Using learned optimizers to make models robust to input noise

Luke Metz 1  Niru Maheswaranathan 1  Jonathon Shlens 1  Jascha Sohl-Dickstein 1  Ekin D. Cubuk 1

Abstract
State-of-the art vision models can achieve superhuman performance on image classification tasks when tested and training data come from the same distribution. However, when models are tested on corrupted images (e.g., due to scale changes, translations, or shifts in brightness or contrast), performance degrades significantly. Here, we explore the possibility of meta-training a learned optimizer that can train image classification models such that they are robust to common image corruptions. Specifically, we are interested in training models that are more robust to noise distributions not present in the training data. We find that a learned optimizer meta-trained to produce models which are robust to Gaussian noise trains models that are more robust to Gaussian noise at other scales compared to traditional optimizers like Adam. The effect of meta-training is more complicated when targeting a more general set of noise distributions, but led to improved performance on half of held-out corruption tasks. Our results suggest that meta-learning provides a novel approach for studying and improving the robustness of deep learning models.

1. Introduction
Modern deep learning algorithms are exceptional at interpolation. For example, they can achieve superhuman performance on image classification tasks when tested on the same distribution of images that they were trained on (Kapathy, 2011; Krizhevsky et al., 2012; Huang et al., 2018). When these models are evaluated on images that are even slightly perturbed, however, their performance often degrades catastrophically (Dodge & Karam, 2017; Hendrycks & Dietterich, 2019; Azulay & Weiss, 2018; Rosenfeld et al., 2018).

A common way of increasing the robustness of deep learning algorithms is to apply perturbations to images during training (Simard et al., 2003; Cubuk et al., 2018). Although models trained with certain image perturbations become more robust to the specific perturbations they were trained with, they remain vulnerable to most other kinds of noise distributions (Dodge & Karam, 2017; Hendrycks & Dietterich, 2019; Azulay & Weiss, 2018; Geirhos et al., 2018).

In this work, we explore the effects of the optimization algorithm on robustness. Specifically, we employ meta-learning to learn an optimizer designed specifically to produce models which perform well on corrupted images. The meta-learning framework consists of two nested learning problems. In the inner-problem, a learned, parametric optimizer trains a model, making use of gradients computed only on clean training data. The outer-problem involves training the parameters of the optimizer so that the model trained in the inner-loop has a low outer-loss. In this work, we employ outer-losses based on validation performance on corrupted images. We find that the learned optimizers produce models which are not only robust to the noise distribution used in outer-training, but, in some cases, are also more robust to additional noise distributions as well.

2. Methods
In this work we train task specific learned optimizers. Consider an inner-problem classifier with logits \( f(x; w) \), parameters \( w \), and input minibatch \( x \). In this work, \( f \) is a 4 layer CNN and \( x \) is a minibatch of data sampled from Cifar10 (Krizhevsky & Hinton, 2009). Training this model can be expressed recursively:

\[
\begin{align*}
    u^{(t+1)} &= u^{(t)} - U \left( \nabla_{w^{(t)}} l(y_{\text{train}}, f(x_{\text{train}}; w^{(t)})) \right), \\
    \text{where } y &\text{ are the prediction targets, and } l \text{ is the cross entropy loss.}
    \end{align*}
\]

(1)

where \( y \) are the prediction targets, and \( l \) is the cross entropy loss. The ellipses (\ldots) denote potential additional features passed to the update rule (e.g., momentum values). An example of an update function \( U \) is SGD, which can be expressed as: \( U_{\text{sgd}}(g; \alpha) = \alpha g \) where \( g \) is the gradient of the inner-loss, and the learning rate \( \alpha \) is the single outer-parameter. In this work, we introduce more complex update functions \( U_{\text{meta}}(g, \ldots; \theta) \) with many outer-parameters \( \theta \).

To evaluate inner-problem performance, we often use held out validation data. In this work, we additionally want to be robust to different kinds of corruptions. As such, to

---

1. Google Brain. Correspondence to: <lmetz@google.com>.

Presented at the ICML 2019 Workshop on Uncertainty and Robustness in Deep Learning. Copyright 2019 by the author(s).
compute the outer-objective at inner-iteration \( t \) we compute:
\[
l(y_{\text{valid}}, f(n(x_{\text{valid}}); \omega^{(t)})),
\]
where \( n(\cdot) \) is a function which injects noise. We emphasize that during outer-training of the optimizers, \( n(\cdot) \) is not used to train the inner-model, only to evaluate it through the outer-objective. In some experiments, we do apply the learned optimizer to noised data after it has been outer-trained.

To find the outer-parameters, \( \theta \), we optimize for performance of the meta-objective (noised validation loss) with a corruption chosen from the meta-training corruption set. In all experiments we employ truncated evolutionary strategies for training. While it is possible to use gradients, the estimators can be very high variance (Metz et al., 2018).

In this work, we parameterize our learned optimizer similar to (Metz et al., 2018), employing a small fully connected network that operates on each inner-parameter independently (with the exception of some cross parameter normalization, described in Appendix A.2). This parameterization leverages existing features from optimization (such as momentum at different scales (Lucas et al., 2018)) and is flexible enough to express common regularization techniques, such as weight decay or learning rate decay, since weight value and timestep are included as input features. See Appendix A for more information on the update rule parameterization and outer-training.

### 3. Related Work

Recent work highlights the contrast between the human visual system and artificial neural networks (ANN), by looking at commonplace corruptions of images. Geirhos et al. (2018) reports that CNN rely much more on texture than shape, relative to humans. They find that data augmentation via style transfer can help ANNs focus more on shape, which leads to improved robustness to the Common Corruptions Benchmark (Hendrycks & Dietterich, 2019). Dodge & Karam (2017) report that while ANNs and humans perform comparably well on clean, high quality images; ANNs perform significantly worse on distorted images. They also report that errors made by humans and ANNs show little correlation (though other work has found surprising similarities in errors (Elsayed et al., 2018)). Azulay & Weiss (2018) show that ANNs are not robust to geometric transformations of objects either, such as translations and scale changes.

On the other hand, Gilmer et al. (2018); Fawzi et al. (2018); Ford et al. (2019) show that robustness to commonplace corruptions and worst-case corruptions (such as adversarial examples (Szegedy et al., 2014)) are directly related. Cubuk et al. (2017) find that the sensitivity of ANNs to distortions at the input has a universal functional form across machine learning models, caused by a lack of correlation between outputs for different classes.

Meta-learning is a general term often used to describe learning some aspects of a learning algorithm. Early work in this area is from Schmidhuber (1987) which involves self-referential algorithms. Optimizer learning has been first been studied in (Bengio et al., 1990; 1992) and then advanced with more complex parametric update rules and inner-models (Andrychowicz et al., 2016; Chen et al., 2016; Li & Malik, 2017; Wichrowska et al., 2017; Bello et al., 2017; Metz et al., 2018). In this work, we target an objective (validation loss on a noised image distribution) different than that used at training time (training loss). This idea has been explored in the context of validation loss, (Metz et al., 2018) as well as in unsupervised learning (Metz et al., 2019) and in reinforcement learning (Houthooft et al., 2018).

### 4. Experiments

We perform experiments on two types of noise distributions. First, we explore a corruption distribution consisting of different amounts of Gaussian noise added to the input image. Second, we explore a noise distribution based on the (Hendrycks & Dietterich, 2019) corruption benchmark. We select an outer-train set of corruptions and test our method on held out corruptions. In all cases the inner-model, the model being trained by an optimizer, consists of a 4 layer CNN on Cifar10. All values reported are cross entropy loss calculated on test images.

To aid in clarity, we color code our experimental setup in Table 1. For both experiments we train a learned optimizer. Our contribution, shown in black, is a learned optimizer outer-trained to perform well on noised validation data. At evaluation time, we can assess performance by inner-training on either clean data (to match how it was outer-trained), or on noised data, and testing performance of the trained model on different noise distributions. For the corruption data, to help isolate the effects of a more powerful optimizer, and of outer-training to target model robustness, we employ a second learned optimizer (blue) where we outer-train targeting clean validation images.

For both experiments we include Adam (Kingma & Ba, 2014) baselines, with learning rate tuned over \( 10^{0.5n} \), \( n \in \mathbb{Z} \), outer-trained on both clean (solid), and noised (dashed) data matching the outer-training corruption distribution. To match standard hyperparameter tuning, we select the learning rate base on the target noise distribution, as opposed to the outer-train noise distribution.

#### 4.1. Gaussian Noise

In this section, we train a learned optimizer to perform well on validation images (scaled 0-1) that have 0.05 per pixel Gaussian noise added to them. In Figure 1a, we show outer-training curves. We find that our learned optimizer starts to
Using learned optimizers to make models robust to input noise

**Table 1.** List of different optimizers tested. Color denotes optimizer type. A learned optimizer outer-trained on noisy validation images, our method (black), a baseline learned optimizer following (Metz et al., 2018) (blue), and LR tuned Adam (red through orange). Solid lines denote evaluations by training a model on clean data, and then evaluating on a different noise distribution. Dashed lines denote evaluations when training on the outer-train noise distribution and evaluated on either the same, or different noise distribution.

![Table 1](image)

**Figure 1.** (a) Outer-training curves. Each point represents an average of 10 inner-training runs using the learned optimizer for 10k iterations. We plot average outer-loss over the course of inner-training. Horizontal lines denote the best of learning rate tuned Adam, inner-trained on clean data (solid), and Adam inner-trained on noisy data (dashed). (b) Test performance on 0.05 noised images (same as outer-train noise amount). Our learned optimizer on clean data outperforms both Adam on clean data (solid yellow), and Adam trained on noisy data (dashed yellow). (c) Test loss evaluated on varying amounts of noise. The model trained with the learned optimizer achieves a lower loss than all models trained with Adam at all noise scales. Solid lines denote clean data used for inner-training while dashed lines indicate training on 0.05 noised data. The vertical dashed line denotes the outer-training noise value.

Outperform the learning rate tuned Adam after 500 outer-iterations and Adam inner-trained on noisy data after 600 outer-iterations. In Figure 1b, we show inner-training of our learned optimizer evaluated on the noise distribution used at outer-training time. We present 2 baselines: first the learning rate tuned Adam trained on clean data, as well as the learning rate tuned Adam on the 0.05 noised-training data. We find that despite never seeing noised data at inner-training time, our learned optimizer can outperform Adam specifically trained at this noise level.

In Figure 1c we show outer-generalization outside the outer-training distribution. We present 2 settings of inner-training: training on clean data (solid) and 0.05 noised data (dashed). On clean data, our learned optimizer outperforms the clean Adam baselines but does not outperform Adam on noised data after 0.08 noise. When training on noised data, we find considerable improvements in robustness and outperform all other models. This is particularly surprising as this learned optimizer has never seen noised inner-training data at outer-training time. Ideally we would like the learned optimizer to outperform Adam when inner-trained on noisy data. While this is true for 0.05 noise, (solid black is lower than dashed yellow), this does not hold at higher noise levels.

**4.2. Novel corruption types**

In this section we explore the effects of transferring between different kinds of corruptions. We take the set of corruptions proposed in Hendrycks & Dietterich (2019), divide the set of the nine corruptions (excluding JPEG corruption) into an outer-train set consisting of 7 training corruptions (Gaussian noise, shot noise, impulse noise, defocus blur, zoom blur, brightness, and contrast), and an outer-test set consisting of 2 corruptions (frosted glass blur and fog). We outer-train only monitoring 2 train corruptions and the 2 test corruptions for computational reasons. In Figure 2, we show two of the better performing corruptions (frosted glass, and shot noise) and provide the other two (fog, and brightness) in Appendix B. As an additional baseline, to isolate the effect of having a better optimizer as opposed to an outer-training against a corruption objective, we also outer-train an optimizer targeting performance on clean validation images.

We find the performance of our learned optimizer varies dramatically across both the outer-train, and outer-test cor-
Using learned optimizers to make models robust to input noise

Figure 2. In each row we present a different corruption type. In top we show the outer-test corruption frosted glass blur, and in the bottom we show an outer-train corruption shot noise. In Column a, we show evaluations of a given optimizer against these corruptions over the course of outer-training. In Column b we perform inner-training of the previous two optimizers using both clean data (solid) and an inner-training set consisting of the same corruptions in the outer-training distribution (dashed). We find our learned optimizer outer-trained to be robust to corruption outperforms LR tuned Adam on clean data in both cases, but does not outperform inner-training on corrupted images (dashed lines). In Column c we show test performance after inner-training on clean data (solid) or noised data matching the meta-training corruption set (dashed). We then evaluate each model with different severities of the target corruption. We find our learned optimizer generalizes outside the severity region we outer-train on (severity 1-3) and outperforms Adam (red-orange) and the learned optimizer baseline (blue) on clean data. Once again we find the inner-training on noise data (dashed) dramatically increases performance with both Adam and our learned optimizers. In all cases, we only inner-train on the outer-train corruption distribution and not on the corruption being evaluated.

...ruptions. We find our learned optimizer outer-trained for robustness, when inner-trained on clean data outperformed both the baseline learned optimizer, and the Adam when also inner-trained on clean data in all cases except the brightness corruption. Once again we find inner-training on the outer-train corruption distribution helps dramatically for both Adam, and both learned optimizers. In the Appendix, we find for fog, and brightness, our baseline learned optimizer outperforms both our learned optimizer, and Adam.

5. Discussion

In this work we demonstrate the use of meta-learning to outer-train optimizers that produce robust classifiers. While small scale, we see our results as the first step towards achieving this goal in real world settings. In this work, we present two extremes of how to parameterize optimizers: our MLP learned optimizer, and the learning rate tuned Adam. The Adam parameterization used in this work is limited, as it isn’t able to make use of learning rate decay and regularizers like our learned optimizer. Designing better inductive biases and parameterizations for robustness on either end of the spectrum would be greatly beneficial. For example, the use of other regularizers (e.g. dropout), or data augmentation techniques would likely improve both our baseline and the learned optimizers.

In this work, we make the simplifying assumption for our learned optimizers that we are always inner-training on clean data. This choice defines a specific experimental paradigm. We outperform the hand designed optimizers in most cases when the hand designed optimizers abide by this paradigm (Adam trained on clean data, solid lines). When we break this experimental setup and train on noised data (dashed) we achieve much better performance with both Adam and our learned optimizers. Future work involves further exploring the impact of the training distribution on the meta-learning procedure. We could, for example, inner-train on a distribution of corruptions, train an optimizer to target a different set, and outer-test on a third set.

A limitation of meta-learning is the need for a distribution of corruptions. We have found the existing set of 9 corruptions presented in Hendrycks & Dietterich (2019) are quite different in nature. This makes outer-generalization to unseen corruptions challenging. Techniques such as meta-supervised learning (Hsu et al., 2018) could be used to build heuristic corruption types to train on with the hope that the learned optimizer would transfer.

Acknowledgements

We would like to thank Justin Gilmer for discussion on this project as well as the rest of the Brain Team.
Using learned optimizers to make models robust to input noise

References


A. Optimizer Details

We briefly give an overview of our optimizer training details. The optimizer used in this work is similar to that used in (Metz et al., 2018).

A.1. Inner-Model

The inner-model used in this work consists of a 4 layer convolutional neural network with ReLU activations. It contains hidden sizes of 32, 32, 64, 64 with strides 2, 2, 1, 1. All layers use a kernel size of 3. The final layer is meaned spatially then passed into a linear projection to 10 units. We use cross entropy loss to train.

When outer-training our learned optimizer, we use clean Cifar10 data rescaled to fall between 0-1. Note that at evaluation time (after the model has been outer-trained) we also inner-train on noised data.

A.2. Learned optimizer architecture

The learned optimizer consists of a 1 hidden layer MLP that is shared across all units. For each unit, we construct a feature vector containing a variety of features commonly used in hand designed optimizers (Wichrowska et al., 2017). These include the gradient values, momentum values at 5 timescales, (0.5, 0.9, 0.99, 0.999, 0.9999), the current weights, the log absolute value of the weights. These values are then normalized by the second moment of each feature across each tensor. We include time based features consisting of \( \sin(\frac{st}{\pi}) \) where \( t \) is the current inner-training iteration, and \( s \) is one of \([2, 10, 20, 100, 200, 1000] \). Additionally, a feature that is the log norm of each tensor value, and the log of the number of units in the tensor.

These features are all passed through a 1 hidden layer MLP with 32 units to produce 2 outputs: \( a, b \). We combine them to produce a step as follows: \( \Delta W = 0.001a\exp(0.001b) \). The form of this update can be thought of as learning a direction \( a \), and a log step length \( b \). We multiply by 0.001 to ensure that the initial step size is stable and so that we do not initialize in an unstable outer-loss regime.

A.3. Outer-training details

We outer-train on an asynchronous, batched distributed cluster containing 256 workers and a batch size of 256. Each worker performs partial truncations and sends gradient information to a centralized learner. A worker then synchronizes weights, and proceeds from where the previous truncation left off. To account and mitigate truncation bias, we use an increasing schedule of truncation length that starts at 100 and linearly increases to 10k over 5k outer-iterations. Note that we never actually train until completion in any of our experiments. To prevent artifacts arising from the truncation schedule, we jitter this truncation amount by 20% while training. If at any point the outer-loss is greater than 2 times the initial loss we stop the unroll, and reinitialize the inner-model randomly.

For a outer-gradient estimator, we make use of variational optimization. As shown in (Metz et al., 2018) we can use a reparametization based gradient (backprop through unrolled training), or a gradient based on evolutionary strategies, or the combination of the 2. In this work, we only use the evolutionary strategies based estimator as it uses less ram with our naive implementation and is thus easier to work with given our computing infrastructure. We expect using the combined estimator would speed up outer-training. For lower variance evolutionary strategies gradients we make use of antithetical sampling with shared randomness where ever possible.

While progress has been made on increasing stability of learned optimizer training, not all random seeds converge. We use the outer-train loss to select the best model out of 4 random seeds for the corruptions experiments, and 3 random seeds for the Gaussian noise experiments.

A.4. Outer-training task distribution: Gaussian experiments

Our outer-objective for the Gaussian noise experiments consists of validation Cifar10 images corrupted with 0.05 Gaussian noise added to them.

A.5. Outer-training task distribution: Corruption experiments

Our outer-objective for the corruption experiments consists of sampling a severity amount, (1, 2, or 3), and a training corruption, (gaussian noise, shot noise, impulse noise, defocus blur, zoom blur, brightness and contrast). Each inner-training we sample a new augmentation to compute the meta-objective with.

B. Additional Corruption Plots
Using learned optimizers to make models robust to input noise

Figure 3. In each row we present a different corruption type. In top we show the outer-test corruption fog, and in the bottom we show an outer-train corruption brightness. In Column a, we show evaluations of a given optimizer against these corruptions over the course of outer-training. In Column b we perform inner-training of the previous two optimizers using both clean data (solid) and an inner-training set consisting of the same corruptions in the outer-training distribution (dashed). In Column c we show test performance after inner-training on clean data (solid) or noised data matching the meta-training corruption set (dashed). We then evaluate each model with different severities of the target corruption.