbation step $\theta = +1$

Initialize: $x' \leftarrow x$, $i \leftarrow 0$, search domain $\Gamma \leftarrow \{1, \dots, n\}$

while $\hat{y}(x') \neq t$ **and** $i < I_{max}$ **and** $|\Gamma| \geq 2$ **do**

- Calculate $\nabla_{x'} f(x')$
- $\gamma \leftarrow 0$
- for** every pixel pair $(p, q) \in \Gamma$ **do**
- $\alpha = \sum_{k=p,q} \nabla_{x'_{(k)}} f(x')_{(t)}$
- $\beta = \sum_{k=p,q} \sum_{c \neq t} \nabla_{x'_{(k)}} f(x')_{(c)}$
- if** $\alpha > 0$ **and** $\beta < 0$ **and** $-\alpha \cdot \beta > \gamma$ **then**
- $p^*, q^* \leftarrow p, q$
- $\gamma \leftarrow -\alpha \cdot \beta$
- end if**
- end for**
- $x'_{(p^*)}, x'_{(q^*)} \leftarrow (x'_{(p^*)} + \theta), (x'_{(q^*)} + \theta)$
- if** $x'_{(p^*)} == 0$ **or** $x'_{(p^*)} == 1$ **then**
- Remove p^* from Γ
- end if**
- if** $x'_{(q^*)} == 0$ **or** $x'_{(q^*)} == 1$ **then**
- Remove q^* from Γ
- end if**
- $i \leftarrow i + 1$

end while

Return: x'

across non-targeted classes will trigger the minimal-saliency criterion. Consequently, as shown in Algorithm 2, the Jacobian-based Saliency Map Attack alters the saliency measures to search over *pairs* of pixels (p, q) instead. Concretely, given a search domain Γ initialized to contain the indices of all input features, the algorithm finds the most salient pixel pair, perturbs both values by $\theta = +1$, and then removes saturated feature indices from the search domain. This process is repeated until either an adversary is found, or in practice following a maximum number of iteration I_{max} , e.g.:

$$I_{max} = \frac{(\# \text{ of input features}) \cdot (\text{maximum desired percentage of perturbed features})}{(\# \text{ of features to be modified per iteration}) \cdot \lceil \theta^{-1} \rceil \cdot 100}, \quad (11)$$

The formulation in Algorithm 2 finds adversarial examples by *increasing* feature values ($\theta > 0$) based on the S^+ saliency measure. An alternative attack variant that *decreases* feature values can be constructed by substituting S^+ with S^- and setting $-1 \leq \theta < 0$. Both variants are targeted attacks that increase a classifier's softmax prediction confidence $f(x)_{(t)}$ for a chosen adversarial target class t .

The original authors prescribed $\theta = 1$ in order to find adversaries in as few iterations as possible. In general though, we can use a smaller feature perturbation step, i.e., $0 < \theta \leq 1$, to produce adversarial examples with fewer saturated features. Additionally, the feature saturation criterion can be also altered to be ϵ -bounded around the initial input values x_i (e.g., using $Clip\{\cdot\}$ from Equation 5), to further constrain per-pixel perceptual difference.

Carlini and Wagner [44] note that the above saliency measures and attack can be alternatively applied to evaluate the gradient of logits $Z(x)$ rather than of the softmax probabilities $f(x)$. While using different saliency measures results in favoring slightly different pixel pairs, both variants successfully find adversarial examples. We designate the original algorithm variants as JSMA+F and JSMA-F, and those using logit-based saliency maps as JSMA+Z and JSMA-Z, where + and - indicate whether input features are increased or decreased.

Papernot et al. [80] showed that JSMA can successfully fool a model by just modifying a few input features. They found that adversaries can be found by just modifying 4% of the input features in order to fool a targeted MNIST model. However, there are still room for improving the misclassification rate and efficiency by picking which features should be updated in a more optimal way. For example, note that Algorithm 2 needs to test every possible pixel pairs in the search domain before deciding on which pixel pairs should be updated for every iteration, which is computationally expensive to perform.

All JSMA variants above must be given a specific target class t . This choice affects the speed and quality of the attack, since misclassification under certain classes are easier to attain than others, such as perturbing a hand-written digit “0” to look like “8”. Instead of *increasing* the prediction probability (or logit) of an adversarial target $t \neq y$, we propose to remove this dependency altogether by instead altering JSMA to *decrease* the model’s prediction confidence of the true class label ($t = y$). These non-targeted JSMA variants are realized by swapping the saliency measure employed, i.e., follow S^- when increasing feature values (NT-JSMA+F / NT-JSMA+Z), or S^+ when decreasing feature values (NT-JSMA-F / NT-JSMA-Z).

Algorithm 3 Maximal Jacobian-based Saliency Map Attack

```

Input:  $n$ -dimensional input  $x$  normalized to  $[0, 1]$ , true class label  $y$ , classifier  $f$ , maximum number of iterations  $I_{max}$ , pixel perturbation step  $\theta \in (0, 1]$ , maximum perturbation bound  $\epsilon \in (0, 1]$ 
Initialize:  $x' \leftarrow x$ ,  $i \leftarrow 0$ ,  $\Gamma = \{1, \dots, n\}$ ,  $\eta = \{0, 0, \dots\}^n$ 
while  $\hat{y}(x') == y$  and  $i < I_{max}$  and  $|\Gamma| \geq 2$  do
    Calculate  $\nabla_{x'} f(x')$ 
     $\gamma \leftarrow 0$ 
    for every pixel pair  $(p, q) \in \Gamma$  and every class  $t$  do
         $\alpha = \sum_{k=p,q} \nabla_{x'_{(k)}} f(x')_{(t)}$ 
         $\beta = \sum_{k=p,q} \sum_{c \neq t} \nabla_{x'_{(k)}} f(x')_{(c)}$ 
        if  $-\alpha \cdot \beta > \gamma$  then
             $p^*, q^* \leftarrow p, q$ 
             $\gamma \leftarrow -\alpha \cdot \beta$ 
            if  $t == y$  then
                 $\theta' \leftarrow -sign(\alpha) \cdot \theta$ 
            else
                 $\theta' \leftarrow sign(\alpha) \cdot \theta$ 
            end if
        end if
    end for
    if  $x'_{(p^*)} == 0$  or  $x'_{(p^*)} == 1$  or  $\eta_{(p^*)} == -\theta'$  then
        Remove  $p^*$  from  $\Gamma$ 
    end if
    if  $x'_{(q^*)} == 0$  or  $x'_{(q^*)} == 1$  or  $\eta_{(q^*)} == -\theta'$  then
        Remove  $q^*$  from  $\Gamma$ 
    end if
     $\eta_{(p^*)}, \eta_{(q^*)} \leftarrow \theta'$ 
     $i \leftarrow i + 1$ 
end while
Return:  $x'$ 

```

Extending further, we propose a combined attack, termed Maximal Jacobian-based Saliency Map Attack (M-JSMA), that merges both targeted variants and both non-targeted variants together. As shown in Algorithm 3, at each iteration the maximal-salient pixel pair is *chosen over every possible class t* , whether adversarial or not. In this way, we find the most influential features across all classes, in the knowledge that changing these is likely to change the eventual classification. Furthermore, instead of enforcing low-saliency

conditions via S^+ or S^- , we identify which measure applies to the most salient pair (p^*, q^*) to *decide on the perturbation direction θ' accordingly*. A history vector η is added to prevent oscillatory perturbations. Similar to NT-JSMA, M-JSMA terminates when the predicted class $\hat{y}(x) = \arg \max_c f(x)_{(c)}$ no longer matches the true class y .

Table 4: Performance comparison of the original JSMA, non-targeted JSMA, and maximal JSMA variants ($|\theta| = 1$, $\epsilon = 1$): % of successful attacks, average L_0 and L_2 perturbation distances, and average entropy $H(f(x))$ of misclassified softmax prediction probabilities.

Attack	MNIST			F-MNIST			CIFAR10					
	%	L_0	L_2	H	%	L_0	L_2	H	%	L_0	L_2	H
JSMA+F	100	34.8	4.32	0.90	99.9	93.1	6.12	1.22	100	34.7	3.01	1.27
JSMA-F	100	32.1	3.88	0.88	99.9	82.2	4.37	1.21	100	36.9	2.13	1.23
NT-JSMA+F	100	17.6	3.35	0.64	100	18.8	3.27	1.03	99.9	17.5	2.36	1.16
NT-JSMA-F	100	19.7	3.44	0.70	99.9	33.2	2.99	0.98	99.9	19.6	1.68	1.12
M-JSMA_F	100	14.9	3.04	0.62	99.9	18.7	3.42	1.02	99.9	17.4	2.16	1.12

Table 4 summarizes attacks carried out on correctly-classified test-set instances in the MNIST [116], Fashion MNIST [119], and CIFAR10 [120] datasets, using targeted, Non-Targeted, and Maximal JSMA variants. For targeted attacks, we consider only adversaries that were misclassified in the *fewest* iterations over target classes. The JSMA+F results showed that on average only $(34.8 L_0 \text{ distance})/(28 * 28 \text{ pixels of an MNIST image}) = 4.4\%$ of pixels needed to be perturbed in order to create adversaries, thus corroborating findings from [80]. More importantly, as evidenced by lower L_0 values, NT-JSMA found adversaries much faster than the *fastest* targeted attacks across all 3 datasets, while M-JSMA was consistently even faster and on average only perturbed $(14.9 L_0 \text{ distance})/(28 * 28 \text{ pixels}) = 1.9\%$ of input pixels. Additionally, the quality of adversaries found by NT-JSMA and M-JSMA were also superior, as indicated by smaller L_2 perceptual differences between the adversaries x' and the original inputs x , and by lower misclassification uncertainty as reflected by prediction entropy $H(f(x)) = -\sum_c f(x)_{(c)} \cdot \log f(x)_{(c)}$. Since M-JSMA considers all possible class targets, and both S^+ and S^- metrics and perturbation directions, these results show that it inherits the combined benefits from both the original JSMA and NT-JSMA.

4.9 Substitute Blackbox Attack

All of the techniques covered so far are whitebox attacks, relying upon access to a model’s innards. Papernot et al. [41] proposed one of the early practical blackbox methods, called the Substitute Blackbox Attack (SBA). The key idea is to train a substitute model to mimic the blackbox model, and use whitebox attack methods on this substitute. This approach leverages the transferability property of adversarial examples. Concretely, the attacker first gathers a synthetic dataset, obtains predictions on the synthetic dataset from the targeted model, and then trains a substitute model to imitate the targeted model’s predictions.

After the substitute model is trained, adversaries can be generated using any whitebox attacks since the details of the substitute model are known (e.g., [41] used the FGSM [32] (see Section 4.2) and JSMA [80] (see Section 4.8)). We refer to SBA based on the type of adversarial attacks used when attacking the substitute model. For example, if the attacker uses FGSM to attack the substitute model, we refer this as FGSM-SBA.

The success of this approach depends on choosing adequately-similar synthetic data samples and a substitute model architecture using high-level knowledge of the target classifier setup. As such, an intimate knowledge of the domain and the targeted model is likely to aid the attacker. Even if the absence of specific expertise, the transferability property suggests that adversaries generated from a well-trained substitute model are likely to fool the targeted model as well.

Papernot et al. [41] note that in practice the attacker is constrained from making unlimited query to the targeted model. Consequently, the authors introduced the Jacobian-based Dataset Augmentation technique, which generates a limited number of additional samples around a small initial synthetic dataset to efficiently replicate the target model’s decision boundaries. Concretely, given an initial sample x , one calculates the

Jacobian of the predicted class' likelihood assigned by the targeted model $f(x)_{(\hat{y})} = \max_c f(x)_{(c)}$ with respect to the inputs. Since the attacker cannot apply analytical backpropagation to the targeted model, this gradient is instead calculated using the substitute model $f'(x)$, which we denote as $\nabla_x f'(x)_{(\hat{y})}$. A new sample x' is then synthesized by perturbing x along the sign of the gradient, $x' = \alpha \cdot \text{sign}(\nabla_x f'(x)_{(\hat{y})})$ by a small step α . While this process resembles FGSM, its purpose is instead to create samples that are likely to be classified with high confidence $f'(x')_{(\hat{y})} \approx f(x')_{(\hat{y})}$. Papernot et al. [41] noted that the resulting augmented dataset better represents the decision boundary of the targeted model, in comparison to randomly sampling more data points that would most likely fall outside the target model's training-set manifold.

Algorithm 4 Substitute Model Training with Jacobian-based Dataset Augmentation [41]

```

Input: initial training set  $X_0$ , targeted model  $f$ , initial substitute model  $f'$ , maximum number of iterations  $I_{max}$ , small constant  $\alpha$ 
Output: refined substitute model  $f'$ 
for  $i = 0$  to  $I_{max}$  do
     $Y_i \leftarrow \{f(X_i)\} \forall x \in X_i$ 
    Train  $f'$  on  $(X_i, Y_i)$  input-label pairs
     $X'_i \leftarrow \{x + \alpha \cdot \text{sign}(\nabla_x f'(x)_{(\hat{y})}) \mid x \in X_i\}$ 
     $X_{i+1} \leftarrow X'_i \cup X_i$ 
end for
Return:  $f'$ 

```

The entire training procedure for the substitute model is summarized in Algorithm 4. The attacker first creates a small initial training set X_0 . For example, X_0 can be initialized by picking one sample from each possible class of a set that represents the input domain of the targeted model. The substitute model is then trained on the synthetic dataset using labels provided by the targeted model (e.g., by querying the targeted model). New datapoints are then generated by perturbing each sample in the existing dataset along the general direction of variation. Finally, the new inputs are added to the existing dataset, i.e., the size of the synthetic dataset grows per iteration. This process is then repeated several times.

It is interesting to note that the targeted model does not have to be differentiable for the attack to succeed. The differentiability constraint applies only to the substitute model. As long as the substitute model has the capacity to approximate the targeted model, this attack is feasible. Papernot et al. [41] showed that substitute blackbox attack can be used to attack other machine learning models like logistic regression, Support Vector Machines (SVM) [40], k-Nearest Neighbor (kNN) [39], and non-differentiable models such as decision trees [38].

The authors evaluated SBA by targeting real world image recognition systems from Amazon, Google, and MetaMind on the MNIST dataset [116], and successfully fooled all targets with high accuracies ($> 80\%$). This method also successfully attacked a blackbox deep neural network model that was trained on German Traffic Sign Recognition Benchmarks (GTSRB) dataset [121]. Furthermore, SBA was shown to also circumvent defense methods that rely on gradient masking such as adversarial training on FGSM adversaries [32] (see Section 6.1.1) and defensive distillation [43] (see Section 6.1.3).

4.10 Hot/Cold Attack

Building on the idea of altering the input to increase classifier loss, as in FGSM [32] (see Section 4.2), Rozsa et al. [82] proposed an attack algorithm based upon setting the values of the classification logits $Z'(x)$. We can then use the gradients with respect to the input to push inputs towards producing the desired logits. The logits are modified such that the per-class gradients will point in directions where the output of the network will increase the probability of target (“hot”) class and decrease the probability of the ground truth (“cold”) class. The Hot/Cold attack alters a target classifier’s logits $Z(x)$ into:

$$Z'(x) = \begin{cases} |Z(x)_{(c)}| & \text{if } c == t \text{ (target class)} \\ -Z(x)_{(c)} & \text{if } c == y \text{ (correct class)} \\ 0 & \text{otherwise,} \end{cases} \quad (12)$$

where $Z(x)_{(j)}$ denotes the j -th element of the logits vector $Z(x)$.

Intuitively, by maximizing these modified logits using gradient ascent on x , $Z(x)_{(t)}$ will be increased (assuming that it starts with a positive setpoint value) while $Z(x)_y$ will be decreased. Correspondingly, the target model will predict the adversarial class with increased likelihood $f(x)_{(t)}$ and predict the true class with decreased likelihood $f(x)_{(y)}$, since the softmax function is monotonically increasing with respect to its logit inputs. Finally, letting the other elements have zero values isolates the adversarial perturbation search to focus only on target and ground truth classes.

Once $Z'(x)$ is obtained, and gradient directions are extracted with respect to the input x , we then search for the closest adversarial perturbations x' along these directions using line search and bisection search, as in the L-BFGS attack. While the original manuscript [82] had some ambiguities on how to exactly compute gradient(s) from $Z'(x)$, one sensible approach is to consider *two separate* directions based on $\nabla_x Z'(x)_{(t)}$ and $\nabla_x Z'(x)_{(y)}$, perform line search on each, and select the closest adversary. Also, while not explicitly specified by the original authors, since the Hot/Cold Attack finds the *closest* adversary via gradient line search, it correspondingly enforces perceptual similarity between x' and x following the L_2 metric.

The authors carried out preliminary assessments of this adversarial attack for the LeNet classification model on the MNIST dataset, and attained decent adversarial rates. Nevertheless, this work's main goal was to use generated adversaries to robustify a classifier model against further attackers via Adversarial Training [32] (see Section 6.1.1). The authors also anecdotally noted that many perturbations found using Hot/Cold Attack had structural visual appearances, and argued that such perturbations resemble patterns in natural images more so than the perceptually random-noise perturbations generated by FGSM [32].

4.11 Carlini & Wagner Attacks

Carlini and Wagner [44] introduced a family of attacks for finding adversarial perturbations that minimize diverse similarity metrics: L_0 , L_2 , and L_∞ . The core insight transforms a general constrained optimization strategy similar to the L-BFGS attack [31] (see Section 4.1) into an empirically-chosen loss function within an *unconstrained* optimization formulation:

$$\mathcal{L}_{CW}(x', t) = \max \left(\max_{i \neq t} \{Z(x')_{(i)}\} - Z(x')_{(t)}, -\kappa \right), \quad (13)$$

where $Z(x')_{(i)}$ denotes the i -th component of the classifier's logits, t denotes the target label, and κ represents a parameter that reflects the minimum desired confidence margin for the adversarial example.

Conceptually, this loss function minimizes the distance in logit values between class t and the second most-likely class. If t currently has the highest logit value, then the difference of the logits will be negative, and so the optimization will stop when this logit difference between t and the runner-up class exceeds κ . On the other hand, if t does not have the highest logit value, then minimizing $\mathcal{L}(x', t)$ brings the gap between the logits of the winning class and the target class closer together, i.e., either reducing the highest class's prediction confidence and/or increasing the target class's confidence.

Furthermore, the κ parameter establishes a best-case stopping criterion, in that the logit of the adversarial class is larger than the runner-up class' logit by at least κ . Thus, κ explicitly encodes a minimum desirable degree of robustness for the target adversary. Note that when $\kappa = 0$, the resulting adversarial examples would misclassify the network with weak robustness, as any further slight perturbations may revert to a non-adversarial softmax selection.

The L_2 C&W attack formulation is given as:

$$\arg \min_w (||x'(w) - x||_2^2 + c \cdot \mathcal{L}_{CW}(x'(w), t)) \quad \text{where } x'(w) = \frac{1}{2} (\tanh(w) + 1), \quad (14)$$

where w is a change of variable such that $x' = \frac{1}{2}(\tanh(w) + 1)$, which is introduced to bound x' to be within $[0, 1]$. The minimum value of the parameter c is chosen through an outer optimization loop procedure, which is detailed further below.

The L_0 C&W attack is much more complex than the L_2 variant, since its associated distance metric is non-differentiable. Instead, an iterative strategy is proposed to successively *eliminate non-significant* input features such that misclassification can be achieved by perturbing as few input values as possible. During initialization, an *allowed set* S is defined to include all input features in x . Next, at each iteration, an L_2 attack attempt is carried out, under the constraint of perturbing only features within S . If the attempt is successful, then the next non-significant feature i is identified and removed from S , where $i^* = \arg \min_i g_{(i)} \cdot r_{(i)}$, $g = \nabla_{x'} \mathcal{L}_{CW}(x', t)$, and $r = x' - x$. This iterative procedure is repeated until the S -constrained L_2 attack fails to find an adversarial example, at which time the latest successful adversarial example is returned. To speed up this iterative algorithm, the authors suggested to “warm-start” each L_2 attack attempt by using the latest adversarial example found in previous iteration, which is pre-modified to satisfy the reduced S set. Intuitively, the selection criterion $g_{(i)} \cdot r_{(i)}$ quantifies how much the loss value is affected by perturbing the i -th feature. Thus, eliminating i^* with the minimum criterion score has the least amount of impact on potential misclassification.

Similar to the L_0 C&W attack, the L_∞ attack variant also requires an iterative algorithm, since the L_∞ metric is not fully differentiable. Its optimization objective is given as:

$$\arg \min_r \left(c \cdot \mathcal{L}_{CW}(x + r, t) + \sum_i \max(0, r_{(i)} - \tau) \right). \quad (15)$$

The parameter τ is initialized to 1, and is reduced after every iteration by a factor of 0.9 if $r_{(i)} < \tau$ for all i , until no adversarial example is found. In short, this strategy successively constrains the magnitude of adversarial perturbations to be bounded by successively smaller τ . Again, similar to the L_0 attack, warm-start can be used at every iteration to speed up the entire process.

As another practical implementation enhancement for finding robust adversaries, the authors recommend to optimize the scale parameter c empirically rather than fixing it to a constant value. Concretely, in an outer optimization loop, c is first set to a very stringent value (e.g., $c = 10^{-4}$), and then iteratively relaxed via doubling until a first adversary is found.

Carlini and Wagner [44] empirically showed their methods to be superior to the state-of-the-art attacks at the time when evaluated on MNIST, CIFAR10, and ImageNet. In their evaluations, the proposed L_0 attack was compared against JSMA [80] (see Section 4.8), L_2 variant was compared against DeepFool [79] (see Section 4.7), and L_∞ method was compared against FGSM [32] (see Section 4.2) and BIM [45, 77] (see Section 4.3). The three C&W attacks consistently outperformed the incumbents in terms of average distortion and attack success rate. Furthermore, they found that JSMA is too expensive to perform when used on ImageNet models since the dimension of ImageNet data are much higher compared to MNIST or CIFAR10, while their L_0 method has no difficulty finding adversarial examples on ImageNet. As mentioned previously, the proposed attacks successfully circumvented defensive distillation with 100% success rate, while keeping the adversarial examples to be similar with the original input under L_0 , L_2 , and L_∞ metrics. Finally, the authors also showed that their attacks transfer between models, even to those trained using defensive distillation. They also report that increases in κ lead to increases in transferability, supporting the notion that κ modulates the robustness of examples.

4.12 Universal Adversarial Perturbation

All of the attack methods covered thus far search for adversarial perturbations of a *specific* input instance, such as distorting a particular image of a dog to be misclassified as “cat”. There are no guarantees that such perturbations will remain adversarial when added to a different input instance. In contrast, [83] demonstrated the existence of Universal Adversarial Perturbations (UAP); perturbations that are input-agnostic. They show that a single perturbation can cause misclassification when added to *most* images from a given dataset

(see Fig. 4 for the illustration of UAP). The authors argued that the high adversarial efficacy of UAP indicates the presence of non-random, exploitable geometric correlations in the target model’s decision boundaries.

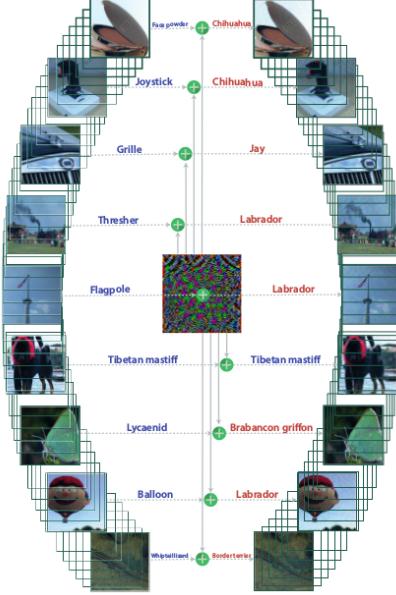


Figure 4: Illustration of UAP (taken from Moosavi-Dezfooli et al. [83]).

UAP works by accumulating perturbations calculated over individual inputs. As shown in Algorithm 5, this meta-procedure runs another *sample-specific* attack (e.g., FGSM [32]) within a loop to incrementally build a sample-agnostic UAP, v . In each iteration, an universally-perturbed input sample $x_i + v$ is further altered by Δv_i via a per-sample attack method. Then, the universal perturbation is adjusted to account for Δv_i , all-the-while satisfying a maximum bound ϵ on the p -norm of the UAP. In this manner, the resulting v can be added to *each* data sample in order to push them towards a nearby decision boundary of the target model. This meta-attack procedure is repeated until the portion of samples that are misclassified, e.g., the “fooling rate”, exceeds a desired threshold ($1 - \delta$).

Algorithm 5 Universal Adversarial Perturbation [83]

```

Input: input-label pairs  $(x_i, y_i)$  from a dataset  $X$  of  $|X| = N$  entries, target classifier  $f$ , maximum  $L_p$  norm constraint  $\epsilon$ , minimum desired fooling rate  $(1 - \delta)$ 
Output: universal adversarial perturbation  $v$ 
Initialize:  $v \leftarrow \{0, 0, \dots\}$ 
while fooling rate $_X \leq 1 - \delta$  do
    for  $i = 1$  to  $N$  do
        if  $f(x_i + v) == y_i$  then
             $\Delta v_i \leftarrow \arg \min_r \|r\|_2$  such that  $f(x_i + v + r) \neq y_i$ 
             $v_i \leftarrow v + \Delta v_i$ 
             $v \leftarrow \arg \min_{v'} \|v_i - v'\|_2$  such that  $\|v'\|_p \leq \epsilon$ 
        end if
    end for
end while
Return:  $v$ 

```

Algorithm 5 is slightly modified from Moosavi-Dezfooli et al. [83], in that we only update v when an

universally-perturbed sample $x_i + v$ is correctly classified (i.e., $f(x_i + v) == y_i$). The original formulation considered all samples that did not change prediction labels $f(x_i + v) == f(x_i)$. These two variants differ only for x_i s that are misclassified by the target model, i.e., $f(x_i) \neq y_i$. Our practical stance is that such data samples *do not need to be perturbed further* to be adversarial, and that further perturbations might actually *make them non-adversarial*, i.e., $f(x_i + v) == y_i$.

The authors demonstrated existence of UAPs for various models including CaffeNet [112], GoogLeNet [42], ResNet-152 [6], and several variants of VGG [113, 122] with fooling rates as high as 93.7% for the ImageNet validation dataset. UAP was also shown to be highly transferable between these models. This method was subsequently extended to find UAP that fools semantic segmentation models [123].

One potential deficiency of Algorithm 5 is that it does not guarantee that each updated UAP v will still be adversarial to data points that appear before the update. Indeed, the proposed method may need to iterate over the same dataset multiple times before it can attain a high desired fooling rate. It would be interesting for future research to identify a UAP variant that can update v without weakening its adversarial nature on previously-seen data samples.

Additionally, we observe there is no mandatory need for Algorithm 5 to enforce L_2 norms, both when computing the per-instance perturbation Δv_i , and when updating v towards v_i . While this choice of norm may be indirectly supported by related bounds for random perturbations in the authors' comparative analyses, it is nevertheless not fully justified. We argue that the UAP meta-attack procedure has two key objectives: finding a robustly-adversarial (i.e., one that confidently mis-classifies the target model) universal perturbation, while being perceptually indistinguishable as quantified by an imposed L_p -norm constraint, $\|v\|_p \leq \epsilon$. When $p \neq 2$, the per-instance attack might find an adversarial perturbation $v + \Delta v_i$ that could arbitrarily violate the latter constraint, and much of its adversarial robustness might be subsequently lost when updating v towards v_i .

To address the above concern, we suggest that Algorithm 5 could be updated to use a per-instance adversarial attack that optimized a matching L_p norm constraint, and also update v as $\arg \min_{v'} \|v_i - v'\|_p$. This might then mitigate the need to re-enforce the ϵ constraint explicitly. This meta-procedure could be further generalized to consider, on each update step, a multitude of adversaries generated by diverse per-instance attacks. One might then be able to choose an update direction for v such that its adversarial robustness is increased while always preserving the stipulated L_p constraint. We encourage the readers to substantiate this conjecture.

4.13 Data-Free UAP

As an extension of UAP [83] (see Section 4.12), Mopuri et al. [84, 124] proposed a new algorithm to generate UAP without requiring access to the training data (i.e., data-free).² The Data-Free UAP (DFUAP) method aims to find an universal perturbation v that saturates all activations of a neural network *by itself*, by minimizing the following loss:

$$\mathcal{L}_{DF} = -\log \left(\prod_{i=1}^L \|f_{l_i}(v)\|_2 \right). \quad (16)$$

Here, $f_{l_i}(v)$ denotes the activations of the model f at the i -th layer (among L total layers), given v as the entire input. As is common for adversarial attacks, a perceptual similarity constraint ϵ is imposed on the magnitude of v under the ∞ -norm, i.e., $\|v\|_\infty < \epsilon$.

To implement the above optimization, v is initialized randomly, and then updated via gradient descent while constrained by the ∞ -norm bound. Also, the authors empirically found that minimizing *a small subset* of activations (e.g., only convolutional layers, or only the last layers of convolutional blocks) resulted in similar fooling rates compared to minimizing *all* activations, thus the former objective should be used in practice for efficiency sakes.

²We mainly focus on the variant proposed by [84], as it improves upon [124].

Although DFUAP was designed to be completely agnostic of training data, it can be slightly altered to take advantage of prior knowledge on the training data when available. For instance, Mopuri et al. [84] suggested how one can leverage information such as the mean of a dataset, dynamic range of the dataset (e.g., [0, 255] for 8-bits RGB images), or samples of the training data. Concretely, in the case where the mean of the training data and dynamic range of the input are available, the loss function can be changed to:

$$\mathcal{L}_d = - \sum_{d \sim \mathcal{N}(\mu, \sigma)} \log \left(\prod_{i=1}^L \|f_{l_i}(d + v)\|_2 \right), \quad (17)$$

where d denotes a random perturbation sampled from Gaussian distribution with mean μ and variance σ such that d lies within the dynamic range of the input. Alternatively, if some training samples $x \in X$ are available, then the loss could be modified to:

$$\mathcal{L}_x = - \sum_{x \sim X} \log \left(\prod_{i=1}^L \|f_{l_i}(x + v)\|_2 \right). \quad (18)$$

Although in general DFUAP is not as effective at fooling the target model as the UAP generated by [83], this method can be significantly faster to compute, since one does not have to iterate through the entire dataset. Mopuri et al. [84] also showed that this method can be used to attack semantic image segmentation (e.g., FCN [8]) and depth estimation (e.g., Monodepth [125]) models. Furthermore, [83] showed that the fooling rate of the data-free UAP method is comparable to the original UAP method when data prior is available. Perhaps more interestingly, they showed that the original UAP method only outperformed the data-free method when the dataset size was sufficiently large (e.g., at least 10,000 images for ImageNet-level models such as the GoogLeNet [42] or CaffeNet [112]).

4.14 VAE Attacks

Although the majority of work in the field has focused upon fooling classifiers, recent research has extended adversarial attacks to generative models. Kos et al. [85] focus upon the scenario where a generative model is being used as a sophisticated compression mechanism, allowing a sender and receiver to efficiently exchange information using a shared latent space. Concretely, a sender takes an input image, encodes it with the model, and sends the receiver the latent code. The receiver uses the same model to decode from this latent representation to an output image. In this case, an adversarial example would be one that is poorly reconstructed after encoding and decoding through the model.

Kos et al. [85] describe ways to find adversarial examples for models like the Variational Autoencoder (VAE) [86] and VAE-GAN [126]. The authors proposed three separate strategies: classifier attack, \mathcal{L}_{VAE} attack, and latent attack. These methods apply to models that specifically have an encoder and a decoder component, which respectively, compresses the input x into a latent representation z , and reconstructs the input \hat{x} from z , i.e., $z = f_{enc}(x)$ and $\hat{x} = f_{dec}(z)$.

The simplest method, the classifier attack, augments the frozen generative model (e.g., VAE or VAE-GAN), by training a new classifier network $y = f_{classifier}(f_{enc}(x))$, and then applies an existing algorithm like FGSM [32] (see Section 4.2) to find adversaries x' . During the process, this approach also alters the latent encoding z into an adversarial counterpart z' such that the decoder $f_{dec}(z')$ produces poor reconstructions \hat{x}' . Nevertheless, there are no general guarantees that success in fooling the classifier will result in fooling the decoder.

The setup of the second attack method, \mathcal{L}_{VAE} attack, involves altering the loss function for training a VAE:

$$\mathcal{L}_{VAE}(x, \hat{x}) = -KL(q(z|x) || p(z)) + E_q [\log p(\hat{x}|z)], \quad (19)$$

where $KL(\cdot)$ denotes the Kullback-Leibler divergence [127], $q(z|x)$ denotes an analytical approximation for the underlying conditional latent distribution $p(z|x)$, $p(z)$ is a prior distribution of z that is assumed to

be Gaussian, and $E_q[\log p(x|z)]$ is the evidence lower bound (ELBO), which in this setup entails the cross-entropy loss between the input x and its reconstruction \hat{x} .

When training a VAE normally, the reconstruction target \hat{x} of $\mathcal{L}_{VAE}(\cdot)$ is naturally set to the output of the encoder-decoder networks, i.e., $\hat{x} = f_{dec}(f_{enc}(x))$. However, this loss metric can be altered to quantify the gap between a given input x , and the reconstruction of another *adversarial target* input \hat{x}_t . Subsequently, an optimization formulation resembling methods such as the L-BFGS attack [31] (see Section 4.1) can be formulated as:

$$\arg \min_{x'} (c\|x - x'\|_2 + \mathcal{L}_{VAE}(x', \hat{x}_t)) \text{ such that } x' \in [0, 1]. \quad (20)$$

Similar to the L-BFGS attack, the scaling parameter c is initially set to a small value, and then incrementally increased via line search till an adversary is found. This outer optimization loop ensures that the resulting adversary strictly enforces the $\mathcal{L}_{VAE}(x', \hat{x}_t)$ loss.

The third strategy, latent attack, differs in the goal of matching $f_{enc}(x')$ to an adversarial target *latent vector* z_t , in contrast to the \mathcal{L}_{VAE} attack's aim of matching the reconstructions between x' and an adversarial target *input* x_t . To this end, a different loss function is used:

$$\mathcal{L}_{latent}(x', z_t) = \|f_{enc}(x') - z_t\|_2, \quad (21)$$

while the adversarial optimization process remains the same:

$$\arg \min_{x'} (c\|x - x'\|_2 + \mathcal{L}_{latent}(x', \hat{x}_t)) \text{ such that } x' \in [0, 1]. \quad (22)$$

Kos et al. [85] showed that the above attack strategies successfully fool VAE and VAE-GAN on various datasets such as MNIST [116], SVHN [128], and CelebA [129]. However, the classifier attack produces lower quality reconstructions than the \mathcal{L}_{VAE} and latent attacks, which may be due to the fact that the classifier itself is easier to fool compared to the generative model. The authors also report that the \mathcal{L}_{VAE} attack was the slowest since this method builds a reconstruction at every iteration, whilst the latent attack was found to be the most effective.

Although these attacks are meant to fool generative reconstruction models rather than discriminative classification models, some adversarial defense techniques use similar generative models to remove adversarial perturbations from an input, such as PixelDefend [53] (see Section 6.1.11) and DefenseGAN [52] (see Section 6.1.12). Consequently, knowing that generative models can also be attacked may alert one from naively favoring generative models as a defense strategy.

4.15 Adversarial Transformation Networks

Instead of using optimizers like L-BFGS attack directly (see Section 4.1), Adversarial Transformation Networks (ATN) [87] are neural networks that either transform encode-and-reconstruct non-adversarial inputs into adversarial counterparts, or generates an additive adversarial perturbation given a specific input. Once trained, the network can swiftly generate new adversarial examples. The former variant, the Adversarial Auto-Encoding (AAE) network, is depicted in Fig. 5a, which contrasts with the latter Perturbation ATN (P-ATN) model, as seen in Fig. 5b.

Given a pre-trained target classifier network f , in both variants the generator G is trained to minimize:

$$\mathcal{L}_x(x, x') + \alpha \mathcal{L}_y(f(x'), r(y, t)), \quad (23)$$

where \mathcal{L}_x enforces perceptual similarity between x and x' ³, while \mathcal{L}_y forces the softmax probabilities of the perturbed input, $f(x')$, to match an adversarial class distribution $r(y, t)$. The scaling hyper-parameter α is either set heuristically or empirically optimized to adequately balance between the perceptual similarity and adversarial misclassification objectives.

³While the original authors used L_2 metrics for \mathcal{L}_x and \mathcal{L}_y , this is not a mandatory requirement, as others have found adversaries using other similarity metrics, such as L_2 loss in feature space [130, 131].

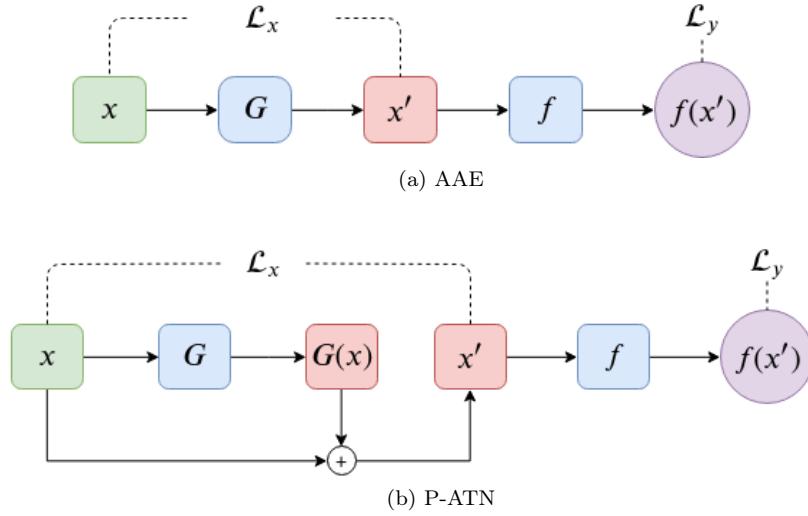


Figure 5: Illustrations of AAE and P-ATN.

One naive instantiation of ATN is to set the adversarial class distribution $r(y, t)$ to a one-hot encoding of t , as when training normal classification models. Nevertheless, the authors proposed a more effective *reranking* function, whose k -th components are minimally different from the softmax probabilities of the pre-trained classifier $f(x)_{(k)}$:

$$r(y, t)_{(k)} \propto \begin{cases} \beta \cdot \max(f(x)) & \text{if } k = t \\ f(x)_{(k)} & \text{otherwise} \end{cases} \quad (24)$$

Since the $\beta > 1$ hyper-parameter enhances the desired confidence for the adversarial class, in general $r(y, t)$ needs to be vector-re-normalized. It is important to note that each trained ATN generator can only produce adversarial examples that will be misclassified as a particular class by the targeted model. Multiple ATNs must be trained in order to fool a given classifier into diverse adversarial classes.

Baluja and Fischer [87] found that the transferability of adversarial examples generated by ATN is fairly poor, but can be enhanced by training the ATN to fool multiple networks at the same time (e.g., the gradients coming from attacking multiple networks are averaged during backpropagation). ATN exhibits some benefits that other attack methods are lacking: for instance, since ATN takes advantage of the expressiveness of neural networks, the adversarial examples generated by ATN tend to be more diverse. This diversity of adversarial examples can also be leveraged for adversarial training [32] (see Section 6.1.1). Similar to preliminary investigations by Hamm [132], a future interesting research direction is to formulate a min-max game between a classifier and an ATN that can provide some *guarantee* of the classifier’s robustness, by learning from diverse sets of adversarial examples generated by the ATN without suffering from catastrophic forgetting [133] between training iterations.

4.16 Dense Adversary Generation

Dense Adversary Generation (DAG) [88] is a targeted attack method for semantic image segmentation and object detection models. DAG generalizes from attacks on classification models in that it aims to misclassify *multiple target outputs* associated to each given input, namely multiple pixel labels for semantic segmentation tasks, or multiple region proposals for object detection tasks. DAG requires both the ground truth class labels as well as specific adversarial labels for every target output of a given model. Using this information, DAG incrementally builds an adversarial input perturbation r that decreases the predicted logits for the

true classes while increasing the logits for the adversarial labels among target outputs, thus resulting in as many misclassified outputs as possible.⁴

Formally, given an image x , we expand the definitions of the logit vectors $Z(x, \tau)$, softmax probabilities $f(x, \tau)$, and predicted class labels $\hat{y}_\tau(x) = \arg \max_c f(x, \tau)_{(c)}$ to be specific to each of the target outputs $\tau \in 1 : N$ of the target model. As shown in Algorithm 6, the input x is incrementally perturbed by r'_i into x'_{i+1} on each iteration i . To compute each such perturbation, first DAG identifies the set of target outputs \mathcal{T} that are still correctly classified by the model given x'_i . Among each $\tau \in \mathcal{T}$, the r_i vector is then built by accumulating the positive input-gradients of logits for output-specific adversarial classes $\{t_n\}$, i.e., $\nabla_{(x'_i)} Z_{(t_n)}(x'_i, \tau)$, as well as the negative input-gradients of the true-class logits, $\nabla_{(x'_i)} Z_{(y_n)}(x'_i, \tau)$. This resulting perturbation r_i , when added to x'_i , has the effect of amplifying the likelihoods for predicting adversarial classes over true classes among the non-misclassified outputs, thus will likely result in more misclassified outputs overall. For numerical stability, the authors recommend to down-scale r_i by an adversarial gain hyper-parameter γ , e.g., $\gamma = 0.5$. This iterative procedure is repeated for a fixed number of iterations I_{max} , which is empirically set to $I_{max} = 200$ for semantic segmentation tasks and $I_{max} = 150$ for object detection tasks.

Algorithm 6 Dense Adversary Generation [88]

```

Input: input image  $x$ , model  $f$ , ground truth output-specific labels  $\{y_1, \dots, y_N\}$ , adversarial labels  $\{t_1, \dots, t_N\}$ , adversarial gain  $\gamma$ , maximum number of iterations  $I_{max}$ 
Output: adversarial perturbation  $r$ 
Initialize:  $r = \{0, 0, \dots\}$ ,  $i = 0$ ,  $x'_0 \leftarrow x$ ,  $\mathcal{T} \leftarrow \{1, \dots, N\}$ 
while  $i < I_{max}$  and  $\mathcal{T} \neq \emptyset$  do
     $\mathcal{T} = \{\tau : \hat{y}_\tau(x_i) == y_\tau, \tau \in 1 : N\}$ 
     $r_i \leftarrow \sum_{\tau \in \mathcal{T}} [\nabla_{(x'_i)} Z_{(t_n)}(x'_i, \tau) - \nabla_{(x'_i)} Z_{(y_n)}(x'_i, \tau)]$ 
     $r'_i \leftarrow \frac{\gamma}{\|r_i\|_\infty} r_i$ 
     $r, x'_{i+1} \leftarrow r + r'_i, x'_i + r'_i$ 
     $i \leftarrow i + 1$ 
end while
Return:  $r$ 

```

The authors showed that DAG can be used to attack various Fully Convolutional Networks (FCN) [8] for semantic segmentation tasks, as well as some variants of Faster-RCNN [15] for object detection tasks. Intriguingly, the generated adversarial perturbations for attacking a semantic segmentation model can also be used to fool an object detection model, and vice-versa. This transfer is particularly effective when both models employ the same convolutional backbone (e.g., both FCN and Faster-RCNN models use a VGG16 architecture).

In practice, for object detection models, the authors noted that region proposal target outputs often change drastically when different perturbations are added. Consequently, they heuristically recommend to consider only outputs that have an Intersection over Union (IoU) with the closest ground truth object that is larger than 0.1 along with a confidence score greater than 0.1. If there are several target outputs belonging to the same object satisfy both conditions, only the one with the largest IoU is considered. This heuristic assumes that the changes in values among nearby region proposals will transfer to each other accordingly.

4.17 Zeroth Order Optimization

Chen et al. [89] introduced a blackbox attack method called the Zeroth Order Optimization (ZOO). Given only the capability to query a target model, ZOO approximates the gradients of the objective function with respect to the input using finite-difference numerical estimates. Unlike other methods that use stochastic

⁴While the original formulation for DAG computes input-gradients targeting the logit layer $Z(x, \tau)$ rather than targeting the normalized softmax probabilities $f(x, \tau)$, there is no fundamental limitation to forbid undertaking the latter variant. Nevertheless, as shown by Carlini and Wagner [44] and others, in certain setups such as with defensively-distilled models [43], attack methods that operate on the logit layer tend to be significantly more successful than those targeting the softmax layer.

gradient descent [134], ZOO employs stochastic coordinate descent [135] over small batches of input dimensions per iteration, to avoid calculating derivatives with respect to all input features (e.g., all pixels of an image).

Two ZOO variants were introduced: ZOO-Adam and ZOO-Newton. ZOO-Adam uses first-order approximations for calculating the derivatives and then use the Adam optimizer [136] to update the input. Given a particular loss function $\mathcal{L}(x)$ to optimize for misclassification, the coordinate-wise Jacobian is estimated as:

$$J_i = \frac{\partial \mathcal{L}(x)}{\partial x_{(i)}} \approx \frac{\mathcal{L}(x + h \cdot e_i) - \mathcal{L}(x - h \cdot e_i)}{2h}, \quad (25)$$

where $x_{(i)}$ is the i -th element of the input x , h is a small constant (e.g., $h = 10^{-10}$), and e_i is an elementary vector where only the i -th element is set to 1 while other entries are 0. The algorithm for ZOO-Adam can be found in Algorithm 7.

Algorithm 7 ZOO-Adam [89]

Input: original input $x \in \mathbb{R}^n$, model f , learning rate α , Adam hyper-parameters $\beta_1, \beta_2, \epsilon$

Output: adversarial input x'

Initialize: first-moment vector estimate for Adam $m \leftarrow \{0, \dots, 0\}^n$, second-moment vector estimate for Adam $v \leftarrow \{0, \dots, 0\}^n$, per-coordinate timestep for Adam $t \leftarrow \{0, \dots, 0\}^n$, $x' \leftarrow x$

while x' is not adversarial **do**

 set e_i by randomly choosing coordinate $i \in \{1, \dots, n\}$

$$J_i \leftarrow \frac{\mathcal{L}(x + h \cdot e_i) - \mathcal{L}(x - h \cdot e_i)}{2h}$$

 update Adam estimates and compute δ :

$$t_{(i)} \leftarrow t_{(i)} + 1$$

$$m_{(i)} \leftarrow \beta_1 m_{(i)} + (1 - \beta_1) J_i$$

$$v_{(i)} \leftarrow \beta_2 v_{(i)} + (1 - \beta_2) J_i^2$$

$$\hat{m}_{(i)} \leftarrow \frac{m_{(i)}}{1 - \beta_1^{t_{(i)}}}$$

$$\hat{v}_{(i)} \leftarrow \frac{v_{(i)}}{1 - \beta_2^{t_{(i)}}}$$

$$\delta \leftarrow -\alpha \frac{\hat{m}_{(i)}}{\sqrt{\hat{v}_{(i)}} + \epsilon}$$

$$x'_{(i)} \leftarrow x'_{(i)} + \delta$$

end while

Return: x'

On the other hand, ZOO-Newton employs second-order approximations for derivatives, and thus additionally requires estimates for the coordinate-wise Hessian:

$$H_i = \frac{\partial^2 \mathcal{L}(x)}{\partial x_i^2} \approx \frac{\mathcal{L}(x + h \cdot c_i) - 2\mathcal{L}(x) + \mathcal{L}(x - h \cdot c_i)}{h^2}. \quad (26)$$

Algorithm 8 demonstrates how ZOO-Newton works.

In both algorithms, one component of the algorithm remains to be specified: the adversarial loss function $\mathcal{L}(\cdot)$. The authors presented both a targeted variant (with adversarial target class t) as well as a non-targeted version (with y as the ground truth label), with κ being a minimal confidence gap hyper-parameter:

$$\mathcal{L}^{targeted}(x, t) = \max \left\{ \max_{i \neq t} \log(f(x)_{(i)}) - \log(f(x)_{(t)}), -\kappa \right\}, \quad (27)$$

$$\mathcal{L}^{non-targeted}(x) = \max \left\{ \log(f(x)_{(y)}) - \max_{i \neq y} \log(f(x)_{(i)}), -\kappa \right\}. \quad (28)$$

While these loss functions are inspired and thus similar to those used in the C&W attack [44] (see Section 4.11), the authors argued that the use of the log transform of $f(x)$ was important to reduce the potentially

Algorithm 8 ZOO-Newton [89]

Input: original input $x \in \mathbb{R}^n$, model f , learning rate α
Output: adversarial output x'

```

while  $x'$  is not adversarial do
    set  $e_i$  by randomly choosing coordinate  $i \in \{1, \dots, n\}$ 
     $J_i \leftarrow \frac{\mathcal{L}(x+h \cdot e_i) - \mathcal{L}(x-h \cdot e_i)}{2h}$ 
     $H_i \leftarrow \frac{\mathcal{L}(x+h \cdot e_i) - 2\mathcal{L}(x) + \mathcal{L}(x-h \cdot e_i)}{h^2}$ 
    if  $H_i \leq 0$  then
         $\delta \leftarrow -\alpha J_i$ 
    else
         $\delta \leftarrow -\alpha \frac{J_i}{H_i}$ 
    end if
     $x'_i \leftarrow x'_i + \delta$ 
end while
Return:  $x'$ 
```

large differences in prediction scores between the best class and its runner-up. Another difference with the loss functions of ZOO and C&W is that the former targets the softmax layer, while the latter targets the logit layer. While the authors compared ZOO to C&W attacks, it would nevertheless be interesting to evaluate variants of ZOO where the loss functions are computed with respect to logits $Z(x)_{(i)}$ rather than softmax probabilities $f(x)_{(i)}$.

Several suggestions were made to increase the efficiency of ZOO. First, [89] suggested to perform dimensionality reduction on the attack space using bilinear interpolation or discrete cosine transformations [137]. Although this trick reduces the computational costs, note that it also lowers the chance of finding adversarial examples. The authors thus proposed a hierarchical attack scheme, which gradually increasing the attack space dimensionality every several number of iterations until satisfactory examples are found. Second, when the attack space dimension is large, importance sampling can be used to only update the most influential coordinates, as a further optimization heuristic. This can be realized by first dividing an input into 8 by 8 pixel regions, where each region is assigned a sampling probability. At the beginning of attack process, sampling probabilities for each region are assigned uniformly. During the attack process, after every few iterations, these probabilities are calculated by performing max pooling on the absolute pixel value changes in each region, which are then normalized to $[0, 1]$ in order to get the probability values.

Although ZOO algorithms are empirically slower compared to the SBA [41] (see Section 4.9), Chen et al. [89] showed that ZOO are more effective in terms of attack success rate on models that rely on defensive distillation [43] (see Section 6.1.3), and comparable even to C&W attacks [44].

4.18 One-Pixel Attack

The One-pixel Attack (OPA) [90] is a “semi-blackbox” method⁵ that uses an Evolutionary Algorithm strategy called Differential Evolution [138, 139] to find adversarial perturbations. OPA aims to fool the target model by modifying as few as one feature of a given image x . In practice the authors have shown high misclassification rates for diverse models and datasets by perturbing only 3 or 5 pixels.

Concretely, given an image x , an N -pixel attack works by evolving a population of candidate modifications over many generations to ultimately home in onto a globally-optimal solution. Each candidate r is represented as a N -tuple of coordinates and values to be modified from x . For example, a candidate in a 3-pixel attack on an RGB image consists of a vector of (3 pixels) \times ((2 coordinates) + (3 intensity values)) = 15 elements.

⁵The authors coined the term “semi-blackbox” to denote the requirements of needing both the predicted classes $\hat{y}(x)$ and the softmax prediction probabilities $f(x)$ from the target model. This semantic designation is questionable, as only some blackbox models in practice provide prediction probabilities.

A “fitness function” $F(x \oplus r)$ quantifies the optimality of a resultant image after applying (\oplus) the modification r onto the source image x . OPA can be instantiated as either a targeted attack or a non-targeted one, which differ only in their fitness functions. Notably, the former fitness function is the model’s softmax prediction probability for a specified adversarial class t , i.e., $F(\cdot) = f(x \oplus r)_{(t)}$, while the latter fitness function for a non-targeted attack is the *negative* of the softmax probability for the ground-truth class y , i.e., $F(\cdot) = -f(x \oplus r)_{(y)}$.

As summarized in Algorithm 9, a population of $P = 400$ candidates is initialized randomly, with pixel coordinates sampled uniformly and 8-bit intensity values sampled from Gaussian distributions $\mathcal{N}(\mu = 128, \sigma = 127)$. This population is evolved for up to $I_{max} = 100$ generation. An early-stopping heuristic is also employed when a sufficiently large portion of the population becomes adversarial. During the i -th generation, the p -th candidate is evolved by choosing the modification with greater fitness between either the existing vector r_p^i or a donor mutation r' combined from 3 other distinct candidates:⁶

$$r_p^{i+1} = \arg \max \left(F(x \oplus r_p^i), F(x \oplus r') \right), \text{ where } r' = r_{p_1}^i + \lambda(r_{p_2}^i - r_{p_3}^i); p_1 \neq p_2 \neq p_3 \in \{1, 2, \dots, P\}, \quad (29)$$

and $\lambda = 0.5$ is a scaling hyper-parameter.

Algorithm 9 Targeted Variant of One-Pixel Attack [90]

Input: input x , model f , target class label t , population size P , maximum number of generations I_{max} , mutation scale λ , minimum population ratio of adversarial examples for early-stopping ρ

Output: adversarial output x'

define fitness function $F(x') \leftarrow f(x')_{(t)}$

randomly initialize population $\{r_p^1\}$ for $p \in \{1, 2, \dots, P\}$

$i \leftarrow 0$

while $i < I_{max}$ **do**

$i \leftarrow i + 1$

for $p \in \{1, 2, \dots, P\}$ **do**

 sample distinct $p_1, p_2, p_3 \in \{1, 2, \dots, P\}$ such that $p_1 \neq p_2 \neq p_3$

$r' \leftarrow r_{p_1}^i + \lambda(r_{p_2}^i - r_{p_3}^i)$

$r_p^{i+1} = \arg \max \left(F(x \oplus r_p^i), F(x \oplus r') \right)$

end for

if ratio of $\{p : \hat{y}(x \oplus r_p^i) == t, p \in \{1, 2, \dots, P\}\} \geq \rho$ **then**

break

end if

end while

Return: $\arg \max_{x'} \{F(x') : x' = x \oplus r_p^i, p \in \{1, 2, \dots, P\}, \hat{y}(x') == t\}$

As practical considerations, each donor mutation vector r' should be clipped to be within the respective bounds for pixel dimensions and intensity values. Also, all pixel intensity values should be discretized to the same resolution as x , e.g., 8-bits.

The authors showed that many images in CIFAR10 [120] and ImageNet [1, 2] can be minimally modified to fool various classification models, such as the All Convolutional Net [140], Network in Network [117], VGG16 [122], and AlexNet [3].

⁶The proposed OPA procedure [90] is a simplified variant of the standard Differential Evolution algorithm [139] in that there is no crossover mutation between the existing candidate r_p^i and the donor r' . Also, Das and Suganthan [139] prescribes the 3 randomly sampled candidates to be distinct from the existing candidate as well, i.e., $p \neq p_1 \neq p_2 \neq p_3$. Nevertheless, we have empirically corroborated that the simplified evolutionary strategy used by OPA can successfully find adversaries, despite possibly suffering from reduced search efficiency.

4.19 Houdini

All optimization-based adversarial attacks operate by maximizing an *attack loss* $\ell^{atk}(x', y)$, such as the distance between the model prediction $\hat{y}(x')$ versus the ground-truth target y , while constrained by a perceptual bound $\|x' - x\|_p \leq \epsilon$ of the input perturbations:

$$x' = \arg \max_{x'' : \|x'' - x\|_p \leq \epsilon} \ell^{atk}(x'', y)$$

Typically, the attack loss ℓ^{atk} is derived from the *training loss* $\ell^{train} = \mathcal{L}(f(x'), y)$ of a given model f . For most tasks, since \mathcal{L} is differentiable, this has the convenient consequence of allowing attacks to use efficient gradient-based optimization strategies. Nevertheless, to generate robust adversaries, one should ideally choose an attack loss ℓ^{atk} that maximally damages the *evaluation criterion* ℓ^{eval} , which is different from the training loss for some family of tasks such as structured prediction. This poses a technical challenge for the attack however, as often the evaluation metric is non-differentiable and even combinatorial. For example, while semantic segmentation models are trained to minimize per-pixel misclassification error, they are evaluated using the mean Intersection-Over-Union (mIOU) ratio across classes. The latter metric is more desirable as it does not exhibit over-confidence for imbalanced class labels [91].

To address the above challenge, Cissé et al. [91] introduced a differentiable surrogate attack loss, called Houdini ℓ_H , for efficiently generating adversarial examples in structured prediction tasks. This is achieved by combining a non-differentiable evaluation metric ℓ^{eval} with a stochastic margin on $\delta(x, y) = f(y) - f(\hat{y}(x))$:

$$\ell_H(x, y) = \mathbb{P}_{\gamma \sim \mathcal{N}(0, 1)} [\delta(x, y) < \gamma] \cdot \ell^{eval}(x, y) = \frac{1}{\sqrt{2\pi}} \int_{\delta(x, y)}^{\infty} e^{-\frac{v^2}{2}} dv \cdot \ell^{eval}(x, y), \quad (30)$$

where γ is a random variable following a unit Gaussian distribution $\mathcal{N}(0, 1)$. Importantly, this formulation assumes that the victim model f generates a numeric (e.g., probability) *score map* $f(y')$ over all possible output values y' . For classification tasks, $f(y' = c)$ pertains to the softmax probability of a specified output class c . More complex score maps also exist for structured prediction tasks such as semantic segmentation, which we will clarify when presenting concrete examples below.

The form of Equation 30 is less important in practice than its derivative. Since the stochastic margin is expressed as an *integral* of an exponential term, its *derivative* shares the integrand's form. Thus, the input-Jacobian of the Houdini loss decomposes into a total-derivative sum of products, each containing a Houdini-specific partial derivative and a standard network backpropagation term:

$$\nabla_x \ell_H(x, y) = \sum_{y'} \frac{\partial \ell_H(x, y)}{\partial f(y')} \frac{\partial f(y')}{\partial x}, \quad (31)$$

with the first term given as:

$$\frac{\partial \ell_H(x, y)}{\partial f(y')} = \begin{cases} -\frac{1}{\sqrt{2\pi}} e^{-\frac{\delta(x, y)^2}{2}} \cdot \ell^{eval}(x, y), & y' = y \\ \frac{1}{\sqrt{2\pi}} e^{-\frac{\delta(x, y)^2}{2}} \cdot \ell^{eval}(x, y), & y' = \hat{y}(x) \\ 0, & \text{otherwise.} \end{cases} \quad (32)$$

This input-Jacobian can be used to maximize the attack loss $\ell_H(x, y)$ using non-targeted methods such as the FGSM [32] (see Section 4.2). Alternatively, one can apply it to minimize the attack loss $\ell_H(x, t)$ of an adversarial class $t \neq y$, using algorithms such as JSMA [80] (see Section 4.8).

A desirable property of the Houdini loss is that it is consistent with the task evaluation criterion, and thus choosing an input perturbation x' that optimizes ℓ_H would adversarially impact $\ell^{eval}(x', y)$. Moreover, even when a perturbation x' does not change ℓ^{eval} (e.g., due to discretization), the gradients in Equation 32 *smoothly* point towards the direction that reduces the score gap δ between the predicted output $\hat{y}(x')$ and the true target y .

The authors demonstrated attacks using the Houdini loss for three structured prediction setups. Firstly, consider a human pose estimation task, where the goal is to use an input image to predict image-plane

positions of human body keypoints, namely neck, wrists, elbows, knees, and ankles. A family of models tackle this problem by generating a sequence of confidence maps for each body part, and predicting the location of each keypoint as maximally-confident coordinates [141, 142]. Even though these models can be trained using smooth losses such as the Mean Squared Error (MSE), in contrast the standard evaluation metric, namely the Percentage of Correctly-detectable Keypoints (PCKh), rejects all hypotheses that are not within an epsilon neighborhood of ground truth positions. Despite having this non-differentiable ℓ_{eval} , the Houdini loss can be used, by considering $f(y')$ to be the *product of (normalized) confidences of a set of body part keypoints* y' . The authors successfully demonstrated both non-targeted as well as targeted attacks using the Houdini loss with the Fast Gradient Value (FGV) method [82] (see Section 4.2).

The second example focuses on semantic segmentation tasks, which labels each pixel in an input image of a natural scene as one of different semantic classes, such as sky, road, and pedestrian. A number of semantic segmentation models are trained using per-pixel classification cross-entropy loss, while prediction performance is evaluated on across-class mIOU ratios instead. The Houdini loss augments mIOU by comparing the *across-pixel product of class probabilities* between the prediction and ground truth maps. While the Dense Adversarial Generation (DAG) method [88] (see Section 4.16) can attack these models using the per-pixel cross-entropy training loss ℓ^{train} , Cissé et al. [91] has shown that Houdini-based attacks, both non-targeted and targeted, can find adversaries that achieve equal levels of adversarial damage to mIOU compared to DAG while being more perceptually similar.

The third setup centers around a speech recognition task, where the goal is to predict a text transcript given an input audio spectrogram containing speech segments. Although standard evaluation for speech recognition focuses on Word Error Rate (WER), which is non-differentiable, modern models are trained using a specialized Connectionist Temporal Classification (CTC) loss. Thankfully, since this model is trained to maximize the likelihood of the conditional probabilities of a sequence of text labels l given an input spectrogram x , the Houdini attack loss can combine this smooth probability map with the non-smooth WER evaluation criterion. The authors have thus successfully demonstrated non-targeted attacks, targeted attacks, and even blackbox attacks based on this surrogate loss function ℓ_H .

4.20 Momentum Iterative Fast Gradient Sign Method

Dong et al. [92] proposed a family of improvements to BIM and ILLCM [45, 77] (see Sections 4.3 and 4.4) called the Momentum Iterative Fast Gradient Sign Method (MI-FGSM) by leveraging momentum during optimization process. Momentum terms have been frequently used to accelerate the convergence of iterative optimization processes [143]. When applied to optimization-based adversarial attacks such as FGSM, the authors argued that the use of momentum helps to stabilize the update directions for perturbations, and also helps to escape from weak local maxima and thus resulting in an increase in the adversarial example’s transferability. This work extends upon a previous observation made by [45] that adversarial examples generated by BIM are less transferable compared to FGSM [32] (see Section 4.2), i.e., stronger adversaries are typically less transferable.

The algorithm for non-targeted variant of MI-FGSM is shown in Algorithm 10. Note that the $Clip\{\cdot\}$ function is the same as the one defined in Equation 5 (see Section 4.3). In particular, g_i is a (scaled) exponential moving average term that accumulates the *directions* of gradients rather than their raw values, hence the use of a normalizing denominator $\|\nabla_{x'_i} \mathcal{L}(x'_i, y)\|_1$. This is used to smoothly perturb the adversarial example over iterations, and to prevent strongly oscillatory updates on x'_i .

To further increase transferability and robustness of adversaries, an Ensemble MI-FGSM variant can be used to attack multiple models for the same task (e.g., having the same input and output representations). To achieve consensus, logits from each of the M victim models are combined together, e.g., via $Z^{ens}(x) = \sum_{m=1}^M Z^m(x)$. The ensemble loss function $\mathcal{L}^{ens}(x, y)$ can then be computed using the softmax of $Z^{ens}(x)$.

Yet another variant, MI-FGM, can be constructed by varying how the underlying FGSM works. Rather than constraining FGSM’s perturbations by an ∞ -norm bound, the authors propose to instead use an L_2 constraint:

Algorithm 10 Non-targeted MI-FGSM

Input: original input x , ground truth label y , targeted model f , step size α , max. number of iterations I_{max} , perturbations size ϵ , decay factor μ

Output: adversarial input x'

Initialize: $\alpha = \frac{\epsilon}{I_{max}}$, gradients accumulator $g_0 = 0$

for $i = 0$ **to** I_{max} **do**

$$g_{i+1} \leftarrow \mu \cdot g_i + \frac{\nabla_{x'_i} \mathcal{L}(x'_i, y)}{\|\nabla_{x'_i} \mathcal{L}(x'_i, y)\|_1}$$

$$x'_{i+1} \leftarrow Clip_\epsilon \left\{ x'_i + \alpha \cdot \text{sign}(g_{i+1}) \right\}$$

end for

Return: $x'_{I_{max}}$

$$x'_{i+1} \leftarrow x'_i + \alpha \cdot \frac{\nabla_{x'_i} \mathcal{L}(x'_i, y)}{\|\nabla_{x'_i} \mathcal{L}(x'_i, y)\|_2}, \quad (33)$$

which they called as the Fast Gradient Method (FGM). Note that this is nearly identical to the Fast Gradient Value (FGV) method proposed by [82], which applies a step size α to the non-normalized gradient $\nabla_x \mathcal{L}(x, y)$. Similar to the change from FGSM to FGM, the MI-FGM attack is formulated as:

$$x'_{i+1} \leftarrow Clip_\epsilon \left\{ x'_i + \alpha \cdot \frac{g_{i+1}}{\|g_{i+1}\|_2} \right\}. \quad (34)$$

Finally, also note that all of the above methods can be turned into targeted attacks by changing the target class from y to t and negating the sign of the perturbation, similar to how BIM can be extended to ILLCM.

Dong et al. [92] showed that MI-FGSM enhances the transferability of the adversarial examples compared to both FGSM and BIM when evaluated on various ImageNet models. Furthermore, the use of momentum is argued to let MI-FGSM to have more stable updates. This is substantiated empirically by showing that the attack success rate of MI-FGSM plateaus as the number of iterations increases, while the attack success rate of BIM *decreases* under the same setup. The authors thus argue that BIM easily “overfits” the victim model, which causes the adversaries to be less transferable. Additionally, the Ensemble MI-FGSM variant was shown to further increase the transferability rate, and achieved higher attack success rates against models defended using ensemble adversarial training [47] (see Section 6.1.6). Finally, MI-FGSM attained first-place performances at the NIPS 2017 Competition on Adversarial Attacks and Defenses, under both the targeted and non-targeted attack categories [144].

4.21 AdvGAN

Similar to P-ATN [87] (see Section 4.15), AdvGAN [93] aims to generate adversarial perturbations by using a neural network. The generator G in AdvGAN outputs perturbations r which when added to the original instance x will result in adversarial examples x' . The difference between AdvGAN and P-ATN is that AdvGAN adds a discriminator network D , and trains the generator adversarially as a Generative Adversarial Network (GAN) [63] framework. Fig. 6 illustrates the proposed method. In contrast, whilst P-ATN also employs a generator network, it does not rely on a real/synthetic discriminator for training, and rather uses a custom loss (e.g., L_2) for learning perturbations.

The objective function for the generator consists of several terms, including a classifier loss (\mathcal{L}_{adv}), an anti-discriminator GAN loss (\mathcal{L}_{GAN}), and a hinge loss (\mathcal{L}_{hinge}):

$$\mathcal{L} = \mathcal{L}_{adv} + \alpha \mathcal{L}_{GAN} + \beta \mathcal{L}_{hinge}, \quad (35)$$

where

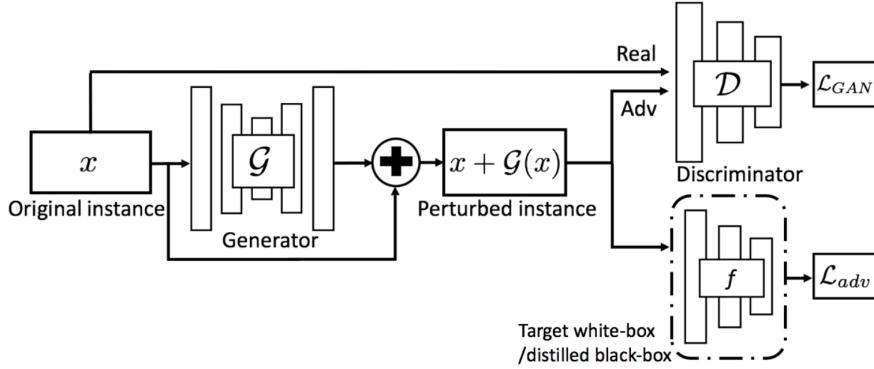


Figure 6: Illustration of AdvGAN (taken from Xiao et al. [93]).

$$\mathcal{L}_{adv} = \mathbb{E}_x[\mathcal{L}_f(x + G(x), t)], \quad (36)$$

$$\mathcal{L}_{GAN} = \mathbb{E}_x[\log D(x)] + \mathbb{E}_x[\log(1 - D(x + G(x)))] \quad (37)$$

$$\mathcal{L}_{hinge} = \mathbb{E}_x[\max(0, ||G(x)||_2 - c)]. \quad (38)$$

Here, α and β are constants that control the weighting of the loss terms, \mathcal{L}_f is the classification loss function used by f (e.g., cross-entropy), t is the target misclassification label, and c is a constant that represents the bound for the hinge loss. These terms together contribute to help generate perturbations that are adversarial (classifier loss), perceptually similar to the real data distribution (GAN loss), and bounded in magnitude (hinge loss).

AdvGAN was shown to achieve greater performance over FGSM [32] and C&W [44] methods when challenged with models defended via adversarial training [32] (see Section 6.1.1), ensemble adversarial training [47] (see Section 6.1.6), and PGD adversarial training [145] (see Section 6.1.5). Also, as a preliminary assessment, the authors evaluated AdvGAN with a modified loss function, $\mathcal{L} = \mathcal{L}_{adv} + ||G(x)||_2$, which is more similar to that of P-ATN, and found that AdvGAN's original loss function attained superior results when tested on the MNIST dataset. Finally, the authors performed a human perceptual study following the procedure described in [146, 147] and concluded that the adversarial examples generated by AdvGAN are perceptually-indistinguishable from real images.

One potential drawback of the presented experiments was that only FGSM adversaries were included in the adversarial training setups. Thus, while AdvGAN was shown to be capable of finding adversaries that circumvent defense methods that stymie FGSM and C&W methods, these may not generalize to broader setups comparing against other baseline adversarial attack and defense methods.

4.22 Boundary Attack

Boundary attack [94] is a blackbox method for finding an adversarial example resembling a source image x . It works by iteratively perturbing another “seed” image x'_0 , belonging to a different class than x , towards and along the decision boundaries between the corresponding class of x and adjacent classes. This method does not utilize the victim model’s input Jacobian $\nabla_x f$, and optimizes instead using a rejection sampling formulation that merely queries the model on various perturbed images, $f(x'_i), i \in \{0, 1, 2, \dots\}$.

This attack can either be targeted or non-targeted, with the sole difference being how the “adversarial” condition is defined. For example, for the non-targeted attack variant, one can for example start from a randomly-sampled image whose class prediction is different from that of x (i.e., adversarial). The boundary attack process perturbs this adversary first towards and then along the decision boundary bordering the

ground truth class of the source image, until ultimately the perturbed adversary minimizes the perceptual difference $d(x, x'_i)$ (e.g., L_2 metric) with respect to x .

Algorithm 11 Targeted Variant of Boundary Attack [94]

```

Input: ( $D$ -dimensional) source input  $x$ , seed input  $x'_0$  with adversarial class, victim model  $f$ , initial hyperparameters  $\epsilon_0$  and  $\delta_0$ , number of stochastic samples  $K$ , max number of iterations  $I_{max}$ 
Initialize:  $i \leftarrow 1$ ,  $\epsilon \leftarrow \epsilon_0$ ,  $\delta \leftarrow \delta_0$ 
while  $i \leq I_{max}$  do
     $isAdversarial = False$ 
    while not  $isAdversarial$  do
         $O, A \leftarrow \emptyset, \emptyset$ 
        for  $k = 1$  to  $K$  do
             $\eta \sim \mathcal{N}(0, 1)^D$ 
             $x_{i,k}^\delta \leftarrow x'_{i-1} + \frac{\delta}{\|\eta\|_2} \cdot \eta$ 
             $x_{i,k}^\perp \leftarrow x + \frac{\|x'_{i-1} - x\|_2}{\|x_{i,k}^\delta - x\|_2} (x_{i,k}^\delta - x)$ 
             $x_{i,k}^\perp \leftarrow \min(\max(x_{i,k}^\perp, 0), 1)$ 
             $x_{i,k}^\epsilon \leftarrow x_{i,k}^\perp - \epsilon(x_{i,k}^\perp - x)$ 
             $x_{i,k}^\epsilon \leftarrow \min(\max(x_{i,k}^\epsilon, 0), 1)$ 
             $O \leftarrow O \cup x_{i,k}^\perp$ 
             $A \leftarrow A \cup x_{i,k}^\epsilon$ 
            if  $f(x_{i,k}^\epsilon) == f(x'_0)$  then
                 $isAdversarial = 1$ 
            end if
        end for
        if  $isAdversarial == 1$  then
             $x'_i \leftarrow \arg \min_{x' \in A, f(x') == f(x'_0)} \|x' - x\|_2$ 
        else
             $x'_i \leftarrow x'_{i-1}$ 
        end if
        adaptively update  $\delta, \epsilon$  using  $O, A$ 
    end while
     $i = i + 1$ 
end while
Return:  $x'_i$ 

```

Each iteration i of the boundary attack process in Algorithm 11 is depicted geometrically in Figure 7. In essence, each iteration samples K perturbed inputs from x'_{i-1} , and is importantly driven by two parameters δ, ϵ . The k -th sample begins by updating x'_{i-1} towards a randomly-sampled direction, and by a distance of δ , to obtain $x_{i,k}^\delta$. Then, $x_{i,k}^\delta$ is projected to be at the same distance of x'_{i-1} away from the source image x , resulting in $x_{i,k}^\perp$. Note that the update from x'_{i-1} to $x_{i,k}^\perp$ points along a direction that is orthogonal to the gap between the current candidate x'_{i-1} and the source image x . Next, the candidate is moved towards x by a relative distance of ϵ , yielding $x_{i,k}^\epsilon$. In practice, both $x_{i,k}^\perp$ and $x_{i,k}^\epsilon$ are capped to be within the range of valid inputs. Finally, the closest $x_{i,k}^\epsilon$ to x that satisfies the adversarial condition is set as the latest candidate adversarial input x'_i ; if none of the samples are adversarial, then this iteration is repeated again with K new samples.

This boundary attack efficiently samples new perturbations based on the current local landscape of decision boundaries. This is achieved by adaptively updating the two parameters δ, ϵ during each attack iteration. In particular, δ controls the spatial range to sample orthogonal perturbations $x_{i,k}^\perp \in O$, i.e., perturbations that are equidistant to x just like x'_{i-1} . Ideally, δ should be sufficiently large so that the adversarial/non-adversarial decision boundary exhibits a locally linear relationship with respect to the sampling spatial range.

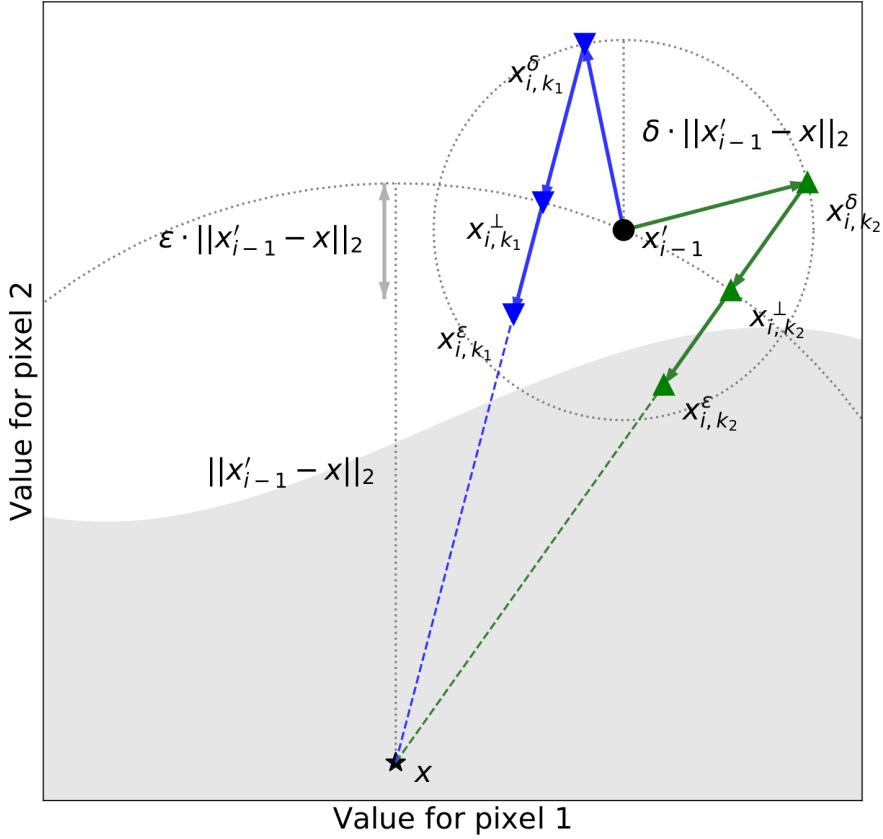


Figure 7: One step of the boundary attack process.

This linear relationship can be verified by checking if roughly 50% of the samples in O are adversarial. If this percentage is much lower than 50%, then δ is decreased by $\delta \leftarrow \delta * \delta_{dec}$; otherwise δ is increased by $\delta \leftarrow \delta * \delta_{inc}$.

Similarly, ϵ controls the relative distance to move the samples $x_{i,k}^\perp$ orthogonally towards x . An efficient ϵ setting should ensure that roughly 50% of the shrunken samples $x_{i,k}^\epsilon \in A$ remain adversarial. If the percentage of adversarial shrunken samples is too small, that means that ϵ took too large of a step, and thus should be decreased by $\epsilon \leftarrow \epsilon * \epsilon_{dec}$. On the other hand, if this percentage is too large, that means that ϵ can be safely increased, i.e., $\epsilon \leftarrow \epsilon * \epsilon_{inc}$. Theoretically, ϵ should converge to 0 when the attack finds a locally optimal adversary.

Due to the brute-force nature of rejection sampling, this adversarial attack may require many iterations (e.g., hundreds of thousands of updates) to find high-quality adversarial examples. Nevertheless, this blackbox method generally applies to a wide range of real world attack situations, as it merely queries the victim model without needing to know its internals. The simplicity of the Boundary Attack raises concerns on the security of existing machine learning models since it shows how attackers do not necessarily need a complicated strategy to find adversarial examples.

Brendel et al. [94] demonstrated how boundary attack is comparable even to whitebox attacks such as FGSM [32] (see Section 4.2), DeepFool [79] (see Section 4.7), and C&W attacks [44] (see Section 4.11). They also showed that boundary attack can be used to circumvent defensive distillation [43] (see Section 6.1.3) and gradient masking defenses since boundary attack does not rely on gradient information.

4.23 Natural Adversarial Attack

In the computer vision domain, an adversarial example is designed to look like a source image when seen by a human. However, in the context of natural language, adversaries must further remain coherent, both in terms of grammar (syntax) and in terms of content (semantics). The need for an adversarial example to be *natural*, i.e., lying within the manifold of natural inputs (be it images, or sentences), is a shortcoming of early adversarial attacks that simply perturb inputs in their raw representation (namely pixel intensities, or characters).

Zhao et al. [60] developed a generalized blackbox technique to generate such *natural* adversarial examples, by searching within a pre-learned latent representation space. This way, any perturbed latent point should be able to project into an input in the raw space that adheres to the complex statistics of natural instances, for instance an image of a natural object or a naturally-occurring scene, or a naturally coherent sentence. We refer to this method as Natural Adversarial Attack (NAA).

Prior to being able to generate adversarial examples, this method first learns a statistic model of natural input instances using the Wasserstein GAN framework [148]. The generator network G in such a formulation maps a latent representation z onto an instance x within the distribution of natural inputs (e.g., images or sentences), i.e., $G : z \mapsto x$. For NAA, one learns an additional inverter network I that maps from x back to z , by optimizing

$$\min_{\gamma} \mathbb{E}_{x \sim p_{real}(x)} \|G(I(x)) - x\| + \lambda \cdot \mathbb{E}_{z \sim p_z(z)} \|I(G(z)) - z\|, \quad (39)$$

where the hyperparameter λ controls the relative weights of two terms, and γ denotes the trainable parameters of the inverter. This loss function is similar to the cycle consistency loss introduced in CycleGAN [149]. Still, NAA differs by first training G (adversarially along with a discriminator network D) until convergence, and then separately optimizing the inverter.

After having trained a G and I on an input dataset, a natural adversarial example $x' = G(z')$ can be generated by searching (through various means discussed below) for a mis-classified latent instance z' :

$$z' = \arg \min_{\tilde{z}} \|\tilde{z} - I(x)\|, \text{ such that } f(G(\tilde{z})) \neq f(x), \quad (40)$$

where f is the victim model.

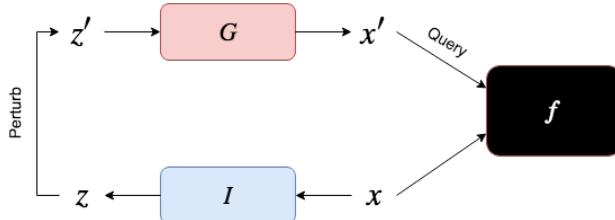


Figure 8: Illustration of NAA (adapted from Zhao et al. [60]).

Two methods were proposed for finding z' : iterative stochastic search and hybrid shrinking search, as shown in Algorithms 12 and 13. The common approach is to perturb the latent representation of the source input $z = I(x)$ by uniformly sampling a vector ϵ_i within a specific range of magnitudes, and testing whether $G(z + \epsilon_i)$ is adversarial. For iterative stochastic search, the range of magnitude is initially small, and iteratively grown if no adversaries are found. More efficiently, hybrid shrinking search first finds an adversarial example within a broad radius around the source input, and then iteratively refines this candidate by searching for smaller-magnitude adversaries. Empirically, the latter approach is shown to be $4\times$ faster than iterative stochastic search, while producing similar adversarial performance.

For a handwritten digit classification task, the authors demonstrated that natural adversarial examples perturbed pixels around relevant image features, instead of injecting arbitrarily-located noise. Furthermore,

Algorithm 12 Iterative Stochastic Search [60]

Input: source input x , victim model f , trained generator G , trained inverter I , search radius increment Δr , number of perturbations per iteration N

Output: adversarial image x'

Initialize: $z = I(x)$, $r = 0$

while no adversarial examples found **do**

- $S \leftarrow \emptyset$
- for** $i = 0$ **to** N **do**
- $\epsilon_i \sim U[(r, r + \Delta r)]$
- $z'_i \leftarrow z + \epsilon_i$
- $x'_i \leftarrow G(z'_i)$
- if** $f(x'_i) \neq f(x)$ **then**
- $S \leftarrow S \cup z'_i$
- end if**
- end for**
- if** $S == \emptyset$ **then**
- $r \leftarrow r + \Delta r$
- else**
- Return:** $\arg \min_{z' \in S} \|z' - z\|$
- end if**
- end while**

NAA successfully generated adversarial texts with minimal grammatical errors on both textual entailment and machine translation tasks where their models were trained on the Stanford Natural Language Inference (SNLI) dataset [150].

4.24 Spatially Transformed Adversarial Attack

Perceptual similarity is an important attribute for adversarial examples in many cases, as ideally they should be indistinguishable from natural images when viewed by humans. However, many adversarial attacks rely on L_2 or L_∞ distances in pixel intensities to quantify perceptual similarity, which may not be an ideal metric [151]. Spatially Transformed Adversarial Attack (stAdv) [95] instead optimizes for *geometrical* similarity between a source and adversarial image pair.

To do this, the authors leverage the representation of a flow field $f(\Delta u, \Delta v) \in \mathbb{R}^{H \times W \times 2}$ to represent a spatially-transformed version of a given image. Each element in the flow field represent a change in horizontal and vertical coordinates away from a designated sampling location, and so the transformed image can be constructed by sampling each pixel at these changed coordinates. Sampling is done using a differentiable implementation of bilinear interpolation [152, 153]; first, let $UV(u, v) \in \mathbb{R}^{H \times W \times 2}$ contain spatial coordinates of each pixel in the input x :

$$UV' = \begin{bmatrix} (u_1 = 1, v_1 = 1) & \dots & (u_1 = 1, v_W = W) \\ \vdots & \ddots & \vdots \\ (u_H = H, v_1 = 1) & \dots & (u_H = H, v_W = W) \end{bmatrix}. \quad (41)$$

Then, by defining $UV' = UV - f$, we can sample the i -th element of the modified image x' around the 4-pixel neighborhood \mathcal{N} of its (real-valued) spatially-transformed coordinate $(u_i, v_i) = (u'_i, v'_i) + (\Delta u_i, \Delta v_i)$:

$$x'_i = \sum_{n \in \mathcal{N}(u, v)} x_n (1 - |u_i - u_n|)(1 - |v_i - v_n|). \quad (42)$$

Algorithm 13 Hybrid Shrinking Search [60]

Input: source input x , victim model f , trained generator G , trained inverter I , maximum search radius r , search radius increment Δr , number of perturbations per iteration for initial search N , number of perturbations for refinement K , shrink factor l

Output: adversarial image x'

Initialize: $z = I(x)$, $l = 0$

while $r - l \geq \Delta r$ **do**

- $S \leftarrow \emptyset$
- for** $i = 0$ **to** N **do**

 - $\epsilon_i \sim U[(l, r)]$
 - $z'_i \leftarrow z + \epsilon_i$
 - $x'_i \leftarrow G(z'_i)$
 - if** $f(x'_i) \neq f(x)$ **then**

 - $S \leftarrow S \cup z'_i$

 - end if**

- end for**
- if** $S == \emptyset$ **then**

 - $l \leftarrow \frac{l+r}{2}$

- else**

 - $z' \leftarrow \arg \min_{z' \in S} \|z' - z\|$
 - $l \leftarrow 0$
 - $r \leftarrow \|z' - z\|$

- end if**

end while

while $k < K$ **and** $r > 0$ **do**

- $S \leftarrow \emptyset$
- $l \leftarrow \max(0, r - \Delta r)$
- for** $i = 0$ **to** N **do**

 - $\epsilon_i \sim U[(l, r)]$
 - $z'_i \leftarrow z + \epsilon_i$
 - $x'_i \leftarrow G(z'_i)$
 - if** $f(x'_i) \neq f(x)$ **then**

 - $S \leftarrow S \cup z'_i$

 - end if**

- end for**
- if** $S == \emptyset$ **then**

 - $k \leftarrow k + 1, r \leftarrow r - \Delta r$

- else**

 - $z' \leftarrow \arg \min_{z' \in S} \|z' - z\|$
 - $k \leftarrow 0$
 - $r \leftarrow \|z' - z\|$

- end if**

end while

Return: z'

Note that all operations in the equations above are differentiable, as well as finding floored/ceiling-ed neighboring coordinates of a given spatially-transformed coordinate. Furthermore, actual pixel values of each neighbor, x_n , can be pre-computed beforehand, which makes this entire process differentiable.

stAdv searches for adversaries using this flow field representation by minimizing:

$$\mathcal{L}_{flow}(f) + \alpha \cdot \mathcal{L}_{adv}(x', t) \quad (43)$$

where α is the weight factor, $\mathcal{L}_{adv}(x', t)$ is the classification loss (e.g., the C&W loss function as in Equation 13 in Section 4.11), and $\mathcal{L}_{flow}(\cdot)$ is a Total Variation loss [154] that encourages small and smooth perturbations. In their experiments, the authors used L-BFGS [100] as the optimizer.

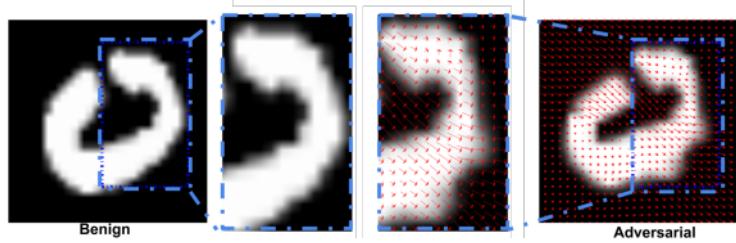


Figure 9: Illustration of spatially transformed adversarial example that is misclassified as the digit “2” where the red arrows show how the pixels are moved from benign to adversarial image (taken from Xiao et al. [95]).

Adversarial examples generated by stAdv were shown to be perceptually indistinguishable from the original example by a human, following the procedure in [146, 147]. The authors also evaluated stAdv against a variety of methods that rely upon L_p norm as the similarity metric, such as FGSM [32] and C&W [44], evaluating against defenses including adversarial training [32] (see Section 6.1.1), ensemble adversarial training [47] (see Section 6.1.6), and PGD adversarial training [145] (see Section 6.1.5). In this experiment, stAdv was found to be more effective than L_p norm attacks by a large margin. Nevertheless, since the authors only considered baseline adversaries generated using FGSM, it remains to be seen if stAdv can produce stronger adversaries than other attacks such as C&W. Still, we conclude that the use of different perceptual metric may produce different types of adversaries, which can be used to attack defenses that are designed to be robust against L_p adversaries.

4.25 Expectation Over Transformation

Early adversarial examples typically have lessened adversarial effects when the source input is transformed, e.g., when a source image is rotated or translated. In order to create adversaries that are robust to such transformations, Athalye et al. [96] proposed a method called the Expectation Over Transformation (EOT). Such a robustness attribute is especially important for physical-realizable adversarial examples, e.g., images that are printed or displayed in the real-world and imaged under from different view angles (see Section 5 for more details).

EOT is a meta-optimization process that can be coupled with various optimization-based attacks. The key addition is to pre-process each input instance x by one or more parameterized transforms $t(x)$, and to optimize the expectation of the objective function over the probability distributions T of the transformation parameters:

$$\arg \min_{x'} \mathbb{E}_{t \sim T} \left[\mathcal{L}_{adv}(t(x')) + \mathcal{L}_{perc}(x, x') \right], \quad (44)$$

where \mathcal{L}_{adv} represents an adversarial loss (e.g., to minimize the distance between model predictions and adversarial labels, or to maximize the model’s training error), and \mathcal{L}_{perc} entails a perceptual similarity loss (comparing either the raw source versus perturbed inputs, or their transformed representations). In the reported experiments, perceptual similarity was measured as Euclidean distance in the CIE Lab space, which is designed to correspond more closely to human perceptual distance compared to RGB (while still remaining differentiable) [155].

The authors demonstrated robust adversarial misclassification of generated 2D examples under transformations in the form of $t(x) = Ax + b$ such as rescaling, rotation, and additive Gaussian noise. They also realized robust physical adversaries using 3D printing, and by optimizing the surface texture of a 3D object under pose-based translations. Beyond this initial work, EOT opened up a new research direction towards adversarial examples that are physically realizable. Subsequent work from Brown et al. [66] used EOT to generate printable adversarial patch [66] (see Section 5.5). EOT has also been extended to generate adversarial examples that fool Faster R-CNN [15] by performing EOT over region proposals [156].

4.26 Backward Pass Differentiable Approximation

Some defense strategies to adversarial attacks rely on mechanisms that obfuscate a model’s gradients, for instance by using non-differentiable pre-processing functions or non-differentiable network layers. Backward Pass Differentiable Approximation (BPDA) [55] is a technique for modifying an adversarial attack to bypass such defenses, by exploiting a differentiable approximation for the defended model to obtain meaningful adversarial gradient estimates.

A simplistic special case of BPDA applies ideas from the straight-through estimator [157]: assume that an adversarial defense pre-processes each input x using a non-differentiable transformation $g(x)$, and that $g(x) \approx x$ within some local neighborhood (e.g., $g(\cdot)$ is a smoothing function). Then, during the adversarial attack, one can simply approximate its gradient by the identity function. Examples of defense methods that can be circumvented by this technique include bit-depth reduction, JPEG compression, total variance minimization, and quilting-based defense [54] (see Section 6.1.9).

More generally, BPDA works by finding a differentiable approximation for a non-differentiable pre-processing transformation $g(\cdot)$ or a non-differentiable network layer, possibly via an engineered guess. As long as the two functions are similar, adversarial perturbations can still be found by using inexact derivatives from the approximated form during back-propagation, albeit likely needing more attack iterations. Still, the authors noted that forward inference should still use the original non-differentiable transformation $g(\cdot)$ to obtain true loss values, otherwise the attack may become significantly less effective.

As a concrete example, the authors considered the defense method of thermometer encoding [48] (see Section 6.1.10), which obfuscates input gradients by discretizing interval-bounded input values $x_{i,j,c} \in [0, 1]$ (such as pixel intensities) via thermometer encoding:

$$\tau(x_{i,j,c})_k = \begin{cases} 1 & \text{if } x_{i,j,c} \geq \frac{k}{l}, \\ 0 & \text{otherwise} \end{cases}, \quad (45)$$

where $k \in \{1, \dots, l\}$ is the index of the binarized, and l denotes the discretization level (e.g., if $l = 10$, then $\tau(0.66) = '1111110000'$, indexed increasingly from left to right). This encoding function can be approximated as:

$$\hat{\tau}(x_{i,j,c})_k = \min(\max(x_{i,j,c} - \frac{k}{l}, 0), 1), \quad (46)$$

since $\tau(x_{i,j,c})_k = \text{ceil}(\hat{\tau}(x_{i,j,c})_k)$. By using $\hat{\tau}$ during back-propagation, Athalye et al. [55] successfully applied an optimization-based adversarial attack to confuse a thermometer-encoded network.

4.27 Simultaneous Perturbation Stochastic Approximation Attack

Simultaneous Perturbation Stochastic Approximation (SPSA) [158] is an alternative numerical gradient estimator that is more efficient than the Finite Difference (FD) method. Given a function $f(x)$ where $x \in \mathbb{R}^D$, recall that FD estimates the gradient using 2D elementary-vector queries:

$$\left(\frac{\partial f}{\partial x} \right)_i \approx \left(\frac{f(x + \Delta e_i) - f(x - \Delta e_i)}{2\Delta} \right)_i, \quad (47)$$

where the elementary vector $e_i = [0, \dots, 1, \dots, 0]$ only has a non-zero element at the i -th index, and Δ is a small constant (e.g., $\Delta = 10^{-9}$). In contrast, SPSA estimates the gradient using 2 queries to $f(\cdot)$, regardless of D , by simultaneously perturbing all dimensions using a vector $v \sim \{-1, 1\}^D$ sampled from the Rademacher distribution (i.e., whose elements are either +1 or -1):

$$\frac{\partial f}{\partial x} \approx \frac{f(x + \Delta v) - f(x - \Delta v)}{2\Delta} \cdot v. \quad (48)$$

Uesato et al. [97] showed that SPSA can equally be used in a blackbox attack, similar to how the Zeroth-Order Optimization Attack (ZOO-Adam) [89] (see Section 4.17) uses FD to numerically estimate gradients of a victim model. As seen in Algorithm 14, the SPSA Attack makes N numerical estimates of the gradient of an adversarial loss function \mathcal{L} with respect to the input x . It then perturbs the input along the negative averaged gradient direction, and projects the updated input onto the epsilon-ball $N_\epsilon(x_0)$ around the source input x_0 to enforce perceptual similarity. In their experiments, the authors initialized x_0 similar to the strategy used in R+FGSM [47] (see Section 4.5), by sampling random perturbed input within $[x_0 - \epsilon, x_0 + \epsilon]$, to help avoid gradient masking defenses.

Algorithm 14 SPSA [97]

```

Input: input  $x \in \mathbb{R}^D$ , perturbation size  $\Delta$ , step size  $\alpha$ , gradient estimate batch size  $N$ , number of iterations  $I$ 
Initialize:  $x'_0 \leftarrow x$ 
for  $i = 0$  to  $I - 1$  do
    for  $n = 1$  to  $N$  do
         $v_n \sim \{-1, 1\}^D$ 
         $g_n \leftarrow \frac{\mathcal{L}(x'_i + \Delta v_n) - \mathcal{L}(x'_i - \Delta v_n)}{2\Delta} \cdot v_n$ 
    end for
     $x_{i+1} \leftarrow x'_i - \frac{\alpha}{N} \sum_{n=1}^N g_n$ 
     $x'_{i+1} \leftarrow \arg \min_{x \in N_\epsilon(x_0)} \|x_{i+1} - x\|$ 
    end for
Return:  $x_I$ 

```

SPSA was shown to be effective against PixelDefend [53] (see Section 6.1.11), HGD [159] (see Section 6.1.14), and Random Resizing and Padding (RRP) [51] (see Section 6.1.7). The authors also found SPSA to be stronger than ZOO, where ZOO was implemented without the feature reduction and importance sampling methods.

4.28 Decoupled Direction and Norm Attack

Constrained optimization-based attacks such as L-BFGS [31] (see Section 4.1) and C&W [44] (see Section 4.11) often optimize for both the misclassification and perceptual similarity conditions at the same time, possibly using expensive line search to balance between these two objectives. In contrast, Rony et al. [98] proposed the Decoupled Direction and Norm (DDN) attack method, which decouples the perturbation norm penalty and the direction which causes misclassification.

As seen in Algorithm 15, each attack iteration begins by making an update onto a cumulative perturbation vector δ_{i+1} , by descending by α following the gradient of a misclassification-based loss function \mathcal{L} . However, to obtain the next perturbed input x'_{i+1} , only the direction of δ_{i+1} is used, while the magnitude of the perturbation is set to an independent variable ϵ_i . Then, depending on whether x'_{i+1} is adversarial, the adaptive norm ϵ_i is either increased or decreased accordingly. After I total iterations, the adversarial example that is most perceptually similar to the source input is returned.

The authors showed that DDN converged faster (e.g., can be as fast as 100 iterations) and produced adversarial examples with higher perceptual similarity compared to the C&W [44] L_2 attack (see Section 4.11) when tested on MNIST, CIFAR-10, and ImageNet datasets. Additionally, DDN was shown to be able to

Algorithm 15 DDN [98]

Input: input x , victim model f , true label y , target label t (set t to y for non-targeted attack), perturbation size α , adaptive norm factor $\gamma \in [0, 1]$, number of iterations I

Initialize: $x'_0 \leftarrow x$, $\epsilon_0 \leftarrow (1 + \gamma)$, $\delta_0 \leftarrow 0$, $X' \leftarrow \emptyset$

```

if  $t == y$  then
     $\sigma \leftarrow +1$ 
else
     $\sigma \leftarrow -1$ 
end if
for  $i = 0$  to  $I - 1$  do
     $g \leftarrow \nabla_{x'_i} \mathcal{L}(x'_i, t)$ 
     $g \leftarrow \alpha \frac{g}{\|g\|_2}$ 
     $\delta_{i+1} \leftarrow \delta_i + \sigma g$ 
     $x'_{i+1} \leftarrow x + \epsilon_i \frac{\delta_{i+1}}{\|\delta_{i+1}\|_2}$ 
     $x'_{i+1} \leftarrow \min(\max(x'_{i+1}, 0), 1)$ 
    if  $f(x'_{i+1})$  is adversarial then
         $X' \leftarrow X' \cup x'_{i+1}$ 
         $\epsilon_{i+1} \leftarrow (1 - \gamma)\epsilon_i$ 
    else
         $\epsilon_{i+1} \leftarrow (1 + \gamma)\epsilon_i$ 
    end if
end for
Return:  $\arg \min_{x' \in X'} \|x - x'\|_2$ 

```

converge as fast as DeepFool [79] (see Section 4.7), while producing higher attack success rates and lower perturbation norms. In the Adversarial Vision Challenge at the 32nd Neural Information Processing Systems (NeurIPS’18), DDN was ranked first in the non-targeted attack category, and ranked third in targeted attack category.

Furthermore, the authors showed that when DDN was used to perform adversarial training [32] (see Section 6.1.1), the resulting model robustness surpassed PGD adversarial training [145] (see Section 6.1.5) for all ϵ values when evaluated on MNIST and CIFAR10 datasets. Adversarial training with DDN was ranked third in the NeurIPS 2018 Adversarial Vision Challenge when defending against the blackbox attack scenario.

4.29 CAMOU

Zhang et al. [99] proposed a method called CAMOU which involves the use of photo-realistic simulation tool (i.e., Unreal engine) to generate 3D adversarial examples in the simulation. CAMOU is a method to generate adversarial textures which when applied to an object, causes detection models like the Mask R-CNN [9] and YOLOv3 [160] to misdetect the object. In other words, the adversarial texture may act like a *camouflage*, making the object invisible to a detector.

In this work, Zhang et al. [99] apply the texture on a 3D vehicle model. Given information of the 3D vehicle model and background scene, CAMOU aims to find a camouflage texture c that fools a detector model. Zhang et al. [99] performed their attack in the blackbox scenario where they were constrained from calculating the gradients directly from the target detector model. Concretely, they use a substitute network [41] (see Section 4.9) to approximate the output of the target detector, which also helps in bypassing the complex rendering process. EOT [96] (see Section 4.25) is also used to ensure that the adversarial examples are robust to various transformations.

CAMOU works as follows. First, a substitute network f' is created to approximate the detection score of the original model f . The substitute network takes the camouflage texture c , background scene b , and

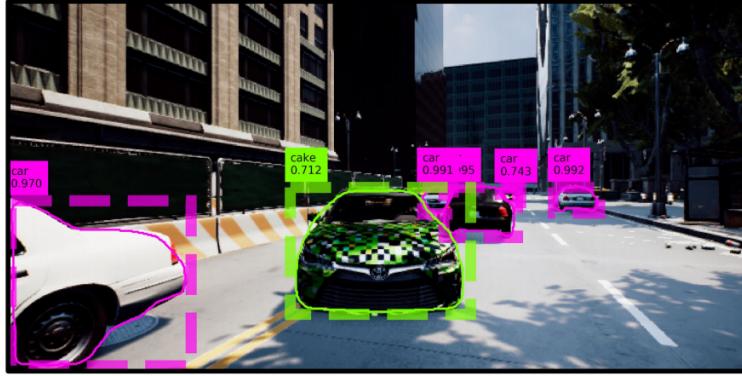


Figure 10: The car with camouflage pattern is misdetected as a cake (taken from Zhang et al. [99]).

foreground (i.e., the vehicle model) v as inputs, and outputs a scalar value that represents the detection score. Note that the ground truth for the detection score can be obtained by querying the target detection model. Once f' is trained, the adversarial camouflage texture c' can be found using EOT by differentiating through f' . Here, the transformations are done by moving the camera to new locations in the simulator, which can simulate various complex 3D transformations. In their implementation, Zhang et al. [99] alternatively trained f' and solved for c' . In every iteration, the adversarial camouflage texture c' is added to a set of camouflage pattern used to train the substitute network. The camouflage is also evaluated over various transformations on the target detection model in order to get the best adversarial camouflage texture. These processes are then repeated for specified number of iterations. This method is presented in Algorithm 16.

Algorithm 16 CAMOU [99]

Input: background scene b , foreground/vehicle model v , target detection model f , substitute detection model f' parameterized by θ , a set of transformation T , a set of camouflage texture C , number of iteration I
Output: adversarial camouflage texture c'
Initialize: lowest score achieved by adversary $s^* \leftarrow \infty$
for $i = 0$ **to** I **do**

$$\theta \leftarrow \arg \min_{\theta} \frac{1}{|C||T|} \sum_{c \in C} \sum_{t \in T} [\mathcal{L}(f(c, t(b), t(v)), f'(c, t(b), t(v))) + \alpha \|\theta\|_2]$$

$$c' \leftarrow \arg \min_c \frac{1}{|T|} \sum_{t \in T} \mathcal{L}(0, f'(c, t(b), t(v)))$$

$$C \leftarrow C \cup c'$$

$$s' \leftarrow \frac{1}{|T|} \sum_{t \in T} f(c', t(b), t(v))$$
if $s' < s^*$ **then**

$$s^* \leftarrow s'$$

$$c^* \leftarrow c'$$
end if
end for
Return: c^*

CAMOU successfully fooled Mask R-CNN [9] and YOLOv3 [160] trained on COCO [161] dataset in the simulation. Zhang et al. [99] also showed how the adversarial texture can be transferred to fool different detection models to a certain extent. Although Zhang et al. [99] did not print the texture and apply it to a vehicle in the real world, the method offers an important direction to generate adversarial examples in the simulation. In the future, the adversarial examples will be easier to fabricate in the real world as the quality of images produced by the simulation software increases, and as our knowledge on domain adaptation increases.

5 Towards Real World Adversarial Attacks

This section discusses the danger of adversarial examples in real world scenarios. Most work on adversarial attacks only test adversarial examples in the virtual domain, raising the question of whether or not these adversarial examples are still effective in the 3D real world environment. Some works presented in this section focus on physically realizable adversarial examples, and others show that adversarial examples need not be physically realizable to be dangerous in real world. We refer physically realizable adversaries as adversarial examples that are still adversarial when viewed in the 3D world from various viewpoints.

5.1 Printed Adversarial Examples

Kurakin et al. [77] studied whether adversarial examples generated using FGSM [32] (see Section 4.2), BIM [45, 77] (see Section 4.3), and ILLCM [45, 77] (see Section 4.4) can be printed and remain adversarial in the physical world. This was evaluated by capturing pictures of printed adversarial examples using a cellphone camera, and classified these images with Inception-v3 [111] model.

In their experiments, they found adversaries generated by FGSM to be the most robust in the physical world, while ILLCM is the least robust. They hypothesized that this is due to the fact that BIM and ILLCM attempt to find more subtle perturbations, which are easier to be destroyed in the real world environment. Further, Kurakin et al. [77] demonstrated the transferability of the printed adversarial examples by fooling an open source mobile application that performs image classification. Note that the adversarial examples were generated to fool Inception-v3 model, and not the model deployed by the mobile application.

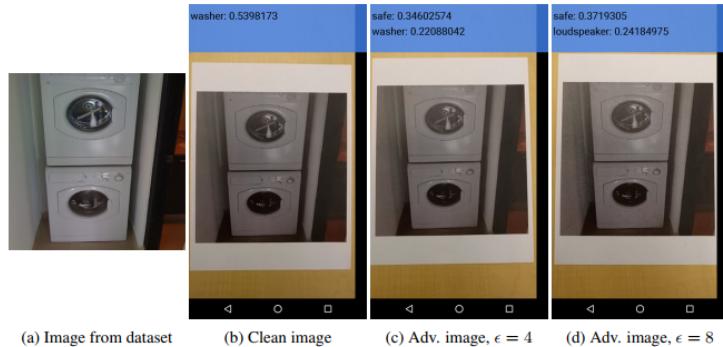


Figure 11: Printed adversarial example still fools an image classifier (taken from Kurakin et al. [77]).

The printed adversarial examples generated by this method seem to only work in some limited settings such as when the printed image is located right in front of the camera with small variations in lighting, distance, and camera angle, but they have not been evaluated on more diverse and extreme sets of 2D and 3D transformations. Still, both this work and the adversarial eyeglasses [64] (see Section 5.2) ignited the discussion of adversarial examples in the physical world.

5.2 Adversarial Eyeglasses

Sharif et al. [64] demonstrated how a printable adversarial eyeglass can fool face recognition systems. As in the L-BFGS attack [31] (see Section 4.1), Sharif et al. [64] model this problem as an optimization problem that can be solved using gradient descent. In order to generate an adversary that looks like an eyeglass, a masking matrix M_x is used so that only pixels inside the mask are allowed to change during the optimization process. Sharif et al. [64] noticed the challenges in fabricating the eyeglass as a printer may produce slightly different color when printing. An additional loss term called the Non Printability Score (NPS) was then introduced as part of the optimization process to ensure that the generated adversary is made of colors that are printable by a particular printer. NPS is defined as

$$NPS(\hat{p}) = \prod_{p \in P} |\hat{p} - p|, \quad (49)$$

where $P \subset [0, 1]^3$ represents the set of printable RGB triplets, and \hat{p} represents a pixel in the adversarial image. In other words, NPS goes to 0 if \hat{p} is in P . In order to get P , Sharif et al. [64] took a picture of a printed color palette that contains one fifth of the RGB color space, and assumed the RGB triplets received from the camera to be printable by that particular printer. The optimization objective then becomes to find perturbation r that optimizes

$$\arg \min_r \left(\left(\sum_{x \in X} \mathcal{L}(f(x + M_x \cdot r), t) \right) + \lambda_1 \cdot TV(M_x \cdot r) + \lambda_2 \cdot NPS(M_x \cdot r) \right), \quad (50)$$

where t denotes the target misclassification class, and λ_1 and λ_2 are the weighting factors for the objectives.



Figure 12: Example of the printed adversarial eyeglass (taken from Sharif et al. [64]). The top row shows images of persons that are misclassified as the persons shown in the bottom row. For example, the person in the top row of second column is misclassified as Milla Jovovich.

Sharif et al. [64] showed this method can generate adversarial eyeglasses when tested on various face recognition models, including the model proposed by [162] which was the state of the art face recognition model on the Labeled Faces in the Wild dataset (LFW) [163, 164]. They further showed that the eyeglasses could be printed, fooling various models based on the architecture of [162] trained on a dataset which contains pictures of 5 persons from the authors' lab, as well as 5 celebrities from the PubFig dataset [165] (see Fig. 12).

Sharif et al. [166] extended this work to create adversarial eyeglasses independent of the attacker's face. In order to do this, Sharif et al. [166] leverage the GAN [63] framework to train a generator network that generates adversarial eyeglass, where the job of the discriminator is to discriminate between fake and real eyeglasses. The objective of the generator is to minimize a similar loss function in Equation 50). We refer readers to the paper for implementation details.

5.3 Adversarial Stop Signs

Evtimov et al. [65] proposed an attack called the Robust Physical Perturbation (RP_2), showing that adversaries can be crafted to be robust to change in angle, distance, and lighting. RP_2 was specifically tested on various road signs. Similar to the strategy used to generate adversarial eyeglasses [64] (see Section 5.2), a masking matrix M_x is used to constrain the area of perturbations. In order to ensure that the adversarial examples generated are robust to change in various conditions and transformations, Evtimov et al. [65] collected pictures of the same road signs images taken under various conditions, and used them as part of adversarial examples generation process. Formally, the RP_2 objective is defined by

$$\arg \min_r \left(\left(\sum_{x \in X} \mathcal{L}(f(x + M_x \cdot r), t) \right) + \lambda_1 \cdot \|M_x \cdot r\|_p + \lambda_2 \cdot NPS(M_x \cdot r) \right), \quad (51)$$

where X is the set of stop sign images taken in various conditions.

RP_2 was used to generate two different types of attacks: poster-printing and sticker attacks. Poster-printing attack is a scenario where an attacker prints a road sign of an actual size on paper which is overlaid on top of a real road sign. Sticker attack is a scenario where an attacker prints some stickers containing the adversarial perturbations and stick them on top of a real road sign. While the masking matrix used in the poster-printing attack allows perturbations to be generated anywhere on the road sign, the mask used in the sticker attack only allows the perturbations to be generated on certain parts of the road sign.



Figure 13: An example of sticker attack where it was misclassified as “Speed Limit 45” sign when viewed from different viewpoints (taken from Evtimov et al. [65]).

Evtimov et al. [65] successfully showed how the generated road signs can be physically realizable and fooled the victim model in a controlled environment. For example, Evtimov et al. [65] demonstrated a sticker attack on a real stop sign that was misclassified as a “Speed Limit 45” sign in a stationary lab setting (see Fig. 13). They also conducted drive-by tests where a camera was placed on top of a moving vehicle to confirm that these examples are adversarial even when viewed from different viewpoints. However, one major limitation of RP_2 remains: collecting real pictures of an object in the real world under various conditions can be expensive to perform and may not be scalable.

Several works have shown that these adversarial road signs are currently not dangerous to object detection models [167, 168] which are more commonly deployed in autonomous vehicles than classification models. However, this does not warrant complacency. Object detection models are also vulnerable to attack: see the sections on DAG [88] (Section 4.16) and attacks on Faster R-CNN [15] using EOT [96] (see Section 4.25) over region proposals [156].

5.4 Adversarial 3D Printed Turtle

Athalye et al. [96] demonstrated the effectiveness of EOT (see Section 4.25) in generating adversarial examples not only in the virtual image domain, but also in generating 3D adversarial objects that remain adversarial in the physical world, where the 3D adversarial object is robust to rotation, translation, lighting change, and viewpoint change to reasonable extent. In practice, Athalye et al. [96] modeled the problem using a texture that can be mapped to a 3D shape, and by considering the 3D rendering process as the transformation function. The texture is then updated through an optimization process in order to find an adversarial texture. They showed how they were able to 3D print an adversarial turtle that is misclassified as a rifle, as shown in Fig. 14.

To generate more robust adversaries, instead of only considering similar transformations used in the 2D case (e.g., translation, rotation, Gaussian noise, etc.), Athalye et al. [96] consider more transformations that better reflect the physical world. These include additive/multiplicative lighting and additive/multiplicative per-channel color inaccuracies. They pointed out that modelling color inaccuracies is necessary to account for printing errors.

This perhaps was the first work that showed how adversarial textures can be projected onto some complex 3D shapes, such as the 3D printed turtle, and remain adversarial when viewed from different angles in the real world. We believe this form of attack as one of the most realistic possible attack scenarios in the real world that can dangerously fool intelligent embodied agents such as autonomous cars or mobile robots. Thus,

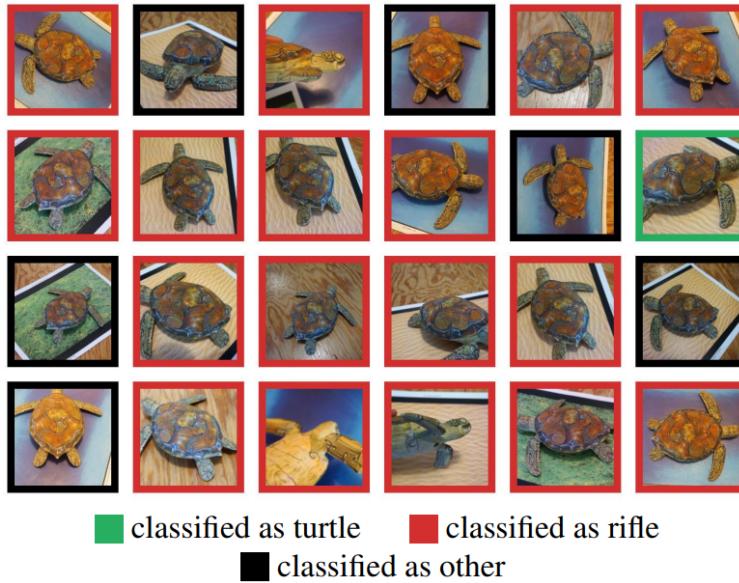


Figure 14: The 3D printed adversarial turtle is misclassified as a rifle in most of the cases even when viewed from different angles (taken from Athalye et al. [96]).

further development of both attack methods that can generate 3D adversarial examples of any shapes in the real world, as well as defense methods that can defend against these adversaries are important research directions.

5.5 Adversarial Patch

While many attacks on image classifier focus on modifying an image such that the adversarial image look similar to its original instance, Brown et al. [66] demonstrated that they were able to generate an adversarial patch that is input-agnostic (i.e., universal, just like UAP [83] (see Section 4.12)), visually visible, but arguably inconspicuous. The adversarial patch does not look like a real object, but will cause a classifier to misclassify an input whenever the patch is present in the image.

Brown et al. [66] generated the adversarial patch using a variant of EOT [96] (see Section 4.25), where the objective is to find the patch p :

$$\arg \max_p \mathbb{E}_{x \sim X, t \sim T, l \sim L} [\mathcal{L}(A(p, x, t, l), y)]. \quad (52)$$

Here, $A(p, x, t, l)$ denotes a patch application operator that transforms patch p at location l on image x with transformation t . In other words, one may see the attack process as the combination of EOT with the method used to generate adversarial eyeglass Sharif et al. [64]. Concretely, the patch application operator can be defined as:

$$A(p, x, t, l) = t(m(l) \cdot p) + [t(1 - m(l)) \cdot x], \quad (53)$$

where $m(l)$ is a binary mask centered at location l .

The adversarial patch was shown to be robust in fooling various ImageNet classifiers in whitebox and blackbox settings. Furthermore, Brown et al. [66] demonstrated that the adversarial patch can be printed and still fool the classifier in the real world. Figure 15 illustrates how the adversarial patch fools the target model into thinking that the image contains a toaster as opposed to a banana.

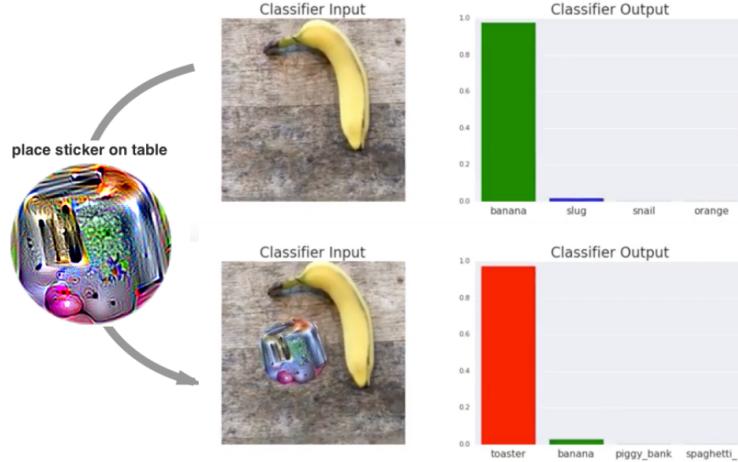


Figure 15: The image of a banana is misclassified as a toaster when the adversarial patch is present (taken from Brown et al. [66]).

5.6 ShapeShifter

Chen et al. [156] extended EOT [96] (see Section 4.25) and C&W attacks [44] (see Section 4.11) to propose ShapeShifter: a method to create physical adversarial objects that fool Faster R-CNN [15]. For example, the perturbed stop sign shown in Fig. 16 is able to fool a Faster R-CNN model that was trained on the MS-COCO dataset [161] to mistakenly detect it as a person with high confidence.



Figure 16: An example of a stop sign misdetected as a person with high confidence (taken from Chen et al. [156]).

Before discussing how the attack works, it is important to realize that Faster R-CNN is made of several main components: (1) region proposal network (RPN) [156] to produce numerous hypotheses where the objects might be, (2) a classification head to classify the region proposals, and (3) a regression head to refine the bounding box coordinates that represent where the objects are in the image. Since object detection models usually remove some of the region proposals using non-maximum suppression which is a non-differentiable operation, Chen et al. [156] only consider the region proposals that survive the pruning after running a single forward pass through the RPN. To further simplify the problem, they also only considered the top- N detected objects based on the level of model’s confidence.

ShapeShifter aims to attack the classification head for each of the region proposals. Given a classifier f , an input image x , a set of transformations T , and a target class y' , the optimization objective is

$$\arg \min_{x'} \mathbb{E}_{t \sim T} \left[\frac{1}{N} \sum_{i=1}^N \mathcal{L}(f(r_i), y') \right] + c \cdot \|\tanh(x') - x\|_2^2, \quad (54)$$

where r_i is the i -th masked region proposal. Since Chen et al. [156] wanted to constraint the location of the perturbations, a masking operator was used. It is not clear how the masking operator was implemented, but it may be similar to the masking operator used to generate adversarial eyeglass [64] (see Section 5.2), except that it has to account for all the region proposals.

Chen et al. [156] showed that the generated adversaries can reasonably fool the Faster R-CNN model in the real world when viewed from different distances and view angles. The adversaries were tested both in a controlled indoor environment and by conducting drive-by tests. They also identified some limitations such as the weakness of the perturbations when viewed from a high viewing angle and lack of transferability to other detection models. However, this work emphasizes once again how adversarial examples can be physically realizable to fool object detection models that are more complex than classification models.

5.7 Non-physical Adversaries in the Real World

In some cases, adversarial attacks do not need to be physically realizable to be dangerous. For example, camera model identification is the task of identifying the specific camera that was used to take an image of interest, which can be used to detect copyright infringement and image falsification. Several works have considered deep learning as a means to perform camera model identification [169, 170, 171]. Güera et al. [172] showed that adversarial attack techniques such as the FGSM [32] (see Section 4.2) and JSMA [80] (see Section 4.8) are sufficient to fool the models that were trained to perform camera model identification. This type of attack does not only exist in the vision domain, but also in the digital audio domain [173], where the attack successfully fooled real world music copyright detectors.

Another area where adversarial examples do not have to be physically realizable is in the field of medical imaging. Deep learning systems have shown promising performance when it comes to medical image analysis [174]. Deep learning has been used for diagnosis of breast cancer [175], pneumonia [176], skin cancer [177, 178], and has demonstrated super-human performance in some of the cases. Finlayson et al. [179] showed that existing adversarial attack methods can be applied on medical images, and discussed various real world scenarios where adversarial examples might negatively impact the healthcare economy when machine learning based systems are used. A bad dermatologist could commit fraud by inserting adversarial perturbations on dermoscopy images in order to create more profit by suggesting to perform unnecessary procedures on patients, which will negatively affect both the patients and insurance companies. A bad pharmaceutical company can apply adversarial perturbations to alter the images used for new drug trials in order to get positive results. A bad insurer can use adversarial examples to alter the healthcare policy by manipulating the rate of surgeries required, which may be based on recommendations from machine learning based systems. All of these are possible scenarios on how adversarial examples can negatively impact the healthcare industry that are important to be addressed.

6 Defenses against Adversarial Attacks

This section covers various defense strategies against adversarial attacks. Figure 17 and Table 5 illustrates the ontology and taxonomy of adversarial defense techniques discussed in this paper, respectively.

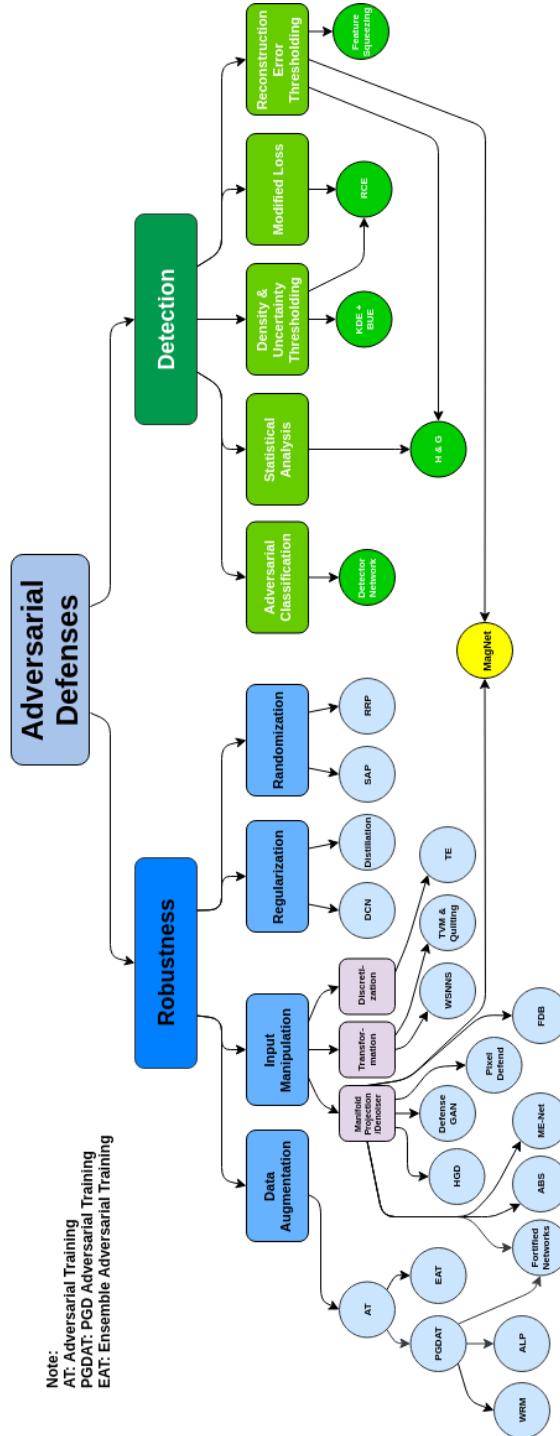


Figure 17: Ontology of adversarial defenses covered in this paper.

Table 5: Taxonomy of adversarial defenses covered in this paper.

Adversarial Defense(s)	Goal	Remarks
Adversarial Training [32]	R	Training on adversarial examples
Ensemble Adversarial Training [47]	R	More robust to blackbox attacks compared to standard adversarial training
DCN [180]	R	Early defense against adversarial attacks with gradient regularization
Defensive Distillation [43]	R	Circumventable by C&W [44], SBA [41], and variant of JSMA [181]
MagNet [81]	R, D	Combination of R & D, circumventable by C&W [44] and SBA [41]
Random Resizing & Padding [51]	R	Circumventable by EOT variant (Expectation Over Randomness) [55]
SAP [50]	R	Circumventable by EOT variant (Expectation Over Randomness) [55]
TVM & Quilting [54]	R	Circumventable by combination of BPDA [55] and EOT [96]
TE [48]	R	Circumventable by BPDA [55]
PixelDefend [53]	R, D	Circumventable by BPDA [55] and SPSA [97]
Defense-GAN [52]	R	Circumventable by BPDA [55]
PGD Adversarial Training [45]	R	Training only on PGD adversaries
WRM [182]	R	Adversarial training with robustness certificate
HGD [159]	R	Circumventable by SPSA [97]
ALP [183]	R	Circumventable by PGD [145] with many iterations [184]
FN [185]	R	Denoising on hidden representations using autoencoders
FDB [186]	R	Denoising on hidden representations using differentiable denoising operation
ABS [187]	R	Model distribution of the inputs for each class using VAE [86]
WSNNs [188]	R	Replace input with its nearest neighbor from a large database of images
ME-Net [189]	R	Defense using matrix estimation algorithms
H&G's Methods [190, 191]	D	Defense using modified C&W [44]
Detector Networks [192, 193, 194, 195]	D	Circumventable by modified C&W [44] and SBA [41]
KDE & BUE [196]	D	Circumventable by modified C&W [44]
Feature Squeezing [197]	D	Detection by comparing the predictions between preprocessed and original inputs
RCE [198]	D	Defense using reverse crossentropy loss

R: Robustness
D: Detection

6.1 Increasing Robustness of Machine Learning Models

A number of approaches have been proposed which seek to make models more robust to adversarial attacks. These techniques do not rely upon the detection of adversarial examples (see Section 6.2), instead formulating models which perform equally well with adversarial and normal inputs. At their heart, many of these methods seek to make models less sensitive to irrelevant variation in the input, effectively regularizing models to reduce the attack surface and limit responsiveness to off-manifold perturbations. However, a recurring theme in this section is that many approaches that were thought to be robust have subsequently been shown to rely upon *gradient masking*, and thus to be vulnerable to the suite of attacks which bypass this form of defense. We will highlight where defenses should be re-evaluated in light of attack methods that are specifically designed to circumvent gradient masking, such as BPDA [55] (see Section 4.26) and SPSA [97] (see Section 4.27).

6.1.1 Adversarial Training

Adversarial training [32] is a defense method in which a model is retrained by injecting adversarial examples into training set at every training iteration. In practice, one can generate adversarial examples using a method of choice such as the FGSM [32] (see Section 4.2) or BIM [45, 77] (see Section 4.3). Formally, the new training objective becomes

$$\alpha\mathcal{L}(x, y) + (1 - \alpha)\mathcal{L}(x', y), \quad (55)$$

where $\mathcal{L}(x, y)$ denotes the classification loss function (e.g., cross-entropy), and x' denotes the adversarial counterpart of clean example x . Here, α is a constant that controls the weighting of the loss terms between normal and adversarial inputs where α is usually set to be 0.5. In this paper, we refer to adversarial training based on the type of adversarial examples the defended model is trained on. For example, if the defended model is trained on FGSM adversaries, we refer this as FGSM adversarial training, or in short, FGSM-AT.

Although adversarial training is relatively simple to implement and performs fairly well, adversarially trained models may still be vulnerable to other types of adversarial examples the model was not trained on. For example, adversarial training on adversarial examples generated using single-step gradient-based attacks (e.g., FGSM) shows robustness against the same type of attacks even when evaluated in large scale [45], but training against single-step methods produces models that are less robust against iterative gradient-based attacks (e.g., BIM).

Furthermore, adversarial training on single-step adversaries can suffer from *label leakage* [45]. Kurakin et al. [45] observed that models trained on adversarial examples generated by a specific single step attack method have higher accuracy on adversarial examples generated by the same method compared to clean examples. This suggests that the adversaries generated by single step methods are too simple and can be easily overfitted by the model. This problem perhaps reflects the limited options for generating adversarial examples at the time of publication. Future research might consider adversarial training on various types of adversaries rather than exclusively on those generated by single-step methods. Furthermore, it would be useful to evaluate robustness against attack techniques that were not used during the training process, assessing the generalization of the defense afforded by this method. Along those lines, it might also be useful to treat the problem as a meta-learning task: given a set of attacks, learn parameters that facilitate swift training of defense to new attacks with as few examples as possible.

Tramèr et al. [47] found that the robustness provided by adversarial training on single-step adversaries was mainly caused by gradient masking (see Section 4.5). As a result, the model can be circumvented by other types of attacks like the R+FGSM [47] (see Section 4.5) or the SBA [41] (see Section 4.9). One proposed solution is to include examples that have been generated to fool *other* models. This is further discussed in Section 6.1.6. An alternative approach is to train on adversarial examples generated by the Projected Gradient Descent (PGD) method [145] (see Section 6.1.5).

6.1.2 Deep Contractive Network

Gu and Rigazio [180] proposed a defense for deep neural networks using a regularization term that is adopted

from the Contractive Autoencoders [199] called the contractive penalty, hence the name Deep Contractive Network (DCN). The contractive penalty encourages the model to be invariant to small changes in directions which are irrelevant in the input space. Given N datapoints, DCN with H number of layers is trained to minimize

$$\sum_{i=1}^N \left(\mathcal{L}(x_i, y_i) + \sum_{j=1}^{H+1} \lambda_j \left\| \frac{\partial h_j^i}{\partial h_{j-1}^i} \right\|_2 \right), \quad (56)$$

where λ is a constant that control the importance of the layer-wise penalty term and $\mathcal{L}(x, y)$ is the classification loss (e.g., cross-entropy). Here, h_j^i represents the activation at the hidden layer j given the i -th input x_i . Intuitively, this method establishes a tension: between the classification loss, which requires the network to capture useful information in the input, and the contractive loss, which encourages it to throw away redundant information. As a result, the model gains some invariance to the small pixel-wise perturbations typically introduced by adversarial attacks.

Gu and Rigazio [180] evaluated this strategy against the L-BFGS attack and showed that while the attack still successfully found adversarial examples that fool DCN, the average adversarial perturbations needed is larger compared to when attacking standard model. This perhaps is one of the earliest defense methods proposed since the findings of adversarial examples for neural networks in Szegedy et al. [31].

6.1.3 Defensive Distillation

The term *distillation* was previously introduced by Hinton et al. [200] as a method to compress knowledge from an ensemble of deep neural networks into a single neural network. Similarly, defensive distillation [43] is a defense method that works by training two networks, where one network (the “student”) is trained to approximate the other (the “teacher”).

Defensive distillation works as follows. First, the “teacher” network is trained with a modified softmax function at the output layer, including a temperature constant T , where $T \geq 1$, that is

$$\text{softmax}(Z(x)) = \frac{e^{Z(x)_i/T}}{\sum_{c=0}^C e^{Z(x)_c/T}}, \quad (57)$$

where $Z(x)$ is the logit vector, and C is the number of classes. Higher temperatures lead to a flatter softmax, thus introducing more noise into the decision process. After training the first network, the second network is trained using the predictions *from the first network* as the training labels for the training data. The hope is that this prevents the distilled network from overfitting. Figure 18 illustrates the mechanics of defensive distillation. During test time, the temperature constant of the distilled model is set back to 1.

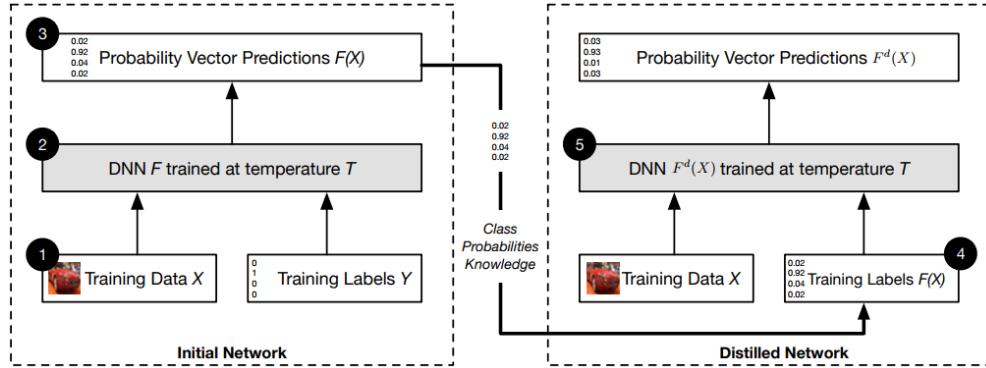


Figure 18: Illustration of defensive distillation (taken from Papernot et al. [43]).

Papernot et al. [43] showed how increasing the temperature of the softmax function causes the probability vector to converge to $\frac{1}{C}$ as $T \rightarrow \infty$. In other words, the predictions from both the teacher and student models are trained to be smooth. They also showed that the Jacobian of the model with respect to input features is inversely proportional to the temperature: the higher the temperature, the lower the dependence upon input features. They argued that when the temperature is brought back to 1 during test time, it will only cause the probability vector to be more discrete but will not change the Jacobian of the model, arriving at a model with reduced sensitivity to small changes in the input (a similar logic to the Deep Contractive Network in Section 6.1.2).

Although defensive distillation was shown to be robust against adversarial examples generated using the JSMA-F [80] (see Section 4.8), this defense was found to be vulnerable to a variant of JSMA-Z [181], C&W attacks [44] (see Section 4.11), as well as SBA [41] (see Section 4.9). Carlini and Wagner [44, 181] evaluated this defense and pointed out how defensively distilled model produces logits with higher values compared to standard models. They observed that if the values of the correct logit are large, the softmax probability of the correct class will be closer to 1.0 while those of the non-maximum elements become smaller. They also found that the values of non-maximum element are even smaller than the precision of 32-bit floating values, and thus are rounded to 0. In this case, the gradients of these units with respect to the input will be 0, which may cause attacks like JSMA-F to fail in some cases. This is an interesting twist, given that the intention of the temperature parameter was originally to produce a smoother output distribution. Carlini and Wagner [181] showed that this defense can be circumvented by JSMA-Z variant where the logits are divided by the temperature constant T before being used to calculate the gradients.

6.1.4 MagNet

MagNet [81] is a multi-pronged approach to robustness, which requires a pair of autoencoders: a detector (D) and a reformer networks (R). Both are trained to reconstruct clean examples. However, the detector D is used to detect if an input is adversarial or not, while the reformer R is used to remove adversarial perturbations from adversarial inputs, moving examples back towards the manifold of clean data.

Since D has been trained to reconstruct clean examples, the detector network outputs images that are close to the distribution of the clean samples, even when the inputs to the detector network are adversarial. If the input was already a clean example, then the output of the detector network looks very similar; if the input was in fact adversarial, then the reconstruction loss between input and output will be high. One can then perform adversarial detection by setting a threshold value on the input reconstruction error.

Since naively measuring the reconstruction error only works if adversarial perturbations are large, [81] leverage the target classifier network f in their detection algorithm. They do this by measuring the Jensen-Shannon Divergence (D_{JS}) [201] between f 's output when fed the original image and f 's output when fed the detector-preprocessed image. The D_{JS} can be understood as symmetric version of the Kullback-Leibler divergence [127]. Formally, the D_{JS} is defined as

$$D_{JS}\left(f(x) \parallel f(D(x))\right) = \frac{1}{2}D_{KL}\left(f(x) \parallel M\right) + \frac{1}{2}D_{KL}\left(f(D(x)) \parallel M\right), \quad (58)$$

where $M = \frac{f(x)+f(D(x))}{2}$, and D_{KL} is the Kullback-Leibler divergence, $D_{KL}(P \parallel Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)}$.

Meng and Chen [81] argued that although the difference between x' and $D(x')$ may be small (e.g., when x and x' are similar), the difference between $f(x')$ and $f(D(x'))$ will be large due to the misclassification by the target network. Conversely, the difference between $f(x)$ and $f(D(x))$ stays small. Thus, the measure of the D_{JS} gives a signal of whether an input is adversarial or not. To improve numerical stability, Meng and Chen [81] set the temperature constant of the softmax function to be larger than one, just as in defensive distillation [43] (see Section 6.1.3).

Meng and Chen [81] realized that the whole MagNet pipeline is differentiable, making it vulnerable in whitebox settings. They thus suggested to use multiple detector and reformer networks, and then to randomly choose two of the candidates as the detector and reformer networks during test time. A regularization term

that penalizes similarity between candidates was also proposed. Formally, the training objective is defined as

$$\sum_{i=1}^n \|x - C_i(x)\|_2 - \lambda \sum_{i=1}^n \|C_i(x) - \frac{1}{n} \sum_{j=1}^n C_j(x)\|_2, \quad (59)$$

where n is the number of candidates and C_i denotes the i -th candidate. In Equation 59, the first term is the reconstruction loss while the second term is the penalty term which encourages diversity of candidates (as the defense will not be meaningful if the candidates are similar).

Meng and Chen [81] showed that MagNet is robust against various attacks such as the FGSM [32] (see Section 4.2), BIM [45, 77] (see Section 4.3), DeepFool [79] (see Section 4.7), and C&W attacks [44] (see Section 4.11). Nevertheless, Carlini and Wagner [202] found that MagNet is still vulnerable to the SBA [41] (see Section 4.9) where the whitebox method used to attack the substitute model was the C&W attack [44] (see Section 4.11).

6.1.5 PGD Adversarial Training

Building on previous attempts [203, 204] which defined adversarial robustness from a robust optimization [205] perspective, Madry et al. [145] proposed a variant of adversarial training [32] (see Section 6.1.1) on worst-case adversaries (see below for an explanation of how “worst-case” is defined). In the framework of robust optimization, the training objective is defined as:

$$\arg \min_{\theta} \mathbb{E} \left[\max_{\|x' - x\|_{\infty}} \mathcal{L}(x', y) \right]. \quad (60)$$

In this formulation, the inner maximization aims to find adversarial examples that maximize a loss function, while the outer minimization refers to the training process which aims to find a set of parameters θ that will minimize the worst-case loss. This is similar to the minimax loss used in game-playing: we are trying to minimize the impact of our adversaries worst moves. Note how this is different than standard adversarial training in the sense that the standard method trains a model on *both* clean and adversarial examples, while in this framework the model is trained only on the adversarial examples. In other words, PGD adversarial training is equivalent to setting α to 0 in Equation 55 in Section 6.1.1.

Madry et al. [145] argued that adversarial examples generated using randomly initialized BIM [45, 77] (see Section 4.3), which they refer to as Projected Gradient Descent (PGD), are the worst case adversarial examples. They showed that even though PGD was restarted from different starting points (e.g., by adding small random perturbations to the initial input) for several runs, the loss value of a model on these adversaries always plateaus at a similar level. They therefore argued that this suggests the existence of numerous local maxima with similar values, which are similar to the global maximum. This perhaps echoes the argument in [206] in which the authors argued that the surface loss of neural networks has *many local minima with similar values*. Based on these findings, Madry et al. [145] suggested that robustness against PGD adversaries approximately solves the min-max formulation in Equation 60, thus should provide robustness against other first-order adversaries. Concretely, PGD adversarial training was performed by training the network *only on adversarial examples* generated by PGD with random starting points, which one may see as an iterative steps variant of R+FGSM [47] (see Section 4.5).

They found that larger capacity models (e.g., models with more tunable parameters) receive more benefit from this defense approach compared to smaller capacity models. They hypothesized that a model needs to be capable of producing more complicated decision boundaries in order to be robust against adversarial examples, and thus may require more capacity. This argument is supported empirically by the observation that maximum loss decreases as the capacity of the model increases. They also found that increases in capacity helps to reduce effectiveness of transferable adversarial examples. The experimental results show how this defense is *consistently* robust to various types of attacks in both whitebox and blackbox settings, although the defended model may not achieve state-of-the-art performance. This defense was the only defense evaluated by Athalye et al. [55] that can live up to its claims. Uesato et al. [97] also showed how this defense

does not rely on gradient masking by evaluating this defense against SPSA (see Section 4.27), which is a gradient-free adversarial attack.

As a follow-up work, Tsipras et al. [207] showed several unexpected benefits to training models with this method. First, they showed how models trained using PGD-AT tend to only utilize features that are strongly correlated with the correct label, effectively reducing the attack surface (thus implicitly achieving the same goal as the Deep Contractive Network, but better, see Section 6.1.2). They argued that standard classifiers utilize too many features that are weakly correlated with the correct label in order to achieve high accuracy, thus sacrificing adversarial robustness. Lastly, they showed how the gradients of a robust model is visually interpretable to a human with no additional steps required, precisely because the robust solution relies upon a small number of important features rather than a large number of weakly relevant ones. Note that other gradient-based explainability methods such as Gradient-weighted Class Activation Mapping (Grad-CAM) [208] needs to perform additional steps to achieve visually interpretable saliency maps. Similar findings were also reported by Engstrom et al. [209].

Although PGD-AT seems to be promising, the benefits do not come for free. For example, PGD-AT was shown to compromise the model’s accuracy on clean examples dramatically [207]. Furthermore, the computational cost of this method is higher than standard adversarial training, since the cost scales with the number of PGD iterations. More recent works also showed how PGD adversarial training is mainly only robust against certain types of adversary used during the training, but not to the others [187, 210, 211].

6.1.6 Ensemble Adversarial Training

Ensemble adversarial training [47] is a variant of adversarial training [32] (see Section 6.1.1) in which a model is retrained on adversarial examples generated to attack *various other pre-trained models*. This decoupling of target model and adversarial training examples overcomes the overfitting observed with the vanilla version of adversarial training. Tramèr et al. [47] argued that ensemble adversarial training is a good approximation of the inner maximization shown in Equation 60 due to the transferability of adversarial examples between different models. Moreover, since the adversarial examples generation process is independent from the model that is being trained, they hypothesized ensemble adversarial training to be more robust to future blackbox attacks compared to the standard adversarial training.

In practice, Tramèr et al. [47] alternate the source of adversarial examples between the currently trained and other pre-trained models, where the pre-trained models are chosen randomly per batch. This is done in order to ensure diversity of adversarial examples during training. Tramèr et al. [47] noted that the gradients of the pre-trained models can be *pre-computed* for the whole training dataset. Since we are not updating the weights of the pre-trained models, the computation needed per training batch in ensemble adversarial training is thus lower compared to standard adversarial training.

Tramèr et al. [47] demonstrated that this method outperforms regular adversarial training on ILLCM adversaries (see Section 4.4) in blackbox settings. In their experiments, the models were evaluated against SBA [41] (see Section 4.9) that used FGSM [32] (see Section 4.2) to attack the substitute model. However, they also found that ensemble adversarial training is slightly less accurate and slower to converge compared to the standard method. They also demonstrated the scalability of ensemble adversarial training by evaluating their defense on ImageNet dataset.

As discussed in Section 4.5, performing standard adversarial training causes the defended model to be more robust against 2-step BIM [45, 77] (see Section 4.3) than R+FGSM [47] (see Section 4.5), strengthening the suspicion of gradient masking. Tramèr et al. [47] showed that this ratio is decreased in the ensemble case. Nevertheless, ensemble adversarial training is still not immune to adversarial examples as it is still circumventable by R+FGSM.

6.1.7 Random Resizing and Padding as a Defense

Xie et al. [51] introduced a defense based on Random Resizing and Padding (RRP). The goal of this approach is to remove perturbations through input transformation and introduce randomness during inference so that the gradient of the loss with respect to the input is harder to compute. Concretely, RRP is implemented

as two additional layers placed right after the input layer of a neural network. The random resizing layer resizes the input image to several numbers of resized images, where the differences between dimensions of input images before and after resizing layer are small. The random padding layer randomly pads the resized images with zeros, returning several padded images. One of these padded images is then randomly selected to be classified by the classifier.

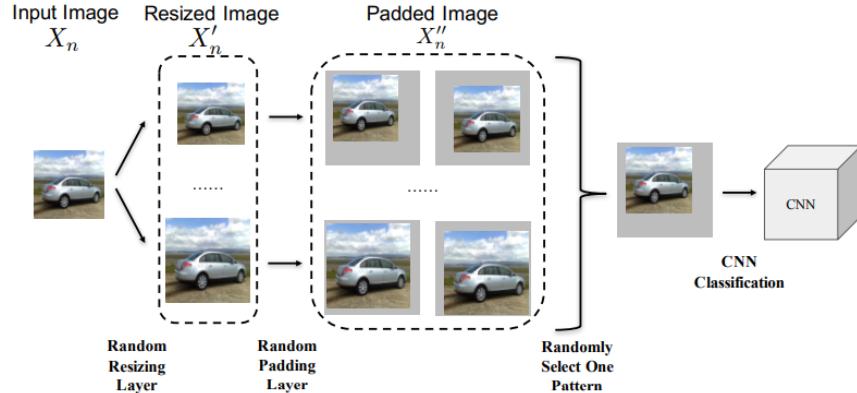


Figure 19: Illustration of RRP (taken from Xie et al. [51]).

They demonstrated that the proposed method requires no fine-tuning of the defended model without sacrificing accuracy on clean examples and can be combined with other defense methods such as adversarial training [32] (see Section 6.1.1). This defense method showed good performance against various whitebox attacks such as the FGSM [32] (see Section 4.2), BIM [45, 77] (see Section 4.3), DeepFool [79] (see Section 4.7), and C&W [44] (see Section 4.11) attacks. Furthermore, this defense was ranked 2nd in the NIPS 2017 adversarial examples defense challenge [144].

Xie et al. [51] argued that the space of random resizing and padding is sufficiently large as to be computationally intractable for an attacker. However, both Athalye et al. [55] and Uesato et al. [97] showed that RRP relies on gradient masking [55], and can be circumvented using EOT [96] (see Section 4.25).

6.1.8 Stochastic Activation Pruning

Dhillon et al. [50] proposed a defense mechanism based on stochastic policy called Stochastic Activation Pruning (SAP) which randomly prunes or drops some activations (i.e., set to 0) during test time. The probability of the nodes j at i -th layer p_j^i to be sampled, or survive, is proportional to the magnitude of the activation. This means that the larger an activation is, the smaller the probability that activation will be pruned. The survival probability p_j^i is calculated as

$$p_j^i = \frac{|h_j^i|}{\sum_{k=1}^{K^i} |h_k^i|}, \quad (61)$$

where h_j^i denotes the activation of the j -th node at layer i , and K^i denotes the number of activation nodes at the i -th layer.

The magnitude of the activations that survive at the i -th layer are then scaled up by the inverse of p_j^i given by

$$h_j^i \odot \frac{\mathbb{I}(h_j^i)}{1 - (1 - p_j^i)^{r^i}}, \quad (62)$$

where $\mathbb{I}(h_j^i)$ returns 1 if h_j^i was sampled at least once, and returns 0 otherwise, i.e., the node is pruned. Here, r^i denotes the number of samples to be drawn at i -th layer. Dhillon et al. [50] argued that the goal of

rescaling the activations is to make the pruned model behaves similarly to the original model when dealing with non-adversarial inputs, while being more robust to adversarial examples since the stochasticity in SAP causes the gradients to be hard to compute by an attacker. The SAP algorithm is described in Algorithm 17.

Algorithm 17 SAP [50]

Input: input $x = h^0$, neural network f with L layers, weights of the neural network W at each layer, non-linear activation functions used in each layer ϕ , number of samples per layer r^i , set of activation units not to be pruned S

Output: predicted label $\hat{y}(x)$

Initialize: $S \leftarrow \{\}$

for each layer i **do**

$h^i \leftarrow \phi^i(W^i h^{i-1})$

for each activation unit j in layer i **do**

$p_j^i \leftarrow \frac{|h_j^i|}{\sum_{k=1}^{K^i} |h_k^i|}$

end for

$S \leftarrow \{\}$

for number of samples r^i **do**

Sample $j \sim h^i$ based on p_j^i

$S \leftarrow S \cup \{j\}$

end for

for each index $j \notin S$ **do**

$h_j^i \leftarrow 0$

end for

for each index $j \in S$ **do**

$h_j^i \leftarrow \frac{h_j^i}{1 - (1 - p_j^i)^{r^i}}$

end for

end for

$\hat{y}(x) \leftarrow \arg \max_c (\text{softmax}(h^L))_{(c)}$

Return: $\hat{y}(x)$

This method is similar to performing dropout [212] during test time. The difference is that dropout assigns the probability for the nodes to be pruned uniformly, while SAP assigns them based on the magnitude of the activation and rescales the magnitude of the surviving nodes. Dhillon et al. [50] argued that these differences allow SAP to be added to any pre-trained models without the need of fine-tuning, whilst maintaining accuracy on clean data.

Dhillon et al. [50] showed that SAP can defend against FGSM [32] (see Section 4.2), where Monte Carlo sampling [213] is used to approximate the gradients. SAP was also shown to increase the robustness of Double Deep Q-Learning (DDQN) [214] algorithm, which is a reinforcement learning algorithm that uses neural networks to parametrize the action-value function, against adversarial inputs when tested on various Atari games environment [108]. Furthermore, they also showed how SAP can be combined with other defense methods such as adversarial training [32] (see Section 6.1.1) to further enhance robustness.

Nevertheless, SAP has been shown to rely on gradient masking and vulnerable to an iterative attack which computes the gradients based on the expectation of randomness [55]. Instead of computing $\nabla_x f(x)$ once for each input, the attack computes it based on k predictions and moves in the direction of $\sum_{i=1}^k \nabla_x f(x)$. Athalye et al. [55] also suggested performing gradient clipping when attacking SAP to avoid exploding gradients due to the existence of many nodes with zero activations.

6.1.9 Total Variance Minimization and Quilting

Chuan Guo [54] apply various image transformations to an input before classification. These transformations

included image cropping and rescaling, bit-depth reduction [197], JPEG compression [215], Total Variance Minimization (TVM) [154], and image quilting [216]. They found that TVM and image quilting were the most effective, especially when the model is trained on the transformed images. Both TVM and image quilting introduce randomness, and are non-differentiable operations which makes it harder for an attacker to compute the gradient of the model. These defenses are model-agnostic which means the model does not need to be retrained or fine-tuned, although finetuning was shown to improve the performance of the defended model. These defenses can also be coupled with other defense methods.

TVM as a defense can be implemented by randomly picking pixels from an input and performing iterative optimization to find an image whose colors are consistent with the randomly picked pixels. Concretely, this can be implemented by solving

$$\arg \min_{\hat{x}} \|(1 - \tilde{x}) \odot (\hat{x} - x)\|_2 + \lambda \cdot TV(\hat{x}), \quad (63)$$

where \tilde{x} is Bernoulli random variables (i.e., either 0 or 1) sampled at each pixel location in the input x (i.e., \tilde{x} has the same dimension as x), and λ is a weighting constant. Here, the total variance $TV(\hat{x})$ is calculated by

$$TV(\hat{x}) = \sum_{k=1}^{Ch} \left[\sum_{i=2}^R \|\hat{x}_{(i,:,k)} - \hat{x}_{(i-1,:,k)}\|_p + \sum_{j=2}^C \|\hat{x}_{(:,j,k)} - \hat{x}_{(:,j-1,k)}\|_p \right], \quad (64)$$

where R , C , and Ch denote the number of rows, columns, and channels, respectively. In their work, Chuan Guo [54] set $p = 2$. The intuition behind performing total variance minimization is to encourage spatial smoothness, which may lead to the removal of adversarial perturbations.

Image quilting involves reconstructing an image using small patches taken from some database. As an adversarial defense method, one needs to ensure that the database only contains non-adversarial patches. Given a patch from an image, one can first find the nearest neighbors of the patch (e.g., using kNN) in the database according to the distance in the pixel space. One of the patches found is then randomly chosen to replace the original patch. The intuition behind image quilting is to construct an image that is free of adversarial perturbations, since quilting only uses clean patches to reconstruct the image. In addition, quilting also adds some randomization components during the process of selecting clean patches.

Chuan Guo [54] showed that total variance minimization and quilting outperform other image transformation methods when tested against FGSM [32], BIM [45, 77], DeepFool [79], and C&W [44] attacks when the model is also trained on transformed images. However, there are some tradeoffs of using these defenses. For example, total variance minimization causes slower inference since it needs to solve the optimization for every input, while image quilting degrades the accuracy of the model on non-adversarial inputs. Furthermore, these defense methods were not evaluated in whitebox settings where an attacker can adapt the attack strategy based on the defense used, and were later found to be circumventable using combination of BPDA [55] through the identity function (see Section 4.26) and EOT (see Section 4.25) [96].

6.1.10 Thermometer Encoding

Thermometer Encoding [48] (TE) is a defense based upon the hypothesis that the linearity of neural networks render them vulnerable to attack [32]. TE quantizes and discretizes the input data, effectively drowning out the effect of small perturbations of the kind typically introduced by adversarial attacks. Formally, the input signal is first quantized according to the desired discretization level l . Given the i -th element of an input signal x_i , the quantization function $q(x_i)$ returns the largest index $k \in \{1, \dots, l\}$ where $x_i < \frac{k}{l}$. For example, if $l = 10$, then $q(0.72) = 8$.

The thermometer vector τ can then be found by

$$\tau(q(x_i))_k = \begin{cases} 1 & \text{if } k \geq q(x_i) \\ 0 & \text{otherwise} \end{cases}, \quad (65)$$

where $k \in \{1, \dots, l\}$ is the index of the thermometer encoded vector, i.e., $\tau(q(x_i)) \in \mathbb{R}^l$. For example, if $l = 10$, then $\tau(q(0.13)) = [011111111]$. For simplicity, we denote $T_e = \tau(q(x_i))$.

Intuitively, small perturbations that are less than the minimum discretization level will not have an effect on the thermometer-encoded signals (e.g., for $l = 10$, $x_i = 0.72$ or $x_i = 0.75$ will produce same encoded signal, that is $T_e = [0000000111]$). Furthermore, TE works as a defense because the thermometer encoding is non-linear and non-differentiable, which makes it harder for the attacker to compute the gradients.

Jacob Buckman [48] showed that the combination of TE and adversarial training [32] (see Section 6.1.1) yields high adversarial robustness, and even surpasses PGD adversarial training [145] (see Section 6.1.5). In their experiment, l was set to 16, and the evaluations were done on MNIST, CIFAR10, CIFAR100, and SVHN datasets. Nevertheless, TE is considered to rely on gradient masking and circumventable using BPDA [55] (see Section 4.26, where we also provide a concrete example on how to circumvent TE with BPDA as shown by Athalye et al. [55]), which approximates thermometer encoding function in a differentiable form, allowing an attacker to approximate the gradients of the model.

6.1.11 PixelDefend

Yang Song [53] introduced PixelDefend, which aims to “purify” an input before passing it to the classifier. They argued that adversarial examples lie in the low probability regions of the training data distribution which lead a model to suffer from covariate shift [217]. PixelDefend uses a generative model trained only on clean data in order to approximate the distribution of the data. The trained generative model should then output data that represents the distribution of the clean training data even when dealing with adversarial inputs. The principle here is strongly reminiscent of MagNet (see Section 6.1.4), although in this case a single model plays the role of both detector and reformer.

In PixelDefend, the generative model used was the PixelCNN [218, 219]. Note that for an 8-bits RGB image x , $P_{CNN}(x)$ is in $\mathbb{R}^{i \times j \times c \times dr}$ where (i, j, c, dr) denotes the (row, column, channel, dynamic range) of the input. The dynamic range in this case is 256.

Algorithm 18 PixelDefend [53]

```

Input: image  $x \in \mathbb{R}^{i \times j \times c}$ , pre-trained PixelCNN  $P_{CNN}$ , defense parameter  $\epsilon_{defend}$ 
Output: purified image  $\hat{x}$ 
Initialize:  $\hat{x} \leftarrow x$ 
for each row  $i$  do
    for each column  $j$  do
        for each channel  $c$  do
            range  $R \leftarrow [\max(x_{i,j,c} - \epsilon_{defend}, 0), \min(x_{i,j,c} + \epsilon_{defend}, 255)]$ 
             $\hat{x}_{i,j,c} \leftarrow \arg \max_{z \in R} P_{CNN}(\hat{x})_{i,j,c,z}$ 
        end for
    end for
end for
Return:  $\hat{x}$ 

```

Algorithm 18 describes how PixelDefend works. Note that one needs to set the value of ϵ_{defend} , which controls the maximum change in pixel value during purification process such that $\|\hat{x} - x\|_\infty \leq \epsilon_{defend}$. If ϵ_{defend} is too large, the purified input may not look like the original input anymore, leading to misclassification. If ϵ_{defend} is too small, the purified input may not be completely free of adversarial perturbations. In an ideal situation, given that an attacker can generate adversarial examples where $\|x' - x\|_\infty \leq \epsilon_{attack}$, ϵ_{defend} should be set to be equal to ϵ_{attack} .

In addition, Yang Song [53] showed that PixelDefend can also be used to detect and reject adversarial examples instead of robustifying the target classifier by performing statistical hypothesis testing using a p -value. This is done by comparing the probability density of an input to the training examples under the generative model.

PixelDefend was shown to be effective against various attacks such as FGSM [32] (see Section 4.2), BIM [45, 77] (see Section 4.3), DeepFool [79] (see Section 4.7), and C&W [44] (see Section 4.11). Nevertheless, PixelDefend was later found to be vulnerable to BPDA [55] (see Section 4.26) and SPSA [97] (see Section 4.27).

6.1.12 Defense-GAN

Similar to PixelDefend [53] (see Section 6.1.11), a concurrent work called Defense-GAN [52] uses generative model trained only on clean data as a way to remove adversarial perturbations. Defense-GAN uses a generative transformation network G that is trained using the GAN framework [63] with Wasserstein loss [148]. Projection of an adversarial example onto the manifold of the trained generator is believed to remove adversarial components from an adversarial input.

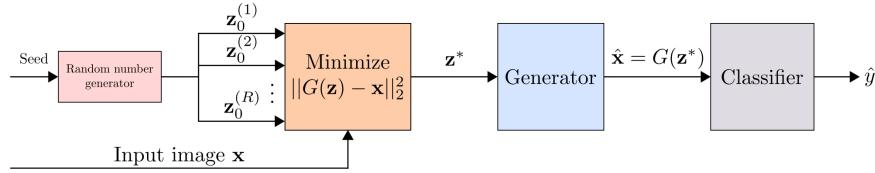


Figure 20: Illustration of Defense-GAN (taken from Pouya Samangouei [52]).

Defense-GAN works as follows. Defense-GAN first initializes R random vectors, i.e., $Z = \{z_0, \dots, z_R\}$, and tries to find $z^* = \arg \min_{z \in Z} \|G(z) - x\|_2^2$, where Z^* is found by performing gradient descent for each $z \in Z$ to minimize $\|G(z) - x\|_2^2$. Once done, z^* is used to generate the input instance by passing it through the generator, which will then be classified. Although the extra gradient descent steps increases computational complexity, Pouya Samangouei [52] argued that Defense-GAN is harder to be attacked by gradient-based attacks since one has to “unroll” the gradient descent iterations.

Pouya Samangouei [52] showed that Defense-GAN can also be used to detect and reject adversarial examples. For example, this can be done by performing threshold-based detection on the value of $\|G(z^*) - x\|_2^2$. They showed how this method can be used to reliably detect FGSM adversaries on MNIST [116] and Fashion MNIST (F-MNIST) [119] datasets with fairly high AUC score.

Defense-GAN was found to be more stable compared to MagNet [81] and adversarial training [32] (see Section 6.1.1) when tested on various models on MNIST and F-MNIST datasets in blackbox setting against FGSM-SBA [41] (see Section 4.9) although the robustness of adversarial training is sometimes higher. Furthermore, Defense-GAN showed superior performance compared to MagNet and adversarial training when tested against FGSM [32] (see Section 4.2), R+FGSM [47] (see Section 4.5), and C&W L_2 [44] (see Section 4.11) attacks on both MNIST and F-MNIST. Nevertheless, Athalye et al. [55] found that Defense-GAN is not as effective on defending CIFAR10 models. Moreover, just as with PixelDefend, Defense-GAN was also found to be vulnerable to BPDA [55] (see Section 4.26).

6.1.13 WRM: A Distributionally Robust Optimization with Adversarial Training

While adversarial training is relatively easy to implement and reasonably effective, it does not guarantee that an adversarially trained model will be robust against all types of adversaries, nor does it guarantee robustness against some particular type of ϵ -budgeted adversaries. Formal verification techniques of machine learning models that guarantee robustness abound [220, 221, 222]. However, most of these techniques are in general intractable. Sinha et al. [182] proposed a principled adversarial training method called WRM⁷ that balances tractability with provable robustness guarantees, at least to some small ϵ -bounded perturbations under certain similarity metric, that is based on Wasserstein distributional robustness.

Sinha et al. [182] view adversarial defense as a distributionally robust optimization problem. More explicitly, given training distribution X and another data distribution around it X' , if we denote by θ as the

⁷Sinha et al. [182] refer to their method as WRM but we are not entirely sure what WRM stands for.

parameters of a neural network model, $(x', y') \in X'$ as an input-label pair, and some loss function $\mathcal{L}(\cdot)$, the goal is to optimize the following objective function:

$$\arg \min_{\theta} \sup_{X'} \mathbb{E}_{X'} [\mathcal{L}(x', y')]. \quad (66)$$

Sinha et al. [182] first considered some robustness region under the Wasserstein metric $W_c(\cdot)$ where $W_c(X', X) \leq \rho$, and stated that solving Equation 66 for some arbitrary ρ is not tractable. They then considered the Lagrangian relaxation of the problem, and the objective for the inner maximization now becomes

$$\arg \min_{\theta} \left\{ \sup_{X'} \mathbb{E}_{X'} [\mathcal{L}(x', y')] - \gamma W_c(X', X) = \mathbb{E}_X [\sup_{x' \in \mathcal{Z}} \mathcal{L}(x', y') - \gamma \cdot c(x', x)] \right\}, \quad (67)$$

where $x \in X$, $\gamma \geq 0$ is a penalty weight, \mathcal{Z} is the universe of all possible examples, and $c(\cdot)$ is a cost for the attacker to modify x into x' . Concretely, Sinha et al. [182] considered $c(x, x') = \|x - x'\|_p^2$, where $p \geq 1$. They then showed that the worst-case error of a model trained with WRM is bounded by

$$\sup_{X': W_c(X', X) \leq \rho} \mathbb{E}_{X'} [\mathcal{L}(x', y')] \leq \mathbb{E}_{X_{test}} [\sup_{X'} \mathcal{L}(x', y) - \gamma \cdot c(x_{test}, x')] + \gamma \cdot \rho, \quad (68)$$

where X_{test} is the empirical distribution of test data, and $\rho = \mathbb{E}_{X_{test}} [c(x', x_{test})]$ can be calculated empirically. Note that x' is obtained by solving the inner maximization in Equation 67.

Sinha et al. [182] showed that for smooth $\mathcal{L}(\cdot)$ and large enough γ (or small enough ρ by duality), the inner optimization problem is strongly concave and thus solvable using gradient descent. Another important assumption to note is that the activation function used by the neural networks has to be smooth to ensure convergence, so functions like the ReLU should not be used. In practice, Sinha et al. [182] recommend to use either sigmoid or the Exponential Linear Units (ELU) [223]. Keeping all these in mind, WRM was developed and the algorithm is described in Algorithm 19. It is worth to note that the guarantee of WRM does not hold for $p = \infty$. Sinha et al. [182] then proposed a proximal algorithm to solve the inner optimization problem when $p = \infty$. We refer readers to the paper for the proximal algorithm. We also refer readers to the paper for the proofs of all the claims made in developing WRM.

Algorithm 19 WRM [182]

```

Input: A non-adversarial dataset  $X$ , number of iterations  $I$ , stepsize sequence  $\alpha = \{\alpha_0, \dots, \alpha_{I-1}\}$ 
Output: Adversarially robust  $\theta$ 
for  $i = 0$  to  $I$  do
     $x' \leftarrow \arg \max_{x'} \epsilon \cdot \mathcal{L}(x', y) - \gamma \cdot c(x, x')$ , where  $(x, y) \sim X$ 
     $\theta \leftarrow \theta - \alpha_i \nabla_{\theta} \mathcal{L}(x', y')$ 
end for

```

They empirically showed that the worst-case error of WRM is always below what the certificate of robustness guarantees when tested on MNIST for $p = 2$ and $\gamma = 0.3684$. Furthermore, WRM was shown to be more robust compared to various existing adversarial training methods when evaluated against L_2 and L_∞ adversaries for small ϵ . Moving forward, methods that can provide guarantee for higher robustness and works in more complex datasets are still needed.

6.1.14 High-Level Representation Guided Denoiser

Liao et al. [159] argued that in order to mitigate adversarial perturbations, one needs to be able to denoise the adversarial examples. They suggested that this can be done by training a denoiser D that learns to generate negative noise maps $d\hat{x}$ given an image as input, i.e., $D(x) = d\hat{x}$. The function of the generated negative noise maps is to remove adversarial noise when added to the adversarial examples x' , where the

denoised image is calculated by $\hat{x} = x' - d\hat{x}$. In practice, the denoiser that Liao et al. [159] used follows the architecture of U-Net [224].

The training objective of the denoiser is to minimize the difference between the high level representations of the inputs and the denoised inputs, hence the name High-Level Representation Guided Denoiser (HGD). Formally, the denoiser is trained to minimize $\|f_l(\hat{x}) - f_l(x)\|_1$, where $f_l(x)$ denotes the output of the classification convolutional neural network f at the l -th layer. Liao et al. [159] experimented with two different choices of l : the last convolutional layer and the logits layer of f . These models were referred as the Feature Guided Denoiser (FGD) and the Logits Guided Denoiser (LGD), respectively. Another variant of HGD was also introduced by minimizing the classification loss of f called the Class Label Guided Denoiser (CGD). These are illustrated in Fig. 21.

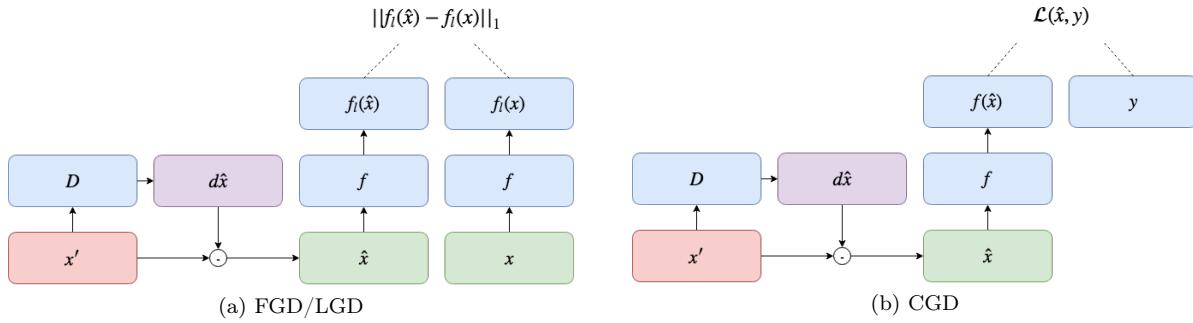


Figure 21: Illustration of FGD, LGD, and CGD (adapted from Liao et al. [159]).

In their experiments, the adversarial examples used to train the denoiser were generated using FGSM [32] (see Section 4.2) and BIM [45, 77] (see Section 4.3) on various ImageNet models. This resulted in 210,000 training data, consisting of 30K clean inputs randomly sampled from ImageNet training set (30 images per class), and 180K adversarial examples. The denoiser can be trained using only these 210K examples, conspicuously more efficient compared to adversarial training [32] (see Section 6.1.1) and ensemble adversarial training method [47] (see Section 6.1.6). HGD requires only 30 training epochs on the 210K examples, a huge improvement in speed relative to ensemble adversarial training on ImageNet which usually requires more than 150 epochs on much larger size of training examples.

Liao et al. [159] suggested that LGD is the best performer compared to FGD and CGD, giving a good balance between correctly classifying clean and adversarial inputs. This defense method was shown to be transferable, in the sense that denoiser that is trained using a particular classifier can also be used to defend other classifiers. HGD is the winning submission for the NIPS 2017 Defense Against Adversarial Attack Competition [144]. Nevertheless, just like PixelDefend [53] (see Section 6.1.11), HGD was also found to be vulnerable to SPSA [97].

6.1.15 Adversarial Logit Pairing

Kannan et al. [183] proposed a logit pairing defense mechanism that encourages the logits of input pairs (i.e., adversarial and non-adversarial input pairs) to be similar. Two different logit pairing strategies were introduced: Adversarial Logit Pairing (ALP) and Clean Logit Pairing (CLP). The motivation behind ALP is to enforce logits invariance between a *clean input* and its *adversarial counterpart*, while CLP enforces logits invariance between *any pairs of inputs*. Surprisingly, the latter approach yields significant robustness improvements, despite the fact that examples are frequently drawn from disparate classes.

Formally, ALP introduces a regularization term that penalizes for the differences of logits in minibatches of clean inputs $\{x_1, \dots, x_{\frac{n}{2}}\}$ and their adversarial counterparts $\{x'_1, \dots, x'_{\frac{n}{2}}\}$ generated by PGD attack [145] (see Section 6.1.5), where n denotes the size of the minibatch. Given $Z(x)$ as the logits vector, the training objective becomes

$$\alpha \cdot \frac{2}{n} \sum_{i=1}^{\frac{n}{2}} \mathcal{L}(x_i, y_i) + (1 - \alpha) \cdot \frac{2}{n} \sum_{i=1}^{\frac{n}{2}} \mathcal{L}(x'_i, y_i) + \lambda \cdot \frac{2}{n} \sum_{i=1}^{\frac{n}{2}} \mathcal{L}_{LP}(Z(x_i), Z(x'_i)), \quad (69)$$

where the first two terms denote the adversarial training loss, similar to Equation 55, and \mathcal{L}_{LP} denotes the logit pairing loss (e.g., Kannan et al. [183] used the L_2 loss in their experiments).

Kannan et al. [183] showed that the combination of adversarial training on PGD attack with ALP resulted in state of the art robustness against both whitebox (variants of FGSM [32] (see Section 4.2) and PGD [45, 77] (see Section 4.3) attacks), as well as blackbox attacks (e.g., SBA [41] (see Section 4.9)) on ImageNet models. Note that scaling adversarial defense methods to large datasets such as ImageNet has been shown to be challenging and computationally expensive [45].

CLP, on the other hand, compares the logits between *random* pairs of clean inputs that *do not have to come from the same class*. The training objective for CLP is defined as:

$$\sum_{i=1}^n \mathcal{L}(x_i, y_i) + \lambda \cdot \frac{2}{n} \sum_{i=1}^{\frac{n}{2}} \mathcal{L}_{LP}(Z(x_i), Z(x_{i+\frac{n}{2}})), \quad (70)$$

where the first term denotes the cross-entropy loss for classification task without including any adversarial examples in the training set. CLP was initially introduced as a way to understand the contribution of the logit pairing itself without the advantage of performing adversarial training.

Surprisingly, they found that the use of CLP alone leads to increase in adversarial robustness. They hypothesized that CLP implicitly encourages the norm of the logits to be small, which prevents the model from being overconfident of its predictions. Building upon the unexpected success of CLP, Clean Logit Squeezing (CLS) was introduced as a method that explicitly penalizes the norm of the logits. The training objective of CLS is

$$\sum_{i=1}^n \mathcal{L}(x_i, y_i) + \lambda \cdot \frac{1}{n} \sum_{i=1}^n \|Z(x_i)\|_p, \quad (71)$$

where p denotes the p -norm. Directly penalizing the loss with the norm of the logits through CLS was shown to also increase adversarial robustness.

Nevertheless, Engstrom et al. [184] showed that ALP can be circumvented by PGD if the attacker performs enough PGD steps. They argued that there are two main differences between ALP and PGD adversarial training which may cause ALP to not have the same level of robustness with PGD adversarial training although ALP is built on top of it. The first difference is that ALP violates the robust optimization formulation by including clean examples during the training process. Note that robust optimization formulation suggests one to *only* optimize on the worst-case scenarios (see Section 6.1.5). The second difference is that Kannan et al. [183] include targeted adversarial examples during training, which also alters the inner maximization formulation. Finally, Engstrom et al. [184] also showed some loss surface visualizations of a model trained with ALP and pointed that the loss surface is “bumpier” compared to the loss surface of some baseline models and with small gradients around the starting point, which can be considered as a form of gradient masking.

6.1.16 Fortified Networks

While many denoising-based defense methods such as Defense-GAN [52] (see Section 6.1.12) and PixelDefend [53] (see Section 6.1.11) operate in the input space, Fortified Networks (FN) [185] is a denoising-based defense that operates in the hidden layers of a neural network. Lamb et al. [185] argued that one of the advantages of performing denoising in the hidden layers instead of the input space is to allow the use of simple generative transformation models such as the Denoising Autoencoders (DAE) [225] which have been previously shown to not work well as a defense mechanism when used in the input space [180]. This is motivated by the evidence that hidden representations of a neural network have simpler statistical properties compared to the features in input space [226].

FN applies one or more DAEs to the hidden layer of a neural network. Formally, we denote decoded representations at the l -th layer by

$$h_{decoded}^l = DAE^l(h^l + \eta), \quad (72)$$

where $\eta \sim \mathcal{N}(\mu, \sigma^2)$ denotes the Gaussian noise, and DAE^l denotes the DAE at the l -th layer. The DAEs are trained to minimize reconstruction error, or in other words

$$\mathcal{L}_{DAE} = \|DAE^l(h^l) - h^l\|_2, \quad (73)$$

where the weights for the encoder and decoder of each DAE are tied. In their experiments, Lamb et al. [185] combined FN with adversarial training (see Section 6.1.1). For the DAE, the target reconstruction for an adversarial example x' at layer l is the hidden representation of the clean input x at the same layer. Formally,

$$\mathcal{L}_{AdvDAE} = \|DAE^l(h_{adv}^l) - h^l\|_2, \quad (74)$$

where h_{adv}^l is the hidden representation at layer l when the input is an adversarial example. The objective function of FN is then:

$$\mathcal{L}_c + \lambda_1 \mathcal{L}_{DAE} + \lambda_2 \mathcal{L}_{AdvDAE}, \quad (75)$$

where \mathcal{L}_c denotes the classification loss function used by the network (e.g., cross-entropy) when dealing with both clean and adversarial inputs, while λ_1 and λ_2 are the weighting factors for the loss terms.

Lamb et al. [185] found that the use of multiple DAEs yields higher robustness and shows improvement compared to the PGD adversarial training [145] (see Section 6.1.5) and Thermometer Encoding [48] (see Section 6.1.10) against attacks like the FGSM [32] (see Section 4.2) and PGD [145] (see Section 6.1.5) when combined with adversarial training on MNIST and CIFAR10 models. They also showed that FN is more robust compared to DefenseGAN [52] (see Section 6.1.12) when tested against FGSM and PGD attacks on both MNIST and F-MNIST models.

6.1.17 Feature Denoising Block

Xie et al. [186] observed how adversarial perturbations cause large changes in the feature maps produced by a model compared to the original input. Motivated by this observation, they proposed a method to denoise the feature maps. This in fact is similar to the idea of fortified networks [185] (see Section 6.1.16).

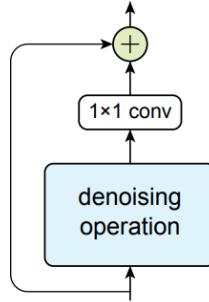


Figure 22: Illustration of the denoising block (taken from Xie et al. [186]).

In this work, the denoising is done by creating what they call a denoising block that can be placed at any levels in the network. Fig. 22 illustrates the denoising block. For the rest of this paper, we refer to this defense as the Feature Denoising Block, or in short, FDB. This block consists of a differentiable denoising operator, a 1×1 convolutional layer, and an identity skip connection. Xie et al. [186] evaluated various

denoising operators: non-local means [227], mean filtering, median filtering, and bilateral filtering [228]. Note that the use of denoising operator may not only remove adversarial perturbations, but also information relevant for classification task. However, Xie et al. [186] argued that the identity skip connection should help to maintain the useful information, while the 1×1 convolutional layer will learn to balance between preserving the useful information and removing adversarial perturbations.

Xie et al. [186] found non-local means denoiser as the best performing denoising operator when compared with other operators used in their experiments. The denoising block was also shown to not significantly sacrifice performances on non-adversarial inputs. Finally, they also showed that when combined with PGD adversarial training [145] (see Section 6.1.5), FDB achieved state of the art adversarial robustness performance in both whitebox and blackbox settings. This method was ranked first in the Competition on Adversarial Attacks and Defenses (CAAD) 2018 where it achieved 50.6% accuracy when evaluated against 48 different attacks.

6.1.18 Analysis by Synthesis

The idea of using generative models as a defense mechanism has previously been proposed. Methods like Defense-GAN [52] (see Section 6.1.12) and PixelDefend [53] (see Section 6.1.11) rely on generative models to learn the distribution of non-adversarial dataset with the goal of being able to project adversarial input to the learned non-adversarial manifold. However, instead of learning the input distribution for the whole dataset, Schott et al. [187] proposed a defense method called Analysis by Synthesis (ABS) that learns the distribution of the input for each class.

ABS uses VAE [86] to model the distribution of each class in a dataset, where one VAE is needed for each class. Given a dataset with C classes, during test time, one then needs to perform gradient descent to find the optimal latent variable that maximizes the lower bound of the log-likelihood for each class y . Formally, given decoder $p_\theta(x|z, y)$, we want to solve for

$$l_y^* = \max_z \log \left[p_\theta(x|z, y) \right] - D_{KL} \left[\mathcal{N}(z, \sigma_q \mathbf{1}) || \mathcal{N}(0, \mathbf{1}) \right]. \quad (76)$$

Concretely, Schott et al. [187] solve this optimization problem using Adam [136]. Once l^* for every class are found, the class probability can be calculated by

$$p(y|x) = \frac{e^{\alpha l_y^*(x)} + \eta}{\sum_{c=0}^{C-1} (e^{\alpha l_c^*(x)} + \eta)}, \quad (77)$$

where α is a scaling factor, and η is an offset term. Schott et al. [187] explained that the reason of adding η is to encourage the model to produce uniform distribution over classes in the case of unrecognizable images. In their implementation, η was chosen so that the median of the confidence on non-adversarial examples is 0.9. They also introduced an ABS variant called Binary ABS that can be used for grayscale image datasets (e.g., MNIST), which binarized the input image according to a certain threshold value.

ABS was shown to work fairly well and more robust than the PGD adversarial training [145] (see Section 6.1.5) when evaluated against L_0 and L_2 adversaries on MNIST. However, the robustness of ABS on L_∞ adversary seems to be very low. Although they demonstrated the robustness of Binary ABS on L_∞ adversaries, Binary ABS cannot be applied to non-grayscale images. It also seems challenging to scale ABS to large datasets that have many classes, since one needs to train multiple VAEs and perform gradient descent during inference for each class. These limitations were properly acknowledged by the authors, and further evaluations of this defense on larger datasets are still needed.

6.1.19 Web-Scale Nearest-Neighbor Search

Assuming adversarial perturbations push an image away from its manifold, Dubey et al. [188] developed a defense with the aim to project an adversarial image back to the true manifold via Web-Scale Nearest-Neighbor Search (WSNNS). The general idea of WSNNS is to find the K nearest neighbors of an input image

from a large database of images, and classifying these neighbors instead of the given input image. Note that the images in the database must be selected to match the task at hand, which can be obtained by looking at their labels, hashtags, or any other available indicators. One may see the similarity between WSNNS and quilting-based defense [54] (see Section 6.1.9). The difference is that while quilting-based defense operates at a patch-level, WSNSS operates at image-level.

Dubey et al. [188] found the K nearest neighbors according to the Euclidean distance in the feature space. In their work, they experimented with various outputs of a certain layer in deep neural networks which may be followed by pooling and dimensionality reduction method (e.g., PCA), as the features. Once the nearest neighbors are identified, all these images are classified where each prediction may be weighted differently. Various weighting strategies were proposed by Dubey et al. [188]. The first strategy is to assign the weights uniformly across predictions (UW strategy). Another strategy is to adjust the weights based on the entropy gap between the prediction and uniform prediction (CBW-E strategy). For CBW-E strategy, given the weights w and C number of classes, w can be computed by

$$w = \left| \log C + \sum_{c=1}^C s_c \log s_c \right|, \quad (78)$$

where s_c is the softmax probability of class c . Finally, the weights can also be computed based on the difference between the maximum value in a prediction and the next top M values (CBW-D strategy):

$$w = \sum_{m=2}^{M+1} (\hat{s}_1 - \hat{s}_m)^P, \quad (79)$$

where \hat{s}_m is the top m -th softmax value. In their experiments, M and P were set to be 20 and 3, respectively.

Dubey et al. [188] found that CBW-D strategy produces more robust defense compared to UW and CBW-E. Although increasing K generally leads to a more robust defense, they also found that the effect of increasing K saturates at a certain point, thus K can be experimentally adjusted depending on the database used and other parameters. They also discussed the tradeoffs between using features from earlier layers versus later layers of deep networks, where they found that using features from earlier layers generally results in higher robustness while using features from later layers produces higher accuracy but lower robustness. Finally, they showed that increasing number of images in the database leads to higher accuracy with a log-linear relation, and engineering the database to only include images that are related to the task at hand can significantly improve the performance. WSNSS was shown to be effective to defend against PGD adversaries in blackbox and graybox settings, where graybox was defined as the case when the adversarial examples was generated by targeting the same model using the substitute blackbox attack [41] (see Section 4.9).

This defense however is not effective to defend against whitebox attacks (i.e., if the attacker has information regarding the defense in place or the database used). Note that the neighbors are determined by the Euclidean distance in the feature space, which is not a robust metric to measure similarity between samples. Hence, the attacker may be able to find a perturbation that will cause an image that belongs to a certain class to be considered close to other images from different class. For example, perhaps AMDR [78] (see Section 4.6) can be used to attack this model. Another possibility is that an attacker may create a substitute database and aims to find an adversarial example that maximizes the sum of the differences between the features of the given image and the features of the images in the substitute database. Another option is for the attacker to maximize the prediction error of both the original input and images in the substitute database. Both variants of these attacks were proposed by Dubey et al. [188] as the nearest-neighbor feature-space attack and nearest-neighbor prediction attack, respectively. Finally, this defense may also exhibit the weaknesses of K nearest neighbors algorithm which it relies heavily on.

6.1.20 ME-Net

Yang et al. [189] proposed a preprocessing-based defense called ME-Net that preprocesses an input with the hope of destroying the structure of adversarial noise. ME-Net works by first dropping pixels in an input image

randomly according to some probability p , which is hypothesized to destroy the adversarial perturbations. The image is then reconstructed using Matrix Estimation (ME) algorithms, which is a family of methods to recover data of a matrix from its noisy observation.

Fig. 23 illustrates the training and inference mechanics of ME-Net. Given a training dataset of images, each image is masked n -times to produce n images according to a set of masking probabilities $\mathbf{p} = \{p_1, p_2, \dots, p_n\}$, where $1 - p_i$ is the probability of each pixel to be set to zero, and \mathbf{p} is initialized randomly. Next, each of the masked images is reconstructed using an ME algorithm. All these preprocessed images are then gathered to form a new dataset for the model to be trained on. As for the inference, given an image, the image is first masked based on the average of the masking probabilities used during training (i.e., $p = \frac{1}{n} \sum_{i=1}^n p_i$) before being preprocessed using an ME algorithm. The preprocessed image is then passed to the classifier to be classified.

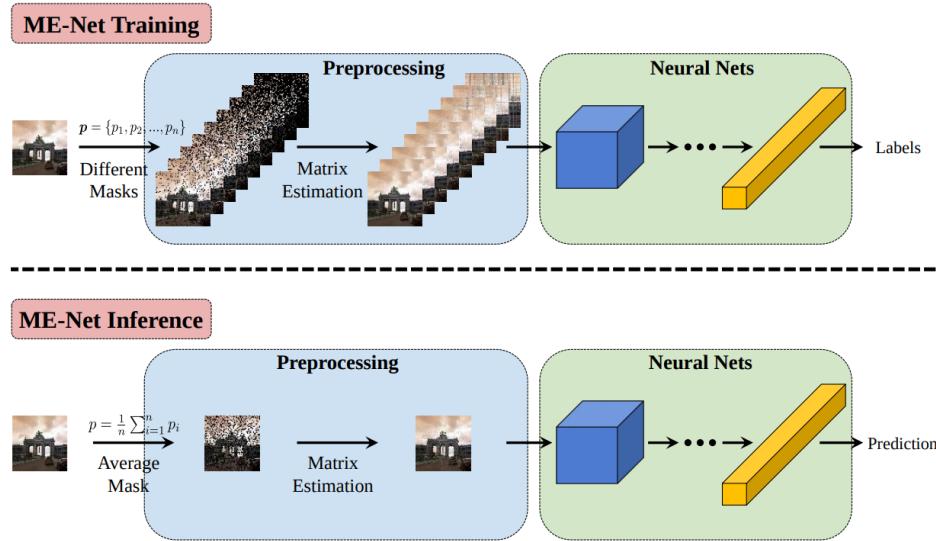


Figure 23: Illustration of ME-Net (taken from Yang et al. [189]).

In their experiments, Yang et al. [189] considered Nuclear Norm Minimization [229], Soft-Impute [230], and Universal Singular Value Thresholding (USVT) [231] as the ME algorithms. They also chose to use 10 masks. When comparing the three ME algorithms, they found that the robustness provided by these algorithms to be comparable. Thus, they suggested to use USVT due to its efficiency compared to the other ME algorithms.

ME-Net was shown to be robust when tested against various L_∞ attacks in both blackbox and whitebox settings on CIFAR-10, MNIST, SVHN, and Tiny-ImageNet. In the case of blackbox attack, ME-Net was evaluated against various variants of the substitute blackbox attack [41] (see Section 4.9) (CW-SBA [44], FGSM-SBA [32], PGD-SBA [145]), Boundary Attack [94] (see Section 4.22), and SPSA [97] (see Section 4.27), where the model successfully maintained its $\sim 90\%$ accuracy on CIFAR10 under all these threats. In whitebox settings, ME-Net successfully defends itself against PGD-based BPDA [55] (see Section 4.26). Note that the evaluation of ME-Net against BPDA is appropriate considering the non-differentiable nature of the preprocessing pipeline. It will be interesting to also evaluate the robustness of the model against the combination of BPDA and expectation over randomness, as this has been shown to successfully circumvent various preprocessing-based defenses. Finally, Yang et al. [189] showed that ME-Net can be combined with adversarial training which further enhances the robustness of the model.

6.2 Detecting Adversarial Attacks

Instead of trying to classify adversarial examples correctly, several works have shown progress in the detection of adversarial examples. A sample can then be rejected if it was detected as an adversarial example. In this section, we cover several adversarial detection methods.

6.2.1 Early Methods: PCA, Softmax, and Reconstruction of Adversarial Images

Hendrycks and Gimpel [190, 191] investigated three methods to perform adversarial detection. Broadly speaking, these methods capitalize upon empirical differences between clean and perturbed inputs, and are all vulnerable to attacks which specifically aim to circumvent them. Together, we refer to these as H & G detection methods.

The first method proposed is to analyze the variance of coefficients of PCA whitened input. Hendrycks and Gimpel [190] found that the later principal components of adversarial images usually have larger variance than those of clean inputs, and thus can be used as an indication to perform threshold based detection. They showed that this method can be used to detect FGSM [32] (see Section 4.2) and BIM [45, 77] (see Section 4.3) adversaries on MNIST, CIFAR10, and Tiny-ImageNet when the attacker is not aware of the defense in place.

However, Carlini and Wagner [232] found that this method can be bypassed if the attacker is aware of the defense strategy, allowing them to constrain the variance of later principal components during adversarial examples generation process. For example, this can be achieved using C&W attack [44] (see Section 4.11) by folding the constraint to the objective function. Furthermore, Carlini and Wagner [232] argued that the reason this method works on MNIST may be due to the certain artifacts that exist in the dataset. For example, the pixel values that are not part of the digit have zero values in a clean image, while pixel values that are not part of the digit in an adversarial image usually no longer have zero values due to the modification to the image. Carlini and Wagner [232] then evaluated this method on CIFAR10 and found that this method is not as effective as when evaluated on MNIST.

Second, Hendrycks and Gimpel [190, 191] suggested that the softmax distribution between clean and adversarial inputs are different, and thus can be analyzed to perform adversarial detection. This can be done by measuring the Kullback-Leibler divergence [127] between uniform distribution and the softmax distribution, then perform threshold-based detection on it. They found that the softmax distribution of normal examples are usually further away from uniform distribution compared to adversarial examples since a model tends to predict an input with a high confidence, at least for adversaries generated by attack methods that do not care about the output distribution as long as the generated adversaries are misclassified.

This method seems to only applicable to specific attacks that stop as soon as an input becomes adversarial such as the JSMA [80] (see Section 4.8), which may be predicted by the model with a low confidence score. Furthermore, evaluation on ImageNet models is needed (and to date, incomplete) since the softmax probability on ImageNet dataset usually is less confident due to the large number of classes. It is also not clear whether or not this strategy will work against adversarial attacks that also target specific confidence score such as the C&W attack [44] (see Section 4.11).

Finally, Hendrycks and Gimpel [190, 191] proposed that adversarial examples can be detected by analyzing the input reconstructions obtained by adding an auxiliary decoder [233] to the classifier model that takes the logits as an input to reconstruct the image. The decoder and classifier are jointly trained only on clean examples. The detection can be done by creating a detector network which takes the input reconstruction, logits, and confidence score as inputs, and outputs a probability of an input being adversarial or not, where the detector network is trained on both clean and adversarial examples. Hendrycks and Gimpel [190] evaluated this method on MNIST model and showed that this method is able to detect adversarial examples generated by FGSM and BIM. They showed qualitatively how reconstruction of adversarial examples are noisier compared to normal inputs, allowing one to compute the differences as a way to detect adversarial examples.

This defense method however is fully differentiable, and an attacker may still be able to find adversarial examples that fool both the classifier and detector networks in whitebox setting. Although this method needs to be evaluated more extensively on different datasets and attack settings, the use of input reconstruction

that is conditioned on the classification seems to be an interesting research direction that can be used to detect both misclassification and adversarial examples.

Hendrycks and Gimpel [190] did admit that these methods are not perfect, and may be circumventable, and in fact have successfully been circumvented. They then suggested that future detection methods should include combination of different detection methods. Indeed, some of the detection methods that we cover in this paper use combination of different strategies to enhance adversarial detection performance.

6.2.2 Adversary Detector Networks

Metzen et al. [192] proposed augmenting a pretrained neural network with a binary detector network. The detector network D is a binary classifier network that is trained to differentiate between real and adversarial examples. It takes the output of the classifier network at a certain layer as an input and outputs the probability of an input being adversarial (i.e., $D(f_l(x)) = y_{adv}$ or y_{clean} , where $f_l(x)$ denotes the output of classifier f at the l -th layer).

The training of the detector network involves generating adversarial examples to be part of the training set for the detector network. In order to account for future attacks with the assumption that attacker have access to both the classifier and detector networks, Metzen et al. [192] generated examples which specifically attempted to fool the detector. They generated adversarial examples according to

$$x'_{i+1} = Clip_\epsilon \left\{ x'_i + \alpha \left[(1 - \sigma) \cdot \text{sign}(\nabla_x \mathcal{L}_{\text{classifier}}(x'_i, y)) + \sigma \cdot \text{sign}(\nabla_x \mathcal{L}_{\text{detector}}(x'_i, y_{adv})) \right] \right\}, \quad (80)$$

where $x'_0 = x$, and σ denotes the weight factor that controls whether the attacker's objective is to attack the classifier or the detector, chosen randomly at every iteration. The training procedure used by Metzen et al. [192] followed that of adversarial training [32] (see Section 6.1.1).

This method was found to be effective against FGSM [32] (see Section 4.2), DeepFool [79] (see Section 4.7), and BIM [45, 77] (see Section 4.3) when evaluated on CIFAR10 and 10-class Imagenet (i.e., a subset of ImageNet dataset that only contains 10 classes). They also found that placing the detector network at different layer depths gives different results for different types of attacks. Finally, Metzen et al. [192] noted that fooling a classifier that includes a detector network is harder than an unprotected classifier, since an attacker needs to find adversaries that fool *both* the classifier and detector.

However, Carlini and Wagner [232] found that this method has relatively high false positive rate against stronger attacks like the C&W attacks [44] (see Section 4.11), and can be circumvented with SBA [41] (see Section 4.9). Furthermore, although Metzen et al. [192] claimed that they did not have to perform extensive tuning to train the detector, Carlini and Wagner [232] found the opposite.

Gong et al. [193] proposed a similar method to Metzen et al. [192] by training a binary classifier network to differentiate between adversarial and clean examples. However, the binary classifier here is a completely separate network from the main classifier. Rather than generating adversarial examples against the detector, they generate adversarial examples for a pretrained classifier, and add these adversarial examples to the original training data to train the binary classifier.

Although the method is relatively simple to implement, Gong et al. [193] observed several limitations on the generalization of this method. First, they found that the detector network is sensitive to the ϵ value used to generate FGSM and BIM adversaries, in the sense that detector trained on adversarial examples with ϵ_1 cannot detect adversarial examples with ϵ_2 , especially when $\epsilon_2 < \epsilon_1$. They also discovered that training a detector on a single type of adversaries is not guaranteed to generalize to other types of adversaries. For example, a detector trained on FGSM adversaries was found to not be able to detect JSMA adversaries. Furthermore, Carlini and Wagner [232] found that this method has high false positive rates when tested on CIFAR10 models, and is vulnerable to C&W attacks.

Another similar method by Grosse et al. [194] is a detection method that works by augmenting a classifier network with an additional class node that represents adversarial class. Given a pretrained model, a new model with an extra class node is trained on clean examples and adversarial examples generated for the pretrained model.

Grosse et al. [194] showed how this method can be used to detect adversaries generated by FGSM [32] (see Section 4.2) and JSMA [80] (see Section 4.8) on MNIST. They also showed how this method can reliably detect SBA [41] (see Section 4.9), particularly FGSM-SBA and JSMA-SBA. Although the method was shown to work on MNIST [116], Carlini and Wagner [232] showed that this method does not work well on more complex datasets such as CIFAR10 as the false positive rate was too high. Furthermore, Carlini and Wagner [232] also found that this method is vulnerable to the C&W attacks in both whitebox and blackbox settings (i.e., C&W-SBA).

Concurrent work from Hosseini et al. [195] proposed a very similar method with slight difference in the detail of the training procedure where the classifier is alternatively trained on clean and adversarial examples (i.e., via adversarial training [32]) (see Section 6.1.1). Furthermore, the labels used for training the model are carefully assigned by performing label smoothing [111]. Label smoothing sets a probability value to the correct class and distributes the rest uniformly to the other classes.

Having a slightly different goal than Grosse et al. [194], Hosseini et al. [195] evaluated their method in the blackbox settings and showed how their method is especially helpful to reduce the transferability rate of adversarial examples. Although the detection method proposed by Hosseini et al. [195] was not evaluated by Carlini and Wagner [232], the method appears to be similar with the method proposed by Grosse et al. [194]. Since the evaluation of this method was only done on MNIST and grayscaled GTSRB [121], it is questionable where or not this method will also exhibit high false positive rate when tested on CIFAR10 or other datasets with higher complexity. Finally, this method needs to be evaluated against the C&W attacks, considering the findings in Carlini and Wagner [232] that shows how C&W attacks can be used to circumvent the detection method proposed in Grosse et al. [194].

6.2.3 Kernel Density and Bayesian Uncertainty Estimates

Assuming that adversarial examples do not lie inside the non-adversarial data manifold, Feinman et al. [196] proposed two methods to perform adversarial detection: Kernel Density and Bayesian Uncertainty Estimates. The objective for using Kernel Density Estimates (KDE) is to identify whether a data point is far from a class manifold, while Bayesian Uncertainty Estimates (BUE) can be used to detect data points that are near the low-confidence region in which KDE is not effective.

The density estimate KDE for an input x is calculated by

$$KDE(x) = \frac{1}{|X_t|} \sum_{x_i \in X_t} e^{-\frac{\|Z(x) - Z(x_i)\|^2}{\sigma^2}}, \quad (81)$$

where $Z(x)$ denotes the logits vector given x as the input, X_t is a set of data of class t , and σ is the kernel bandwidth. Note that the kernel function used is the Gaussian kernel and evaluated in the logits space instead of the input space. The use of the logits is inspired from the work by Bengio et al. [226] and Gardner et al. [234], which showed how the manifold learned by the network becomes increasingly linear and flatter which makes the logit space easier to work with than the input space. An adversarial example x' will have low KDE value if x' is far from the target class manifold, and thus can be detected using threshold based approach. In other words, x is considered adversarial if $KDE(x)$ is less than a certain threshold value. However, Feinman et al. [196] suggested that this method does not work well when x' is near the target class manifold.

Feinman et al. [196] followed the work from Gal and Ghahramani [235] by using dropout [212] at inference time as a way to measure uncertainty. They quantify the uncertainty $U(x)$ of the network by performing N stochastic passes by applying dropout during inference. Formally, $U(x)$ is defined as:

$$U(x) = \frac{1}{N} \sum_{i=1}^N f(x)_i^T f(x)_i - \left(\frac{1}{N} \sum_{i=1}^N f(x)_i \right)^T \left(\frac{1}{N} \sum_{i=1}^N f(x)_i \right), \quad (82)$$

where $f(x)_i$ denotes the i -th stochastic prediction. Intuitively, the uncertainty measure should be large when dealing with adversarial inputs.

Feinman et al. [196] showed how the uncertainty distributions are different between adversarial and normal examples. This was indicated by the ratio $\frac{U(x')}{U(x)}$ that is larger than 1 in most cases when evaluated on MNIST and CIFAR10 against FGSM [32] (see Section 4.2), BIM [45, 77] (see Section 4.3), JSMA [80] (see Section 4.8), and C&W [44] (see Section 4.11) attacks. KDE was also shown to be able to detect adversaries, but especially indicative when evaluated against a variant of BIM that stops the attack process following a fixed number of iterations. This is indicated by the ratio $\frac{KDE(x')}{KDE(x)}$ that are less than 1 in most cases.

Based on these findings, the authors proposed a combined threshold based detection method, using both metrics to perform adversarial detection. This is done by putting threshold values on the uncertainty measurement and on the negative log of the kernel density estimates of a sample. The combined method was shown to be superior against FGSM, BIM, JSMA, and C&W on MNIST, CIFAR10, and SVHN.

Carlini and Wagner [232] evaluated this method and concluded that the KDE method alone does not work well on CIFAR10 and can be circumvented with modified C&W attacks by including an additional objective term defined by $\max(-\log(KDE(x')) - \epsilon, 0)$ both in whitebox and blackbox settings using SBA [41] (see Section 4.9). They also showed that BUE can be circumvented by C&W attacks on the expectations of different models sampled during dropout. However, they noted that the distortions required to generate adversarial examples that fool BUE are also larger compared to other detection methods that they evaluated. As a result, Carlini and Wagner [232] concluded that BUE was the hardest detection method to fool compared to the other methods. It is also relatively straightforward to implement as an add-on to an existing network architecture.

6.2.4 Feature Squeezing

Xu et al. [197] argued that the dimensionality of input features is often unnecessarily large, yielding a large attack surface. They proposed a detection strategy in which they compare the predictions between squeezed and unsqueezed inputs. As the name suggests, the goal of feature squeezing is to remove unnecessary features from an input. Two feature squeezing methods were evaluated: color bit-depth reduction and spatial smoothing, both with local and non-local smoothing. The input is labelled as adversarial if the L_1 difference between the model's prediction on squeezed and unsqueezed inputs is larger than a certain threshold value T . Note that this method is independent of the defended model, and thus can be used together with other defense techniques. Figure 24 illustrates this method.

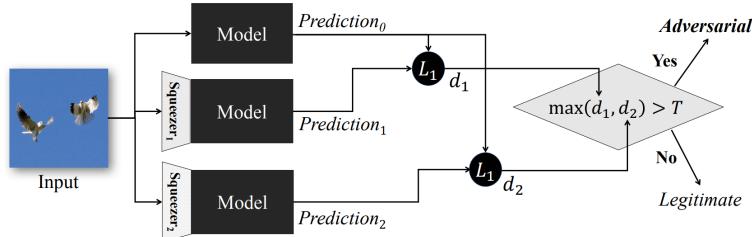


Figure 24: Illustration of feature squeezing (taken from Xu et al. [197]).

For color depth reduction, Xu et al. [197] experimented with various i -bit depth where $1 \leq i \leq 8$. For local smoothing, median filtering was found to be more effective than Gaussian and mean smoothing. In the case of non-local smoothing, non-local means denoising [236] was used. There is no strong motivation for this choice of squeezers; future work on the most effective squeezers is still needed. They also suggested using multiple feature squeezing methods as part of the detection model, since different squeezers are more effective on certain types of adversaries than others. Given n squeezers $\{s_1, \dots, s_n\}$, the output of the detector is defined as

$$Detector(x) = \begin{cases} \text{Adversarial} & \text{if } \max(|f(x) - f(s_1(x))|_1, \dots, |f(x) - f(s_n(x))|_1) > T \\ \text{Benign} & \text{otherwise} \end{cases}, \quad (83)$$

where $f(x)$ is the output vector given by the softmax layer of a deep neural network.

Xu et al. [197] demonstrated that feature squeezing can also be used to increase adversarial robustness. This is similar to the work from Chuan Guo [54] which also attempted to enhance adversarial robustness through various input transformations (see Section 6.1.9). Furthermore, Xu et al. [197] showed that the robustness can be improved by coupling feature squeezing with adversarial training [32] (see Section 6.1.1). However, they acknowledged that feature squeezing alone is not a reliable defense, and thus focus on adversarial detection instead.

Feature squeezing was shown to be able to detect adversarial examples generated by FGSM [32] (see Section 4.2), BIM [45, 77] (see Section 4.3), DeepFool [79] (see Section 4.7), JSMA [80] (see Section 4.8), and C&W [44] (see Section 4.11) attacks on MNIST, CIFAR10, and ImageNet models when the attacker is not aware of the defense strategy used. To be more specific, Xu et al. [197] found that color depth reduction is especially effective against L_2 and L_∞ attacks, but less effective against L_0 attacks. On the other hand, spatial smoothing method was found to be effective against L_0 attack. Intuitively, L_0 attacks cause perturbations that can be thought of as salt-and-pepper noise, in which median filtering has often been used to remove this type of noise. These findings support the need of using joint squeezers configuration to take into account different types of adversarial examples.

Xu et al. [197] also considered a case where the attacker is aware of the detection method. In this setting, the adversary needs to find adversarial examples that fool the classifier and minimize the difference in L_1 score between squeezed and unsqueezed inputs. The defense can then be circumvented by iterative optimization based attacks, such as C&W attacks, by folding in the L_1 constraint. As a result, they suggested to introduce randomness, for example by randomizing the threshold value such that $T' = T \pm \text{rand}(0.1)$, in order to make it harder for the attacker to predict the behavior of the squeezers. Although feature squeezing method is powerful against static adversaries, Xu et al. [197] acknowledged that this method is possibly not immune to adversarial examples in situation where an attacker has full knowledge of the squeezers.

6.2.5 Reverse Cross-Entropy

Pang et al. [198] proposed a detection method by introducing a new objective function called the Reverse Cross-Entropy (RCE). For C classes, RCE loss is defined as

$$\mathcal{L}_{RCE} = -y_r \log f(x), \quad (84)$$

where y_r is the reversed label defined as

$$y_{r(i)} = \begin{cases} 0 & \text{if } i = y \text{ (true label)} \\ \frac{1}{C-1} & \text{otherwise} \end{cases}. \quad (85)$$

They noted that training a model to minimize \mathcal{L}_{RCE} produces a reverse classifier where the probability assigned to the correct class will be the lowest. Thus, Pang et al. [198] suggested to negate the logits such that $f(x) = \text{softmax}(-Z(x))$.

Once the model is trained, one may perform adversarial detection using threshold based detection. Pang et al. [198] performed the detection by computing the Kernel Density Estimate (KDE) [196] (see Section 6.2.3). They also introduced a new metric called the non-maximum element or non-ME defined as

$$\text{non-ME}(x) = - \sum_{i \neq \hat{y}} \hat{f}(x)_i \log(\hat{f}(x)_i), \quad (86)$$

where $\hat{f}(x)_i$ denotes the normalized non-maximum elements in $f(x)$. The detection is performed by setting a threshold value T . If the chosen metric (e.g., KDE or non-ME) is below the threshold value, the input is considered as adversarial. However, Pang et al. [198] found that detection using KDE outperforms non-ME in most cases.

This method was shown to be reliable when evaluated on MNIST and CIFAR10 datasets against FGSM [32] (see Section 4.2), BIM/ILLCM [45, 77] (see Section 4.3), JSMA [80] (see Section 4.8), C&W [44] (see Section 4.11), and modified C&W that takes into account the use of KDE; we refer this as MCW. Furthermore,

this method was also evaluated in blackbox settings against MCW-SBA [41] (see Section 4.9) and showed how the adversarial examples generated by SBA suffer from poor transferability. Even when adversarial examples that fool both detector and classifier models were found, the adversarial examples usually exhibit larger distortions and thus are visually visible to human.

Finally, the use of RCE not only allows one to perform adversarial detection, but also increases robustness of a model in general compared to the use of standard cross-entropy as the objective function. They also showed the comparison of t-SNE embeddings between a model trained with RCE and non-RCE objectives, and showed how the t-SNE [237] visualization of the model that was trained with RCE objective achieved higher separability. The use of new objective functions such as RCE which constrains the ability of attacker to generate adversarial examples seems to be an interesting research area to be explored.

7 Transferability of Adversarial Examples

7.1 What is transferability?

Transferability is a phenomenon where adversarial examples or perturbations generated to fool a particular model can be used to fool others. Many machine learning models, including deep networks, are subject to this phenomenon [31, 41, 67]. Transferability can be carved into several different categories: (1) transferability between different models (e.g., between VGG16 [122] and ResNet [6] in the case of deep neural networks) trained on the same dataset or different subsets of the same dataset, (2) transferability between different machine learning techniques (e.g., between SVMs and deep neural networks), and (3) transferability between models that perform different tasks (e.g., between semantic image segmentation and object detection models [88]). Understanding the transferability phenomenon is critical to creating safer machine learning models. Several adversarial attacks like the SBA [41] (see Section 4.9) work by exploiting this phenomenon. In fact, the transferability property has also been exploited to enable adversarial attacks on real world image classification [41, 67] and detection [99] systems.

7.2 Where does transferability come from?

Goodfellow et al. [32] suggested that the reason why adversarial examples can fool deep neural networks is due to the linearity behavior when using activation functions like the Rectified Linear Units (ReLU) [69] or Maxout [70]. Based on this view, Goodfellow et al. [32] argued that adversarial examples exist in the “contiguous regions of the 1-D subspace defined by the fast gradient sign method” which was contrary to the belief that adversarial examples lie in the low probability regions in the data manifold [31]. This view suggests that there exist many adversarial examples which have higher chance to be transferable because different models will end up learning similar functions, and that the direction of perturbations is the key factor that allows transferable adversarial examples.

Tramèr et al. [238] studied the subspace dimensionality of adversarial examples and asked if there is an intersection between the adversarial subspace of two different models. They introduced a technique called Gradient Aligned Adversarial Subspace (GAAS) to estimate the number of orthogonal adversarial directions. They found that there were many orthogonal adversarial directions, a large percentage of which were transferable. Furthermore, they found that the separating distance between the decision boundaries of two models was on average smaller than the distances between any inputs to the decision boundaries, even on adversarially trained models. This finding suggests that the adversarial subspaces of different models overlap, which is in agreement with the findings from Liu et al. [68], explaining why many adversarial examples are transferable between models.

Tsipras et al. [207] investigated the property of robust classifier and found that robust classifiers tend to only take advantage of robust features (i.e., features that have high correlation with the ground truth label), as opposed to weak features (i.e., features that have low correlation with the ground truth label) during training. Based on this, Tsipras et al. [207] argue that classifiers that rely on weak features will suffer from the same adversarial examples that were created by perturbing these features. This hypothesis was also reinforced by Ilyas et al. [76] that shows how different models tend to exploit similar *non-robust features* in a dataset, and thus adversaries generated for one model can be transferred to the other models.

7.3 What affects transferability?

There are several dimensions that appear to affect transferability. Firstly, model type in turn influences the type of transferability observed. Papernot et al. [67] found empirically that deep neural networks and kNN are more robust to cross-technique transferability, but more vulnerable to intra-technique transferability. On the other hand, linear regression, SVM, decision trees, and ensemble methods are more robust to intra-technique transferability, but more vulnerable to cross-technique transferability.

Secondly, attack strength matters. Kurakin et al. [45] found that stronger adversarial examples that can penetrate through a robustly defended model are less transferable to other models, while adversarial exam-

ples generated to attack undefended model are more transferable. They argued that adversarial examples generated to penetrate specific defense method may have “overfitted” to fool that particular model. Kurakin et al. [45] also found that larger magnitude perturbations often increases the transferability rate.

Thirdly, non-targeted attacks transfer better than targeted ones. Liu et al. [68] investigated the transferability property on large scale datasets like ImageNet and found that transferable non-targeted adversarial examples are easier to find than targeted ones. They further showed that decision boundaries of different models align with each other, hinting why adversarial examples are transferable. They found that the direction of the gradient of the loss function with respect to the input of two different models are orthogonal, and thus that fast gradient based approaches are unlikely to find targeted adversarial examples that transfer. To overcome this, they perform ensemble adversarial attack, successfully generating targeted adversaries that fool several different models.

8 Conclusion and Future Work

We have seen various ways to generate adversarial examples in both whitebox and blackbox settings. While whitebox attack is especially important for evaluating new defenses in the worst-case scenario, works in blackbox attack are as important since they involve more realistic threat model that may happen in the real world. We also discussed several methods to defend against adversarial examples either by trying to robustify a model, or identifying adversarial samples so they can be rejected. However, the majority of these defenses boil down to some form of gradient masking; hiding or disrupting the gradients available to an attacker. The work from Athalye et al. [55] dramatically demonstrated the fragility of such approaches. One of the interesting directions to explore is to investigate the effectiveness of Bayesian inference as an adversarial defense method. It may also be interesting to explore other existing algorithms to perform both adversarial attack and defense. For example, one may further explore the applications of reinforcement learning, meta-learning, and genetic algorithms in the field of adversarial machine learning.

Recent work aiming to improve resistance to adversarial attacks resulted in more generally robust models, which learned features that were immediately intuitive to human users [207, 209, 239]. Ilyas et al. [76] showed how machine learning models can be trained to be robust by just relying on some *robust features*, while models that are trained on *non-robust features* are highly vulnerable to adversarial examples. On somewhat similar notes, Geirhos et al. [240] found that convolutional neural nets are biased towards textures, and how increasing the bias towards shape may improve the robustness of the model. A follow up work by Zhang and Zhu [241] further showed that adversarially trained model is less biased towards textures and more towards shapes or edges. This emphasizes the fruitfulness of asking why machine learning models fail, and exploring those failure modes.

Although there have been many different defense strategies proposed, many of these defense methods have been found to be vulnerable to specific type of attacks, and raises a concern on whether these defenses were evaluated unfairly [55, 97, 202, 232] which may have led to false robustness. Gradient masking and obfuscated gradients seems to be phenomenons that many defense methods often rely, *intentionally or not*. Athalye et al. [55] suggested several tips to identify gradient masking: 1) if single step attacks perform better than iterative attacks, 2) if blackbox attacks perform better than whitebox attacks, 3) if unbounded perturbations do not reach 100% attack success rate, and 4) if random sampling successfully finds adversarial examples while gradient based attacks do not.

We have seen the difficulty of correctly evaluating robustness of defense methods. New defenses not only need to be evaluated against existing strongest adversaries, but also need to be evaluated on adaptive attacks (i.e., evaluated with the assumption that an attacker is aware of the defense strategy used and will seek to overcome it). For example, if the defense strategy aims to perform non-differentiable operation or gradient minimization, then the defense needs to be evaluated against attacks that do not rely on calculating the exact gradient such as BPDA [55] (see Section 4.26) or SPSA [97] (see Section 4.27). Defenses also need to be evaluated against multiple types of adversaries (e.g., L_∞ , L_0 , and L_2 and other types of adversaries) as defense such as adversarial training have been shown to only be robust against certain types of adversaries [47, 187, 210, 211]. Furthermore, the vast majority of defenses are limited to empirical evaluations and do not offer robustness guarantee to unknown attacks. A future direction is to investigate properties that can theoretically guarantee robustness to adversarial attacks, similar to the WRM [182] (see Section 6.1.13), coupled with empirical evaluations. It is important to note that these methods typically offer guarantee robustness only when the difference between the input and its adversarial counterpart is small under a certain metric. However, our understanding in perceptual similarity metric is still very limited. Common perceptual similarity metric such as the mean squared error is definitely not an ideal one [151]. As we discussed in Section 4.24, attacks like stAdv [95] may still be able to penetrate through defenses that focus only on defending against L_p adversaries. Carlini et al. [242] discuss about how to evaluate robustness and some common pitfalls in robustness evaluation in more detail, thus we refer readers to their work for a more comprehensive discussion.

We also discussed about the transferability property, where adversarial examples can be transferred between different machine learning models, different machine learning techniques, and different tasks. In the case of neural networks, future research that evaluates the relation between memorization of deep networks

and transferability property will be interesting. Understanding this phenomena may lead us to better understand the inner workings of existing machine learning models.

As machine learning exerts a greater influence in the real world, so to will adversarial attacks. With an increasing number of commercial machine learning systems, such as face recognition systems, autonomous driving, and medical imaging comes an increasing vulnerability to malevolent actors. Whilst many defense strategies have been proposed, most of the existing defenses focus on imperceptible perturbations. As discussed in Section 5, some of the physically realizable attacks are in the form of visible but inconspicuous perturbations. To the best of our knowledge, there are no defense strategies that combat these types of adversaries as yet. Future works on methods to generate physically realizable adversaries and how to defend against them are thus needed. Moving forward, as training on simulated data becoming popular, a fully differentiable renderer that produces realistic looking images similar to the work done by Liu et al. [243], can be an excellent tool to evaluate the robustness of a model.

Finally, we want to re-emphasize that this paper focuses mainly on the topic of adversarial examples in the computer vision domain. Adversarial examples already exist in other domains such as in computer security [56], speech recognition [57, 58, 59], and text [60]. Continuing in these endeavors are important for the safety of machine learning implementations. We leave these as future works.

References

- [1] 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.
- [2] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A. C. Berg, and L. Fei-Fei, “ImageNet Large Scale Visual Recognition Challenge,” *International Journal of Computer Vision (IJCV)*, vol. 115, no. 3, pp. 211–252, 2015.
- [3] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in *Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1*, ser. NIPS’12. USA: Curran Associates Inc., 2012, pp. 1097–1105. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2999134.2999257>
- [4] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, pp. 436 EP –, May 2015. [Online]. Available: <http://dx.doi.org/10.1038/nature14539>
- [5] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016, <http://www.deeplearningbook.org>.
- [6] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 770–778, 2016.
- [7] G. Huang, Z. Liu, and K. Q. Weinberger, “Densely connected convolutional networks,” *CoRR*, vol. abs/1608.06993, 2016. [Online]. Available: <http://arxiv.org/abs/1608.06993>
- [8] E. Shelhamer, J. Long, and T. Darrell, “Fully convolutional networks for semantic segmentation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 4, pp. 640–651, Apr. 2017. [Online]. Available: <https://doi.org/10.1109/TPAMI.2016.2572683>
- [9] K. He, G. Gkioxari, P. Dollár, and R. Girshick, “Mask R-CNN,” in *Proceedings of the International Conference on Computer Vision (ICCV)*, 2017.
- [10] D. Held, S. Thrun, and S. Savarese, “Learning to track at 100 fps with deep regression networks,” in *European Conference Computer Vision (ECCV)*, 2016.
- [11] L. Bertinetto, J. Valmadre, J. F. Henriques, A. Vedaldi, and P. H. S. Torr, “Fully-convolutional siamese networks for object tracking,” in *ECCV 2016 Workshops*, 2016, pp. 850–865.
- [12] J. Valmadre, L. Bertinetto, J. Henriques, A. Vedaldi, and P. H. S. Torr, “End-to-end representation learning for correlation filter based tracking,” in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, July 2017.
- [13] R. Girshick, J. Donahue, T. Darrell, and J. Malik, “Rich feature hierarchies for accurate object detection and semantic segmentation,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2014.
- [14] R. Girshick, “Fast R-CNN,” in *Proceedings of the International Conference on Computer Vision (ICCV)*, 2015.
- [15] S. Ren, K. He, R. Girshick, and J. Sun, “Faster r-cnn: Towards real-time object detection with region proposal networks,” in *Advances in Neural Information Processing Systems 28*, C. Cortes, N. D. Lawrence, D. D. Lee, M. Sugiyama, and R. Garnett, Eds. Curran Associates, Inc., 2015, pp. 91–99. [Online]. Available: <http://papers.nips.cc/paper/5638-faster-r-cnn-towards-real-time-object-detection-with-region-proposal-networks.pdf>

- [16] A. Graves, A. r. Mohamed, and G. Hinton, “Speech recognition with deep recurrent neural networks,” in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2013, pp. 6645–6649.
- [17] A. Graves and N. Jaitly, “Towards end-to-end speech recognition with recurrent neural networks,” in *Proceedings of the 31st International Conference on International Conference on Machine Learning - Volume 32*, ser. ICML’14. JMLR.org, 2014, pp. II–1764–II–1772. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3044805.3045089>
- [18] Y. Zhang, M. Pezeshki, P. Brakel, S. Zhang, C. Laurent, Y. Bengio, and A. Courville, “Towards end-to-end speech recognition with deep convolutional neural networks,” in *Interspeech 2016*, 2016, pp. 410–414. [Online]. Available: <http://dx.doi.org/10.21437/Interspeech.2016-1446>
- [19] I. Sutskever, O. Vinyals, and Q. V. Le, “Sequence to sequence learning with neural networks,” in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2*, ser. NIPS’14. Cambridge, MA, USA: MIT Press, 2014, pp. 3104–3112. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2969033.2969173>
- [20] J. Gehring, M. Auli, D. Grangier, D. Yarats, and Y. N. Dauphin, “Convolutional sequence to sequence learning,” *CoRR*, vol. abs/1705.03122, 2017. [Online]. Available: <http://arxiv.org/abs/1705.03122>
- [21] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. u. Kaiser, and I. Polosukhin, “Attention is all you need,” in *Advances in Neural Information Processing Systems 30*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds. Curran Associates, Inc., 2017, pp. 5998–6008. [Online]. Available: <http://papers.nips.cc/paper/7181-attention-is-all-you-need.pdf>
- [22] D. Amodei, C. Olah, J. Steinhardt, P. F. Christiano, J. Schulman, and D. Mané, “Concrete problems in AI safety,” *CoRR*, vol. abs/1606.06565, 2016. [Online]. Available: <http://arxiv.org/abs/1606.06565>
- [23] R. McCauley and J. Henrich, “Susceptibility to the muller-lyer illusion, theory-neutral observation, and the diachronic penetrability of the visual input system,” *Philosophical Psychology*, vol. 19, no. 1, pp. 79–101, 2006.
- [24] A. Ahluwalia, “An intra-cultural investigation of susceptibility to ‘perspective’ and ‘non-perspective’ spatial illusions,” *British Journal of Psychology*, vol. 69, no. 2, pp. 233–241, 1978. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.2044-8295.1978.tb01653.x>
- [25] D. Brainard and A. Hurlbert, “Colour vision: Understanding #thedress,” *Current Biology*, vol. 25, no. 13, pp. R551 – R554, 2015. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0960982215005941>
- [26] D. M. Eagleman, “Visual illusions and neurobiology,” *Nature Reviews Neuroscience*, vol. 2, pp. 920–926, 2001.
- [27] C. Blakemore and F. W. Campbell, “On the existence of neurones in the human visual system selectively sensitive to the orientation and size of retinal images,” *The Journal of Physiology*, vol. 203, no. 1, pp. 237–260, 1969. [Online]. Available: <https://physoc.onlinelibrary.wiley.com/doi/abs/10.1113/jphysiol.1969.sp008862>
- [28] R. Blake, R. Overton, and S. Lema-Stern, “Interocular transfer of visual aftereffects,” *Journal of experimental psychology. Human perception and performance*, vol. 7, pp. 367–81, 05 1981.
- [29] L. M. Hurvich and D. Jameson, “An opponent-process theory of color vision,” *Psychological Review*, vol. 64, pp. 384–404, 12 1957.

- [30] W. S. Stiles and J. H. Parsons, “The directional sensitivity of the retina and the spectral sensitivities of the rods and cones,” *Proceedings of the Royal Society of London. Series B - Biological Sciences*, vol. 127, no. 846, pp. 64–105, 1939. [Online]. Available: <https://royalsocietypublishing.org/doi/abs/10.1098/rspb.1939.0012>
- [31] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, “Intriguing properties of neural networks,” in *International Conference on Learning Representations*, 2014. [Online]. Available: <http://arxiv.org/abs/1312.6199>
- [32] I. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” in *International Conference on Learning Representations*, 2015. [Online]. Available: <http://arxiv.org/abs/1412.6572>
- [33] R. Geirhos, C. R. M. Temme, J. Rauber, H. H. Schütt, M. Bethge, and F. A. Wichmann, “Generalisation in humans and deep neural networks,” in *Proceedings of the 32Nd International Conference on Neural Information Processing Systems*, ser. NIPS’18. USA: Curran Associates Inc., 2018, pp. 7549–7561. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3327757.3327854>
- [34] E. D. Cubuk, B. Zoph, S. S. Schoenholz, and Q. V. Le, “Intriguing properties of adversarial examples,” 2018. [Online]. Available: <https://openreview.net/forum?id=rk6H0ZbRb>
- [35] G. F. Elsayed, S. Shankar, B. Cheung, N. Papernot, A. Kurakin, I. Goodfellow, and J. Sohl-Dickstein, “Adversarial examples influence human visual perception,” *Journal of Vision*, vol. 19, no. 10, pp. 190c–190c, 2019.
- [36] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, “Adversarial machine learning,” in *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, ser. AISec ’11. New York, NY, USA: ACM, 2011, pp. 43–58. [Online]. Available: <http://doi.acm.org/10.1145/2046684.2046692>
- [37] G. Robinson, “A statistical approach to the spam problem,” *Linux J.*, vol. 2003, no. 107, pp. 3–, Mar. 2003. [Online]. Available: <http://dl.acm.org/citation.cfm?id=636750.636753>
- [38] L. Breiman, J. H. Friedman, R. A. Olshen, and C. J. Stone, *Classification and Regression Trees*. Wadsworth, 1984.
- [39] T. Cover and P. Hart, “Nearest neighbor pattern classification,” *IEEE Trans. Inf. Theor.*, vol. 13, no. 1, pp. 21–27, Sep. 2006. [Online]. Available: <https://doi.org/10.1109/TIT.1967.1053964>
- [40] C. Cortes and V. Vapnik, “Support-vector networks,” *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, Sep. 1995. [Online]. Available: <https://doi.org/10.1023/A:1022627411411>
- [41] N. Papernot, P. D. McDaniel, I. J. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, “Practical black-box attacks against deep learning systems using adversarial examples,” *CoRR*, vol. abs/1602.02697, 2016. [Online]. Available: <http://arxiv.org/abs/1602.02697>
- [42] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, “Going deeper with convolutions,” in *Computer Vision and Pattern Recognition (CVPR)*, 2015. [Online]. Available: <http://arxiv.org/abs/1409.4842>
- [43] N. Papernot, P. D. McDaniel, X. Wu, S. Jha, and A. Swami, “Distillation as a defense to adversarial perturbations against deep neural networks.” *CoRR*, vol. abs/1511.04508, 2015. [Online]. Available: <http://dblp.uni-trier.de/db/journals/corr/corr1511.html#PapernotMWJS15>
- [44] N. Carlini and D. A. Wagner, “Towards evaluating the robustness of neural networks,” *CoRR*, vol. abs/1608.04644, 2016. [Online]. Available: <http://arxiv.org/abs/1608.04644>

- [45] A. Kurakin, I. J. Goodfellow, and S. Bengio, “Adversarial machine learning at scale,” 2017. [Online]. Available: <https://arxiv.org/abs/1611.01236>
- [46] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, “Sok: Security and privacy in machine learning,” in *2018 IEEE European Symposium on Security and Privacy (EuroS P)*, April 2018, pp. 399–414.
- [47] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, “Ensemble adversarial training: Attacks and defenses,” in *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=rkZvSe-RZ>
- [48] C. R. I. G. Jacob Buckman, Aurko Roy, “Thermometer encoding: One hot way to resist adversarial examples,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=S18Su--CW>
- [49] Y. W. S. M. E. S. W. G. S. M. E. H. D. S. J. B. Xingjun Ma, Bo Li, “Characterizing adversarial subspaces using local intrinsic dimensionality,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=B1gJ1L2aW>
- [50] G. S. Dhillon, K. Azizzadenesheli, J. D. Bernstein, J. Kossaifi, A. Khanna, Z. C. Lipton, and A. Anandkumar, “Stochastic activation pruning for robust adversarial defense,” in *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=H1uR4GZRZ>
- [51] C. Xie, J. Wang, Z. Zhang, Z. Ren, and A. Yuille, “Mitigating adversarial effects through randomization,” in *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=Sk9yuql0Z>
- [52] R. C. Pouya Samangouei, Maya Kabkab, “Defense-GAN: Protecting classifiers against adversarial attacks using generative models,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=BkJ3ibb0>
- [53] S. N. S. E. N. K. Yang Song, Taesup Kim, “Pixeldefend: Leveraging generative models to understand and defend against adversarial examples,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=rJUYGxbCW>
- [54] M. C. L. v. d. M. Chuan Guo, Mayank Rana, “Countering adversarial images using input transformations,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=SyJ7ClWCb>
- [55] A. Athalye, N. Carlini, and D. Wagner, “Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples,” in *Proceedings of the 35th International Conference on Machine Learning, ICML 2018*, Jul. 2018. [Online]. Available: <https://arxiv.org/abs/1802.00420>
- [56] K. Grosse, N. Papernot, P. Manoharan, M. Backes, and P. McDaniel, “Adversarial examples for malware detection,” in *Computer Security – ESORICS 2017*, S. N. Foley, D. Gollmann, and E. Snekkenes, Eds. Cham: Springer International Publishing, 2017, pp. 62–79.
- [57] N. Carlini and D. A. Wagner, “Audio adversarial examples: Targeted attacks on speech-to-text,” *CoRR*, vol. abs/1801.01944, 2018. [Online]. Available: <http://arxiv.org/abs/1801.01944>
- [58] M. Alzantot, B. Balaji, and M. B. Srivastava, “Did you hear that? adversarial examples against automatic speech recognition,” *CoRR*, vol. abs/1801.00554, 2018. [Online]. Available: <http://arxiv.org/abs/1801.00554>
- [59] F. Kreuk, Y. Adi, M. Cissé, and J. Keshet, “Fooling end-to-end speaker verification by adversarial examples,” *CoRR*, vol. abs/1801.03339, 2018. [Online]. Available: <http://arxiv.org/abs/1801.03339>

- [60] Z. Zhao, D. Dua, and S. Singh, “Generating natural adversarial examples,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=H1BLjgZCb>
- [61] X. Yuan, P. He, Q. Zhu, and X. Li, “Adversarial examples: Attacks and defenses for deep learning,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 9, pp. 2805–2824, Sep. 2019.
- [62] N. Akhtar and A. Mian, “Threat of adversarial attacks on deep learning in computer vision: A survey,” *IEEE Access*, vol. 6, pp. 14 410–14 430, 2018.
- [63] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” in *Advances in Neural Information Processing Systems 27*, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, Eds. Curran Associates, Inc., 2014, pp. 2672–2680. [Online]. Available: <http://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf>
- [64] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, “Accessorize 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>
- [65] 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>
- [66] 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>
- [67] N. Papernot, P. D. McDaniel, and I. J. Goodfellow, “Transferability in machine learning: from phenomena to black-box attacks using adversarial samples,” *CoRR*, vol. abs/1605.07277, 2016. [Online]. Available: <http://arxiv.org/abs/1605.07277>
- [68] Y. Liu, X. Chen, C. Liu, and D. Song, “Delving into transferable adversarial examples and black-box attacks,” *CoRR*, vol. abs/1611.02770, 2016. [Online]. Available: <http://arxiv.org/abs/1611.02770>
- [69] X. Glorot, A. Bordes, and Y. Bengio, “Deep sparse rectifier neural networks,” in *Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, G. Gordon, D. Dunson, and M. Dudăčk, Eds., vol. 15. Fort Lauderdale, FL, USA: PMLR, 11–13 Apr 2011, pp. 315–323. [Online]. Available: <http://proceedings.mlr.press/v15/glorot11a.html>
- [70] I. J. Goodfellow, D. Warde-Farley, M. Mirza, A. Courville, and Y. Bengio, “Maxout networks,” in *Proceedings of the 30th International Conference on International Conference on Machine Learning - Volume 28*, ser. ICML’13. JMLR.org, 2013, pp. III–1319–III–1327. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3042817.3043084>
- [71] S. Hochreiter, “The vanishing gradient problem during learning recurrent neural nets and problem solutions,” *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 6, no. 2, pp. 107–116, Apr. 1998. [Online]. Available: <http://dx.doi.org/10.1142/S0218488598000094>
- [72] S. Hochreiter, Y. Bengio, and P. Frasconi, “Gradient flow in recurrent nets: the difficulty of learning long-term dependencies,” in *Field Guide to Dynamical Recurrent Networks*, J. Kolen and S. Kremer, Eds. IEEE Press, 2001.

- [73] R. Pascanu, T. Mikolov, and Y. Bengio, “On the difficulty of training recurrent neural networks,” in *Proceedings of the 30th International Conference on International Conference on Machine Learning - Volume 28*, ser. ICML’13. JMLR.org, 2013, pp. III–1310–III–1318. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3042817.3043083>
- [74] D. Arpit, S. Jastrzebski, N. Ballas, D. Krueger, E. Bengio, M. S. Kanwal, T. Maharaj, A. Fischer, A. Courville, Y. Bengio, and S. Lacoste-Julien, “A closer look at memorization in deep networks,” in *Proceedings of the 34th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, D. Precup and Y. W. Teh, Eds., vol. 70. International Convention Centre, Sydney, Australia: PMLR, 06–11 Aug 2017, pp. 233–242. [Online]. Available: <http://proceedings.mlr.press/v70/arpit17a.html>
- [75] J. Jo and Y. Bengio, “Measuring the tendency of cnns to learn surface statistical regularities,” *CoRR*, vol. abs/1711.11561, 2017. [Online]. Available: <http://arxiv.org/abs/1711.11561>
- [76] A. Ilyas, S. Santurkar, D. Tsipras, L. Engstrom, B. Tran, and A. Madry, “Adversarial examples are not bugs, they are features,” *arXiv preprint arXiv:1905.02175*, 2019.
- [77] A. Kurakin, I. J. Goodfellow, and S. Bengio, “Adversarial examples in the physical world,” *CoRR*, vol. abs/1607.02533, 2016. [Online]. Available: <http://arxiv.org/abs/1607.02533>
- [78] S. Sabour, Y. Cao, F. Faghri, and D. J. Fleet, “Adversarial manipulation of deep representations,” *CoRR*, vol. abs/1511.05122, 2015. [Online]. Available: <http://arxiv.org/abs/1511.05122>
- [79] 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>
- [80] N. Papernot, P. D. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, “The limitations of deep learning in adversarial settings,” *CoRR*, vol. abs/1511.07528, 2015. [Online]. Available: <http://arxiv.org/abs/1511.07528>
- [81] D. Meng and H. Chen, “Magnet: A two-pronged defense against adversarial examples,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’17. New York, NY, USA: ACM, 2017, pp. 135–147. [Online]. Available: <http://doi.acm.org/10.1145/3133956.3134057>
- [82] A. Rozsa, E. M. Rudd, and T. E. Boult, “Adversarial diversity and hard positive generation,” *CoRR*, vol. abs/1605.01775, 2016. [Online]. Available: <http://arxiv.org/abs/1605.01775>
- [83] 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>
- [84] K. R. Mopuri, A. Ganeshan, and R. V. Babu, “Generalizable data-free objective for crafting universal adversarial perturbations,” 2018.
- [85] J. Kos, I. Fischer, and D. Song, “Adversarial examples for generative models,” *CoRR*, vol. abs/1702.06832, 2017. [Online]. Available: <http://arxiv.org/abs/1702.06832>
- [86] D. P. Kingma and M. Welling, “Auto-encoding variational bayes,” *CoRR*, vol. abs/1312.6114, 2013. [Online]. Available: <http://arxiv.org/abs/1312.6114>
- [87] S. Baluja and I. Fischer, “Learning to attack: Adversarial transformation networks,” in *Proceedings of AAAI-2018*, 2018. [Online]. Available: <http://www.esprockets.com/papers/aaai2018.pdf>
- [88] C. Xie, J. Wang, Z. Zhang, Y. Zhou, L. Xie, and A. L. Yuille, “Adversarial examples for semantic segmentation and object detection,” *CoRR*, vol. abs/1703.08603, 2017. [Online]. Available: <http://arxiv.org/abs/1703.08603>

- [89] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, and C.-J. Hsieh, “Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models,” in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*, ser. AISec ’17. New York, NY, USA: ACM, 2017, pp. 15–26. [Online]. Available: <http://doi.acm.org/10.1145/3128572.3140448>
- [90] J. Su, D. V. Vargas, and K. Sakurai, “One pixel attack for fooling deep neural networks,” *CoRR*, vol. abs/1710.08864, 2017. [Online]. Available: <http://arxiv.org/abs/1710.08864>
- [91] M. Cissé, Y. Adi, N. Neverova, and J. Keshet, “Houdini: Fooling deep structured visual and speech recognition models with adversarial examples,” in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, 4-9 December 2017, Long Beach, CA, USA*, 2017, pp. 6980–6990.
- [92] Y. Dong, F. Liao, T. Pang, H. Su, J. Zhu, X. Hu, and J. Li, “Boosting adversarial attacks with momentum,” in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2018.
- [93] C. Xiao, B. Li, J.-Y. Zhu, W. He, M. Liu, and D. Song, “Generating adversarial examples with adversarial networks,” 2018. [Online]. Available: <https://openreview.net/forum?id=HknbyQbC->
- [94] W. Brendel, J. Rauber, and M. Bethge, “Decision-based adversarial attacks: Reliable attacks against black-box machine learning models,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=SyZI0GWCZ>
- [95] C. Xiao, J.-Y. Zhu, B. Li, W. He, M. Liu, and D. Song, “Spatially transformed adversarial examples,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=HyydRMZC->
- [96] A. Athalye, L. Engstrom, A. Ilyas, and K. Kwok, “Synthesizing robust adversarial examples,” in *Proceedings of the 35th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, J. Dy and A. Krause, Eds., vol. 80. Stockholm, Sweden: PMLR, 10–15 Jul 2018, pp. 284–293. [Online]. Available: <http://proceedings.mlr.press/v80/athalye18b.html>
- [97] J. Uesato, B. O’Donoghue, P. Kohli, and A. van den Oord, “Adversarial risk and the dangers of evaluating against weak attacks,” in *Proceedings of the 35th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, J. Dy and A. Krause, Eds., vol. 80. Stockholm, Sweden: PMLR, 10–15 Jul 2018, pp. 5025–5034. [Online]. Available: <http://proceedings.mlr.press/v80/uesato18a.html>
- [98] J. Rony, L. G. Hafemann, L. S. Oliveira, I. B. Ayed, R. Sabourin, and E. Granger, “Decoupling direction and norm for efficient gradient-based L2 adversarial attacks and defenses,” *CoRR*, vol. abs/1811.09600, 2018. [Online]. Available: <http://arxiv.org/abs/1811.09600>
- [99] Y. Zhang, H. Foroosh, P. David, and B. Gong, “CAMOU: Learning physical vehicle camouflages to adversarially attack detectors in the wild,” in *International Conference on Learning Representations*, 2019. [Online]. Available: <https://openreview.net/forum?id=SJgEl3A5tm>
- [100] D. C. Liu and J. Nocedal, “On the limited memory bfgs method for large scale optimization,” *Mathematical Programming*, vol. 45, no. 1, pp. 503–528, Aug 1989. [Online]. Available: <https://doi.org/10.1007/BF01589116>
- [101] Q. V. Le, M. Ranzato, R. Monga, M. Devin, K. Chen, G. S. Corrado, J. Dean, and A. Y. Ng, “Building high-level features using large scale unsupervised learning,” in *Proceedings of the 29th International Conference on International Conference on Machine Learning*, ser. ICML’12. USA: Omnipress, 2012, pp. 507–514. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3042573.3042641>

- [102] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, “Learning representations by back-propagating errors,” *Nature*, vol. 323, pp. 533 EP –, Oct 1986. [Online]. Available: <http://dx.doi.org/10.1038/323533a0>
- [103] S. H. Huang, N. Papernot, I. J. Goodfellow, Y. Duan, and P. Abbeel, “Adversarial attacks on neural network policies,” *CoRR*, vol. abs/1702.02284, 2017. [Online]. Available: <http://arxiv.org/abs/1702.02284>
- [104] R. S. Sutton and A. G. Barto, *Introduction to Reinforcement Learning*, 1st ed. Cambridge, MA, USA: MIT Press, 1998.
- [105] J. Schulman, S. Levine, P. Abbeel, M. Jordan, and P. Moritz, “Trust region policy optimization,” in *Proceedings of the 32nd International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, F. Bach and D. Blei, Eds., vol. 37. Lille, France: PMLR, 07–09 Jul 2015, pp. 1889–1897. [Online]. Available: <http://proceedings.mlr.press/v37/schulman15.html>
- [106] V. Mnih, A. P. Badia, M. Mirza, A. Graves, T. Lillicrap, T. Harley, D. Silver, and K. Kavukcuoglu, “Asynchronous methods for deep reinforcement learning,” in *Proceedings of The 33rd International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, M. F. Balcan and K. Q. Weinberger, Eds., vol. 48. New York, New York, USA: PMLR, 20–22 Jun 2016, pp. 1928–1937. [Online]. Available: <http://proceedings.mlr.press/v48/mnih16.html>
- [107] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S. Legg, and D. Hassabis, “Human-level control through deep reinforcement learning,” *Nature*, vol. 518, no. 7540, pp. 529–533, 02 2015. [Online]. Available: <http://dx.doi.org/10.1038/nature14236>
- [108] M. G. Bellemare, Y. Naddaf, J. Veness, and M. Bowling, “The arcade learning environment: An evaluation platform for general agents,” in *Proceedings of the 24th International Conference on Artificial Intelligence*, ser. IJCAI’15. AAAI Press, 2015, pp. 4148–4152. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2832747.2832830>
- [109] V. Fischer, M. C. Kumar, J. H. Metzen, and T. Brox, “Adversarial examples for semantic image segmentation,” *CoRR*, vol. abs/1703.01101, 2017. [Online]. Available: <http://arxiv.org/abs/1703.01101>
- [110] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, “Inception-v4, inception-resnet and the impact of residual connections on learning,” in *ICLR 2016 Workshop*, 2016. [Online]. Available: <https://arxiv.org/abs/1602.07261>
- [111] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, “Rethinking the inception architecture for computer vision,” in *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*,, 2016. [Online]. Available: <http://arxiv.org/abs/1512.00567>
- [112] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, “Caffe: Convolutional architecture for fast feature embedding,” in *Proceedings of the 22Nd ACM International Conference on Multimedia*, ser. MM ’14. New York, NY, USA: ACM, 2014, pp. 675–678. [Online]. Available: <http://doi.acm.org/10.1145/2647868.2654889>
- [113] K. Chatfield, K. Simonyan, A. Vedaldi, and A. Zisserman, “Return of the devil in the details: Delving deep into convolutional nets,” in *British Machine Vision Conference*, 2014.
- [114] B. Zhou, A. Lapedriza, J. Xiao, A. Torralba, and A. Oliva, “Learning deep features for scene recognition using places database,” in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 1*, ser. NIPS’14. Cambridge, MA, USA: MIT Press, 2014, pp. 487–495. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2968826.2968881>

- [115] A. Mahendran and A. Vedaldi, “Understanding deep image representations by inverting them,” in *Proceedings of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2015.
- [116] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov 1998.
- [117] M. Lin, Q. Chen, and S. Yan, “Network in network,” *CoRR*, vol. abs/1312.4400, 2013.
- [118] K. Simonyan, A. Vedaldi, and A. Zisserman, “Deep inside convolutional networks: Visualising image classification models and saliency maps,” *CoRR*, vol. abs/1312.6034, 2013. [Online]. Available: <http://arxiv.org/abs/1312.6034>
- [119] H. Xiao, K. Rasul, and R. Vollgraf, “Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms,” *CoRR*, vol. abs/1708.07747, 2017. [Online]. Available: <http://arxiv.org/abs/1708.07747>
- [120] A. Krizhevsky, “Learning multiple layers of features from tiny images,” 2009.
- [121] J. Stallkamp, M. Schlipsing, J. Salmen, and C. Igel, “Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition,” *Neural Networks*, no. 0, pp. –, 2012. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0893608012000457>
- [122] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” *CoRR*, vol. abs/1409.1556, 2014.
- [123] J. H. Metzen, M. C. Kumar, T. Brox, and V. Fischer, “Universal adversarial perturbations against semantic image segmentation,” in *submitted*, 2017. [Online]. Available: <https://arxiv.org/abs/1704.05712>
- [124] K. R. Mopuri, U. Garg, and R. V. Babu, “Fast feature fool: A data independent approach to universal adversarial perturbations,” *CoRR*, vol. abs/1707.05572, 2017. [Online]. Available: <http://arxiv.org/abs/1707.05572>
- [125] C. Godard, O. Mac Aodha, and G. J. Brostow, “Unsupervised monocular depth estimation with left-right consistency,” in *CVPR*, 2017.
- [126] A. B. L. Larsen, S. K. Sønderby, H. Larochelle, and O. Winther, “Autoencoding beyond pixels using a learned similarity metric,” in *Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48*, ser. ICML’16. JMLR.org, 2016, pp. 1558–1566. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3045390.3045555>
- [127] S. Kullback and R. A. Leibler, “On information and sufficiency,” *Ann. Math. Statist.*, vol. 22, no. 1, pp. 79–86, 03 1951. [Online]. Available: <https://doi.org/10.1214/aoms/1177729694>
- [128] Y. Netzer, T. Wang, A. Coates, A. Bissacco, B. Wu, and A. Y. Ng, “Reading digits in natural images with unsupervised feature learning,” in *NIPS Workshop on Deep Learning and Unsupervised Feature Learning 2011*, 2011. [Online]. Available: http://ufldl.stanford.edu/housenumbers/nips2011_housenumbers.pdf
- [129] Z. Liu, P. Luo, X. Wang, and X. Tang, “Deep learning face attributes in the wild,” *CoRR*, vol. abs/1411.7766, 2014. [Online]. Available: <http://arxiv.org/abs/1411.7766>
- [130] L. A. Gatys, A. S. Ecker, and M. Bethge, “A neural algorithm of artistic style,” *arXiv*, Aug 2015. [Online]. Available: <http://arxiv.org/abs/1508.06576>
- [131] J. Johnson, A. Alahi, and F. Li, “Perceptual losses for real-time style transfer and super-resolution,” *CoRR*, vol. abs/1603.08155, 2016. [Online]. Available: <http://arxiv.org/abs/1603.08155>

- [132] J. Hamm, “Machine vs machine: Defending classifiers against learning-based adversarial attacks,” *CoRR*, vol. abs/1711.04368, 2017. [Online]. Available: <http://arxiv.org/abs/1711.04368>
- [133] J. Kirkpatrick, R. Pascanu, N. Rabinowitz, J. Veness, G. Desjardins, A. A. Rusu, K. Milan, J. Quan, T. Ramalho, A. Grabska-Barwinska, D. Hassabis, C. Clopath, D. Kumaran, and R. Hadsell, “Overcoming catastrophic forgetting in neural networks,” *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3521–3526, 2017. [Online]. Available: <http://www.pnas.org/content/114/13/3521>
- [134] L. Bottou, “Large-scale machine learning with stochastic gradient descent,” in *in COMPSTAT*, 2010.
- [135] S. J. Wright, “Coordinate descent algorithms,” *Math. Program.*, vol. 151, no. 1, pp. 3–34, Jun. 2015. [Online]. Available: <http://dx.doi.org/10.1007/s10107-015-0892-3>
- [136] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” *CoRR*, vol. abs/1412.6980, 2014. [Online]. Available: <http://arxiv.org/abs/1412.6980>
- [137] N. Ahmed, T. Natarajan, and K. R. Rao, “Discrete cosine transform,” *IEEE Trans. Comput.*, vol. 23, no. 1, pp. 90–93, Jan. 1974. [Online]. Available: <http://dx.doi.org/10.1109/T-C.1974.223784>
- [138] R. Storn and K. Price, “Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces,” *Journal of Global Optimization*, vol. 11, no. 4, pp. 341–359, Dec 1997. [Online]. Available: <https://doi.org/10.1023/A:1008202821328>
- [139] S. Das and P. N. Suganthan, “Differential evolution: A survey of the state-of-the-art,” *IEEE Transactions on Evolutionary Computation*, vol. 15, no. 1, pp. 4–31, Feb 2011.
- [140] J. T. Springenberg, A. Dosovitskiy, T. Brox, and M. A. Riedmiller, “Striving for simplicity: The all convolutional net,” *CoRR*, vol. abs/1412.6806, 2014.
- [141] A. Newell, K. Yang, and J. Deng, “Stacked hourglass networks for human pose estimation,” *CoRR*, vol. abs/1603.06937, 2016. [Online]. Available: <http://arxiv.org/abs/1603.06937>
- [142] Z. Cao, T. Simon, S.-E. Wei, and Y. Sheikh, “Realtime multi-person 2d pose estimation using part affinity fields,” in *CVPR*, 2017.
- [143] B. Polyak, “Some methods of speeding up the convergence of iteration methods,” *USSR Computational Mathematics and Mathematical Physics*, vol. 4, no. 5, pp. 1 – 17, 1964. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0041555364901375>
- [144] A. Kurakin, I. J. Goodfellow, S. Bengio, Y. Dong, F. Liao, M. Liang, T. Pang, J. Zhu, X. Hu, C. Xie, J. Wang, Z. Zhang, Z. Ren, A. L. Yuille, S. Huang, Y. Zhao, Y. Zhao, Z. Han, J. Long, Y. Berdibekov, T. Akiba, S. Tokui, and M. Abe, “Adversarial attacks and defences competition,” *CoRR*, vol. abs/1804.00097, 2018. [Online]. Available: <http://arxiv.org/abs/1804.00097>
- [145] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, “Towards deep learning models resistant to adversarial attacks,” *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=rJzIBfZAb>
- [146] R. Zhang, P. Isola, and A. A. Efros, “Colorful image colorization,” in *ECCV*, 2016.
- [147] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, “Image-to-image translation with conditional adversarial networks,” in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, July 2017.
- [148] M. Arjovsky, S. Chintala, and L. Bottou, “Wasserstein generative adversarial networks,” in *Proceedings of the 34th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, D. Precup and Y. W. Teh, Eds., vol. 70. International Convention Centre, Sydney, Australia: PMLR, 06–11 Aug 2017, pp. 214–223. [Online]. Available: <http://proceedings.mlr.press/v70/arjovsky17a.html>

- [149] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, “Unpaired image-to-image translation using cycle-consistent adversarial networkss,” in *Computer Vision (ICCV), 2017 IEEE International Conference on*, 2017.
- [150] S. R. Bowman, G. Angeli, C. Potts, and C. D. Manning, “A large annotated corpus for learning natural language inference,” *CoRR*, vol. abs/1508.05326, 2015. [Online]. Available: <http://arxiv.org/abs/1508.05326>
- [151] Z. Wang and A. C. Bovik, “Mean squared error: Love it or leave it? a new look at signal fidelity measures,” *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 98–117, Jan 2009.
- [152] M. Jaderberg, K. Simonyan, A. Zisserman, and k. kavukcuoglu, “Spatial transformer networks,” in *Advances in Neural Information Processing Systems 28*, C. Cortes, N. D. Lawrence, D. D. Lee, M. Sugiyama, and R. Garnett, Eds. Curran Associates, Inc., 2015, pp. 2017–2025. [Online]. Available: <http://papers.nips.cc/paper/5854-spatial-transformer-networks.pdf>
- [153] T. Zhou, S. Tulsiani, W. Sun, J. Malik, and A. A. Efros, “View synthesis by appearance flow,” in *European Conference on Computer Vision*, 2016.
- [154] L. I. Rudin, S. Osher, and E. Fatemi, “Nonlinear total variation based noise removal algorithms,” *Physica D: Nonlinear Phenomena*, vol. 60, no. 1, pp. 259 – 268, 1992. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/016727899290242F>
- [155] K. McLaren, “Xiiiâ€”the development of the cie 1976 (l^* a^* b^*) uniform colour space and colourâ€”difference formula,” *Journal of the Society of Dyers and Colourists*, vol. 92, no. 9, pp. 338–341, 1976. [Online]. Available: <https://onlinelibrary.wiley.com/doi/10.1111/j.1478-4408.1976.tb03301.x>
- [156] S. Chen, C. Cornelius, J. Martin, and D. H. Chau, “Robust physical adversarial attack on faster R-CNN object detector,” *CoRR*, vol. abs/1804.05810, 2018. [Online]. Available: <http://arxiv.org/abs/1804.05810>
- [157] Y. Bengio, N. Léonard, and A. C. Courville, “Estimating or propagating gradients through stochastic neurons for conditional computation,” *CoRR*, vol. abs/1308.3432, 2013. [Online]. Available: <http://arxiv.org/abs/1308.3432>
- [158] J. C. Spall, “Multivariate stochastic approximation using a simultaneous perturbation gradient approximation,” *IEEE Transactions on Automatic Control*, vol. 37, no. 3, pp. 332–341, Mar 1992.
- [159] F. Liao, M. Liang, Y. Dong, T. Pang, J. Zhu, and X. Hu, “Defense against adversarial attacks using high-level representation guided denoiser,” *CoRR*, vol. abs/1712.02976, 2017. [Online]. Available: <http://arxiv.org/abs/1712.02976>
- [160] J. Redmon and A. Farhadi, “Yolov3: An incremental improvement,” *CoRR*, vol. abs/1804.02767, 2018. [Online]. Available: <http://arxiv.org/abs/1804.02767>
- [161] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, “Microsoft coco: Common objects in context,” in *Computer Vision – ECCV 2014*, D. Fleet, T. Pajdla, B. Schiele, and T. Tuytelaars, Eds. Cham: Springer International Publishing, 2014, pp. 740–755.
- [162] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep face recognition,” in *British Machine Vision Conference*, 2015.
- [163] 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.

- [164] G. B. H. E. Learned-Miller, "Labeled faces in the wild: Updates and new reporting procedures," University of Massachusetts, Amherst, Tech. Rep. UM-CS-2014-003, May 2014.
- [165] N. Kumar, A. C. Berg, P. N. Belhumeur, and S. K. Nayar, "Attribute and simile classifiers for face verification," in *2009 IEEE 12th International Conference on Computer Vision*, Sept 2009, pp. 365–372.
- [166] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "Adversarial generative nets: Neural network attacks on state-of-the-art face recognition," *arXiv preprint arXiv:1801.00349*, 2017.
- [167] J. Lu, H. Sibai, E. Fabry, and D. A. Forsyth, "NO need to worry about adversarial examples in object detection in autonomous vehicles," *CoRR*, vol. abs/1707.03501, 2017. [Online]. Available: <http://arxiv.org/abs/1707.03501>
- [168] ——, "Standard detectors aren't (currently) fooled by physical adversarial stop signs," *CoRR*, vol. abs/1710.03337, 2017. [Online]. Available: <http://arxiv.org/abs/1710.03337>
- [169] L. Bondi, L. Baroffio, D. GÃ¡ijera, P. Bestagini, E. J. Delp, and S. Tubaro, "First steps toward camera model identification with convolutional neural networks," *IEEE Signal Processing Letters*, vol. 24, no. 3, pp. 259–263, March 2017.
- [170] A. Tuama, F. Comby, and M. Chaumont, "Camera Model Identification With The Use of Deep Convolutional Neural Networks," in *WIFS: Workshop on Information Forensics and Security*, Abu Dhabi, United Arab Emirates, Dec. 2016. [Online]. Available: <https://hal.archives-ouvertes.fr/hal-01388975>
- [171] L. Bondi, D. GÃ¼era, L. Baroffio, P. Bestagini, E. J. Delp, and S. Tubaro, "A preliminary study on convolutional neural networks for camera model identification," *Electronic Imaging*, vol. 2017, no. 7, pp. 67–76, 2017. [Online]. Available: <https://www.ingentaconnect.com/content/ist/ei/2017/00002017/00000007/art00011>
- [172] D. GÃ¼era, Y. Wang, L. Bondi, P. Bestagini, S. Tubaro, and E. J. Delp, "A counter-forensic method for cnn-based camera model identification," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, July 2017, pp. 1840–1847.
- [173] P. Saadatpanah, A. Shafahi, and T. Goldstein, "Adversarial attacks on copyright detection systems," *arXiv preprint arXiv:1906.07153*, 2019.
- [174] D. Shen, G. Wu, and H.-I. Suk, "Deep learning in medical image analysis," *Annu Rev Biomed Eng*, vol. 19, pp. 221–248, Jun 2017, 28301734[pmid]. [Online]. Available: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC5479722/>
- [175] B. E. Bejnordi, M. Veta, P. J. van Diest, B. T. J. van Ginneken, N. Karssemeijer, G. Litjens, J. A. W. M. van der Laak, M. Hermsen, Q. F. Manson, M. Balkenhol, O. Geessink, N. Stathonikos, M. R. C. F. van Dijk, P. Bult, F. Beca, A. H. Beck, D. Wang, A. Khosla, R. Gargeya, H. Irshad, A. Zhong, Q. Dou, Q. Li, H. Chen, H.-J. Lin, P.-A. Heng, C. Hass, E. Bruni, Q. J. J. Wong, U. Halici, M. Ü. Öner, R. ÄGetin Atalay, M. Berseth, V. Khvatkov, A. Vylegzhanin, O. Kraus, M. Shaban, N. M. Rajpoot, R. Awan, K. Sirinukunwattana, T. Qaiser, Y.-W. Tsang, D. Tellez, J. Annuscheit, P. Hufnagl, M. Valkonen, K. Kartasalo, L. Latonen, P. Ruusuvuori, K. Liimatainen, S. Albarqouni, B. Mungal, A. George, S. Demirci, N. Navab, S. Watanabe, S. Seno, Y. Takenaka, H. Matsuda, H. A. Phoulady, V. Kovalev, A. Kalinovsky, V. Liauchuk, G. Bueno, M. del Milagro Fernández-Carrobles, I. Serrano, Ó. Déniz, D. Racoceanu, and R. de Abreu Venancio, "Diagnostic assessment of deep learning algorithms for detection of lymph node metastases in women with breast cancer." *JAMA*, vol. 318 22, pp. 2199–2210, 2017.
- [176] P. Rajpurkar, J. Irvin, K. Zhu, B. Yang, H. Mehta, T. Duan, D. Ding, A. Bagul, C. P. Langlotz, K. Shpanskaya, M. P. Lungren, and A. Y. Ng, "CheXnet: Radiologist-level pneumonia detection on chest x-rays with deep learning," *CoRR*, vol. abs/1711.05225, 2017.

- [177] A. Esteva, B. Kuprel, R. A. Novoa, J. Ko, S. M. Swetter, H. M. Blau, and S. Thrun, “Dermatologist-level classification of skin cancer with deep neural networks,” *Nature*, vol. 542, pp. 115 EP –, Jan 2017. [Online]. Available: <http://dx.doi.org/10.1038/nature21056>
- [178] H. A. Haenssle, C. Fink, R. Schneiderbauer, F. Toberer, T. Buhl, A. Blum, A. Kalloo, A. B. H. Hassen, L. Thomas, A. Enk, L. Uhlmann, and Collaborators, “Man against machine: diagnostic performance of a deep learning convolutional neural network for dermoscopic melanoma recognition in comparison to 58 dermatologists,” *Annals of Oncology*, p. mdy166, 2018. [Online]. Available: <http://dx.doi.org/10.1093/annonc/mdy166>
- [179] S. G. Finlayson, I. S. Kohane, and A. L. Beam, “Adversarial attacks against medical deep learning systems,” *CoRR*, vol. abs/1804.05296, 2018. [Online]. Available: <http://arxiv.org/abs/1804.05296>
- [180] S. Gu and L. Rigazio, “Towards deep neural network architectures robust to adversarial examples,” *CoRR*, vol. abs/1412.5068, 2014. [Online]. Available: <http://arxiv.org/abs/1412.5068>
- [181] N. Carlini and D. A. Wagner, “Defensive distillation is not robust to adversarial examples,” *CoRR*, vol. abs/1607.04311, 2016. [Online]. Available: <http://arxiv.org/abs/1607.04311>
- [182] A. Sinha, H. Namkoong, and J. Duchi, “Certifiable distributional robustness with principled adversarial training,” in *International Conference on Learning Representations*, 2018. [Online]. Available: <https://openreview.net/forum?id=Hk6kPgZA->
- [183] H. Kannan, A. Kurakin, and I. J. Goodfellow, “Adversarial logit pairing,” *CoRR*, vol. abs/1803.06373, 2018. [Online]. Available: <http://arxiv.org/abs/1803.06373>
- [184] L. Engstrom, A. Ilyas, and A. Athalye, “Evaluating and understanding the robustness of adversarial logit pairing,” *CoRR*, vol. abs/1807.10272, 2018. [Online]. Available: <http://arxiv.org/abs/1807.10272>
- [185] A. Lamb, J. Binas, A. Goyal, D. Serdyuk, S. Subramanian, S. I. Mamilakis, and Y. Bengio, “Fortified networks: Improving the robustness of deep networks by modeling the manifold of hidden representations,” *arXiv e-prints*, vol. 1804.02485, Apr. 2018. [Online]. Available: <https://arxiv.org/abs/1804.02485>
- [186] C. Xie, Y. Wu, L. van der Maaten, A. L. Yuille, and K. He, “Feature denoising for improving adversarial robustness,” *CoRR*, vol. abs/1812.03411, 2018.
- [187] L. Schott, J. Rauber, W. Brendel, and M. Bethge, “Towards the first adversarially robust neural network model on mnist,” May 2019. [Online]. Available: <https://arxiv.org/pdf/1805.09190.pdf>
- [188] A. Dubey, L. van der Maaten, Z. Yalniz, Y. Li, and D. Mahajan, “Defense against adversarial images using web-scale nearest-neighbor search,” *CoRR*, vol. abs/1903.01612, 2019. [Online]. Available: <http://arxiv.org/abs/1903.01612>
- [189] Y. Yang, G. Zhang, Z. Xu, and D. Katabi, “ME-net: Towards effective adversarial robustness with matrix estimation,” in *Proceedings of the 36th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, K. Chaudhuri and R. Salakhutdinov, Eds., vol. 97. Long Beach, California, USA: PMLR, 09–15 Jun 2019, pp. 7025–7034. [Online]. Available: <http://proceedings.mlr.press/v97/yang19e.html>
- [190] D. Hendrycks and K. Gimpel, “Visible progress on adversarial images and a new saliency map,” *CoRR*, vol. abs/1608.00530, 2016. [Online]. Available: <http://arxiv.org/abs/1608.00530>
- [191] ——, “A baseline for detecting misclassified and out-of-distribution examples in neural networks,” *CoRR*, vol. abs/1610.02136, 2016. [Online]. Available: <http://arxiv.org/abs/1610.02136>

- [192] J. H. Metzen, T. Genewein, V. Fischer, and B. Bischoff, "On detecting adversarial perturbations," in *Proceedings of 5th International Conference on Learning Representations (ICLR)*, 2017. [Online]. Available: <https://arxiv.org/abs/1702.04267>
- [193] 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>
- [194] 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>
- [195] H. Hosseini, Y. Chen, S. Kannan, B. Zhang, and R. Poovendran, "Blocking transferability of adversarial examples in black-box learning systems," *CoRR*, vol. abs/1703.04318, 2017. [Online]. Available: <http://arxiv.org/abs/1703.04318>
- [196] R. Feinman, R. R. Curtin, S. Shintre, and A. B. Gardner, "Detecting adversarial samples from artifacts," *CoRR*, vol. abs/1703.00410, 2017. [Online]. Available: <http://arxiv.org/abs/1703.00410>
- [197] W. Xu, D. Evans, and Y. Qi, "Feature squeezing: Detecting adversarial examples in deep neural networks," *CoRR*, vol. abs/1704.01155, 2017. [Online]. Available: <http://arxiv.org/abs/1704.01155>
- [198] T. Pang, C. Du, and J. Zhu, "Robust deep learning via reverse cross-entropy training and thresholding test," *CoRR*, vol. abs/1706.00633, 2017. [Online]. Available: <http://arxiv.org/abs/1706.00633>
- [199] S. Rifai, P. Vincent, X. Muller, X. Glorot, and Y. Bengio, "Contractive auto-encoders: Explicit invariance during feature extraction," in *Proceedings of the 28th International Conference on International Conference on Machine Learning*, ser. ICML'11. USA: Omnipress, 2011, pp. 833–840. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3104482.3104587>
- [200] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," in *NIPS Deep Learning and Representation Learning Workshop*, 2015. [Online]. Available: <http://arxiv.org/abs/1503.02531>
- [201] B. Fuglede and F. Topsøe, "Jensen-shannon divergence and hilbert space embedding," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, June 2004, pp. 31–.
- [202] N. Carlini and D. A. Wagner, "Magnet and "efficient defenses against adversarial attacks" are not robust to adversarial examples," *CoRR*, vol. abs/1711.08478, 2017. [Online]. Available: <http://arxiv.org/abs/1711.08478>
- [203] R. Huang, B. Xu, D. Schuurmans, and C. Szepesvári, "Learning with a strong adversary," *CoRR*, vol. abs/1511.03034, 2015. [Online]. Available: <http://arxiv.org/abs/1511.03034>
- [204] U. Shaham, Y. Yamada, and S. Negahban, "Understanding adversarial training: Increasing local stability of supervised models through robust optimization," *Neurocomputing*, vol. 307, pp. 195 – 204, 2018. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0925231218304557>
- [205] A. Ben-Tal, L. El Ghaoui, and A. Nemirovski, *Robust Optimization*, ser. Princeton Series in Applied Mathematics. Princeton University Press, October 2009.
- [206] A. Choromanska, M. Henaff, M. Mathieu, G. B. Arous, and Y. LeCun, "The Loss Surfaces of Multilayer Networks," in *Proceedings of the Eighteenth International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, G. Lebanon and S. V. N. Vishwanathan, Eds., vol. 38. San Diego, California, USA: PMLR, 09–12 May 2015, pp. 192–204. [Online]. Available: <http://proceedings.mlr.press/v38/choromanska15.html>

- [207] D. Tsipras, S. Santurkar, L. Engstrom, A. Turner, and A. Madry, “Robustness may be at odds with accuracy,” *arXiv preprint arXiv:1805.12152*, 2018.
- [208] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, “Grad-cam: Visual explanations from deep networks via gradient-based localization,” in *2017 IEEE International Conference on Computer Vision (ICCV)*, Oct 2017, pp. 618–626.
- [209] L. Engstrom, A. Ilyas, S. Santurkar, D. Tsipras, B. Tran, and A. Madry, “Learning perceptually-aligned representations via adversarial robustness,” in *ArXiv preprint arXiv:1906.00945*, 2019.
- [210] F. Tramèr and D. Boneh, “Adversarial training and robustness for multiple perturbations,” *arXiv preprint arXiv:1904.13000*, 2019.
- [211] D. Kang, Y. Sun, T. Brown, D. Hendrycks, and J. Steinhardt, “Transfer of adversarial robustness between perturbation types,” *arXiv preprint arXiv:1905.01034*, 2019.
- [212] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: A simple way to prevent neural networks from overfitting,” *Journal of Machine Learning Research*, vol. 15, pp. 1929–1958, 2014. [Online]. Available: <http://jmlr.org/papers/v15/srivastava14a.html>
- [213] N. Metropolis and S. Ulam, “The monte carlo method,” *Journal of the American Statistical Association*, vol. 44, no. 247, pp. 335–341, 1949. [Online]. Available: <http://www.jstor.org/stable/2280232>
- [214] H. v. Hasselt, A. Guez, and D. Silver, “Deep reinforcement learning with double q-learning,” in *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, ser. AAAI’16. AAAI Press, 2016, pp. 2094–2100. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3016100.3016191>
- [215] G. K. Dziugaite, Z. Ghahramani, and D. M. Roy, “A study of the effect of JPG compression on adversarial images,” *CoRR*, vol. abs/1608.00853, 2016. [Online]. Available: <http://arxiv.org/abs/1608.00853>
- [216] A. A. Efros and W. T. Freeman, “Image quilting for texture synthesis and transfer,” in *Proceedings of the 28th Annual Conference on Computer Graphics and Interactive Techniques*, ser. SIGGRAPH ’01. New York, NY, USA: ACM, 2001, pp. 341–346. [Online]. Available: <http://doi.acm.org/10.1145/383259.383296>
- [217] H. Shimodaira, “Improving predictive inference under covariate shift by weighting the log-likelihood function,” *Journal of Statistical Planning and Inference*, vol. 90, no. 2, pp. 227 – 244, 2000. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0378375800001154>
- [218] A. van den Oord, N. Kalchbrenner, L. Espeholt, k. kavukcuoglu, O. Vinyals, and A. Graves, “Conditional image generation with pixelcnn decoders,” in *Advances in Neural Information Processing Systems 29*, D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, Eds. Curran Associates, Inc., 2016, pp. 4790–4798. [Online]. Available: <http://papers.nips.cc/paper/6527-conditional-image-generation-with-pixelcnn-decoders.pdf>
- [219] T. Salimans, A. Karpathy, X. Chen, and D. P. Kingma, “Pixelcnn++: A pixelcnn implementation with discretized logistic mixture likelihood and other modifications,” in *ICLR*, 2017.
- [220] X. Huang, M. Kwiatkowska, S. Wang, and M. Wu, “Safety verification of deep neural networks,” *CoRR*, vol. abs/1610.06940, 2016. [Online]. Available: <http://arxiv.org/abs/1610.06940>
- [221] J. Z. Kolter and E. Wong, “Provable defenses against adversarial examples via the convex outer adversarial polytope,” *CoRR*, vol. abs/1711.00851, 2017. [Online]. Available: <http://arxiv.org/abs/1711.00851>

- [222] A. Raghunathan, J. Steinhardt, and P. Liang, “Certified defenses against adversarial examples,” *CoRR*, vol. abs/1801.09344, 2018. [Online]. Available: <http://arxiv.org/abs/1801.09344>
- [223] D. Clevert, T. Unterthiner, and S. Hochreiter, “Fast and accurate deep network learning by exponential linear units (elus),” in *4th International Conference on Learning Representations, ICLR 2016, San Juan, Puerto Rico, May 2-4, 2016, Conference Track Proceedings*, 2016. [Online]. Available: <http://arxiv.org/abs/1511.07289>
- [224] O. Ronneberger, P. Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” in *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015*, N. Navab, J. Hornegger, W. M. Wells, and A. F. Frangi, Eds. Cham: Springer International Publishing, 2015, pp. 234–241.
- [225] P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol, “Extracting and composing robust features with denoising autoencoders,” 2008, pp. 1096–1103.
- [226] Y. Bengio, G. Mesnil, Y. Dauphin, and S. Rifai, “Better mixing via deep representations,” in *Proceedings of the 30th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, S. Dasgupta and D. McAllester, Eds., vol. 28, no. 1. Atlanta, Georgia, USA: PMLR, 17–19 Jun 2013, pp. 552–560. [Online]. Available: <http://proceedings.mlr.press/v28/bengio13.html>
- [227] A. Buades, B. Coll, and J.-M. Morel, “A non-local algorithm for image denoising,” in *Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’05) - Volume 2 - Volume 02*, ser. CVPR ’05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 60–65. [Online]. Available: <http://dx.doi.org/10.1109/CVPR.2005.38>
- [228] C. Tomasi and R. Manduchi, “Bilateral filtering for gray and color images,” in *Proceedings of the Sixth International Conference on Computer Vision*, ser. ICCV ’98. Washington, DC, USA: IEEE Computer Society, 1998, pp. 839–. [Online]. Available: <http://dl.acm.org/citation.cfm?id=938978.939190>
- [229] E. Candès and B. Recht, “Exact matrix completion via convex optimization,” *Commun. ACM*, vol. 55, no. 6, pp. 111–119, Jun. 2012. [Online]. Available: <http://doi.acm.org/10.1145/2184319.2184343>
- [230] R. Mazumder, T. Hastie, and R. Tibshirani, “Spectral regularization algorithms for learning large incomplete matrices,” *J. Mach. Learn. Res.*, vol. 11, pp. 2287–2322, Aug. 2010. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1756006.1859931>
- [231] S. Chatterjee, “Matrix estimation by universal singular value thresholding,” *Ann. Statist.*, vol. 43, no. 1, pp. 177–214, 02 2015. [Online]. Available: <https://doi.org/10.1214/14-AOS1272>
- [232] 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>
- [233] Y. Zhang, K. Lee, and H. Lee, “Augmenting supervised neural networks with unsupervised objectives for large-scale image classification,” in *Proceedings of The 33rd International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, M. F. Balcan and K. Q. Weinberger, Eds., vol. 48. New York, New York, USA: PMLR, 20–22 Jun 2016, pp. 612–621. [Online]. Available: <http://proceedings.mlr.press/v48/zhangc16.html>
- [234] J. R. Gardner, M. J. Kusner, Y. Li, P. Upchurch, K. Q. Weinberger, and J. E. Hopcroft, “Deep manifold traversal: Changing labels with convolutional features,” *CoRR*, vol. abs/1511.06421, 2015. [Online]. Available: <http://arxiv.org/abs/1511.06421>
- [235] Y. Gal and Z. Ghahramani, “Dropout as a bayesian approximation: Representing model uncertainty in deep learning,” in *Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48*, ser. ICML’16. JMLR.org, 2016, pp. 1050–1059. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3045390.3045502>

- [236] A. Buades, B. Coll, and J.-M. Morel, “Non-Local Means Denoising,” *Image Processing On Line*, vol. 1, pp. 208–212, 2011.
- [237] L. van der Maaten and G. Hinton, “Visualizing data using t-SNE,” *Journal of Machine Learning Research*, vol. 9, pp. 2579–2605, 2008. [Online]. Available: <http://www.jmlr.org/papers/v9/vandermaaten08a.html>
- [238] F. Tramèr, N. Papernot, I. J. Goodfellow, D. Boneh, and P. D. McDaniel, “The space of transferable adversarial examples,” *CoRR*, vol. abs/1704.03453, 2017. [Online]. Available: <http://arxiv.org/abs/1704.03453>
- [239] C. Etmann, S. Lunz, P. Maass, and C.-B. Schönlieb, “On the connection between adversarial robustness and saliency map interpretability,” *arXiv preprint arXiv:1905.04172*, 2019.
- [240] R. Geirhos, P. Rubisch, C. Michaelis, M. Bethge, F. A. Wichmann, and W. Brendel, “Imagenet-trained CNNs are biased towards texture; increasing shape bias improves accuracy and robustness.” in *International Conference on Learning Representations*, 2019. [Online]. Available: <https://openreview.net/forum?id=Bygh9j09KX>
- [241] T. Zhang and Z. Zhu, “Interpreting adversarially trained convolutional neural networks,” in *Proceedings of the 36th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, K. Chaudhuri and R. Salakhutdinov, Eds., vol. 97. Long Beach, California, USA: PMLR, 09–15 Jun 2019, pp. 7502–7511. [Online]. Available: <http://proceedings.mlr.press/v97/zhang19s.html>
- [242] N. Carlini, A. Athalye, N. Papernot, W. Brendel, J. Rauber, D. Tsipras, I. Goodfellow, A. Madry, and A. Kurakin, “On evaluating adversarial robustness,” *arXiv preprint arXiv:1902.06705*, 2019.
- [243] H.-T. D. Liu, M. Tao, C.-L. Li, D. Nowrouzezahrai, and A. Jacobson, “Beyond pixel norm-balls: Parametric adversaries using an analytically differentiable renderer,” in *International Conference on Learning Representations*, 2019. [Online]. Available: <https://openreview.net/forum?id=SJl2niR9KQ>