

Benchmarking Neural Network Robustness to Common Corruptions and Surface Variations

Dan Hendrycks*

University of California, Berkeley
hendrycks@berkeley.edu

Thomas G. Dietterich

Oregon State University
tgd@oregonstate.edu

Abstract

In this paper we establish new benchmarks for image classifier robustness. Our first benchmark, IMAGENET-C, standardizes and expands the corruption robustness topic, while showing which classifiers are preferable in safety-critical applications. Unlike recent robustness research, this benchmark evaluates performance on commonplace not worst-case adversarial corruptions. We find that there are negligible changes in relative corruption robustness from AlexNet to ResNet classifiers, and we discover ways to enhance corruption robustness. Then we propose a new dataset called ICONS-50 which opens research on a new kind of robustness, surface variation robustness. With this dataset we evaluate the frailty of classifiers on new styles of known objects and unexpected instances of known classes. We also demonstrate two methods that improve surface variation robustness. Together our benchmarks may aid future work toward networks that learn fundamental class structure and also robustly generalize.

1 Introduction

The human vision system is robust in ways that existing computer vision systems are not [2, 46]. Unlike current deep learning classifiers [34, 18, 52], the human vision system is not fooled by small changes in query images. Humans are also not confused by many forms of corruption such as snow, blur, pixelation, and novel combinations of these. Humans can even deal with abstract changes in structure and style. Achieving these kinds of robustness is an important goal for computer vision and machine learning. It is also essential for creating deep learning systems that can be deployed in safety-critical applications.

Most work on robustness in deep learning methods for vision has focused on the important challenges of adversarial example robustness [49, 5, 6] and data poisoning robustness [20, 48]. In contrast, we develop and validate datasets for two other forms of robustness. Specifically, we introduce the IMAGENET-C dataset for input *corruption robustness* [51] and the ICONS-50 dataset for *surface variation robustness*. These new challenges can be overcome by future networks which learn representations that track the fundamental structure of the classes.

To create IMAGENET-C, we introduce a set of 75 common visual corruptions and apply them to the ImageNet object recognition challenge [9]. We hope that this will serve as a general dataset for benchmarking robustness to image corruptions and prevent methodological problems such as moving goal posts and result cherry picking. We evaluate the performance of current deep learning systems and show that there is wide room for improvement on IMAGENET-C. We also introduce methods and architectures that improve robustness on IMAGENET-C without losing accuracy.

We then benchmark surface variation robustness. In this setting the fundamental class structure is unchanged, but the object’s surface-level statistics and superficial aspects vary but are not corrupted. To benchmark surface variation robustness, we introduce the ICONS-50 dataset. This dataset is intended to support research on robustness to surface variations such as the introduction of new styles and novel animal species. We then describe two methods that improve surface variation robustness. Our aim is that defining and benchmarking surface variation robustness and corruption robustness

*Work done while at OSU.

will lead to classifiers which do not heavily rely on image cues inessential to the object’s class and also generalize to new data.

2 Related Work

Adversarial Examples. An adversarial image is a clean image perturbed by a small corruption so as to confuse a classifier. These deceptive corruptions can occasionally fool black-box classifiers [35]. Algorithms have been developed that search for the smallest corruption in RGB space that is sufficient to confuse a classifier [8]. Thus adversarial corruptions serve as type of worst-case analysis for network robustness. Its popularity has often led “adversarial robustness” to become interchangeable with “robustness” in the literature [3, 45]. In efforts to ground adversarial robustness research, several competing robustness measures have been introduced [3, 7, 8, 40, 30]. New defenses [39, 43, 41, 19] quickly succumb to new attacks [13, 5, 6].

Robustness in Speech. Speech recognition research emphasizes robustness to common corruptions over worst-case, adversarial corruptions [36, 42]. Common acoustic corruptions (e.g., street noise, background chatter, wind) receive greater focus than adversarial audio, because common corruptions are ever-present and unsolved. There are several popular datasets containing noisy test audio [22, 21]. Robustness in noisy environments requires robust architectures, and some research finds convolutional networks more robust than fully connected networks [1]. Additional robustness has been achieved through pre-processing techniques such as standardizing the statistics of the input [37, 50, 17, 32].

ConvNet Fragility Studies. Several studies demonstrate the fragility of convolutional networks on simple corruptions. For example, Hosseini, Xiao, and Poovendran [2017] use impulse noise to break Google’s Cloud Vision API. Using Gaussian noise and blur, Dodge and Karam [2017] demonstrate the superior robustness of human vision to convolutional networks, *even after networks are fine-tuned* on Gaussian noise or blur. Geirhos et al. [2017] compare networks to humans on noisy and elastically deformed images. They find that fine-tuning on specific corruptions does not generalize, and classification error patterns underlying network and human predictions are not similar. Others show that networks fail to generalize to images deformed by slight geometric transformations [2].

Robustness Enhancements. In an effort to reduce classifier fragility, Vasiljevic, Chakrabarti, and Shakhnarovich [2016] fine-tune on blurred images. They find it is not enough to fine-tune on one type of blur to generalize to other blurs. Furthermore, fine-tuning on several blurs can marginally decrease performance. Zheng et al. [2016] also find that fine-tuning on noisy images can cause underfitting, so they encourage the noisy image softmax distribution to match the clean image softmax. Dodge and Karam [2017] address underfitting via an ensemble. They fine-tune each network on one corruption and classify with an mixture of these corruption-specific experts, though they do not assess combinations of known corruptions.

3 The IMAGENET-C Corruption Robustness Benchmark

3.1 The IMAGENET-C Dataset

IMAGENET-C Design. Our corruption robustness benchmark consists of 15 diverse corruption types, exemplified in Figure 1. The benchmark covers noise, blur, weather, and digital categories. Research that improves performance on this benchmark should indicate general robustness gains, as the corruptions are varied and great in number. These 15 corruption types each have five different levels of severity, since corruptions can manifest themselves at varying intensities. The Supplementary Materials gives an example of a corruption type’s five different severities. Real-world corruptions also have variation even at a fixed intensity. To simulate these, we introduce variation for each corruption when possible. For example, each fog cloud is unique to each image. These algorithmically generated corruptions are applied to the ImageNet [9] validation images to produce our corruption robustness dataset IMAGENET-C. The dataset can be downloaded or re-created by visiting <https://github.com/hendrycks/robustness>. Our benchmark tests networks with IMAGENET-C images, *but networks do not train on these images*. Networks are trained with datasets such as ImageNet but not IMAGENET-C. To enable further experimentation, we also designed an extra corruption for each noise, blur, weather, or digital category. Extra corruptions are depicted and explicated in the Supplementary Materials and also available at the aforementioned URL. Even more experimentation is possible by applying these distortions to other images, such as those from Places365. We find

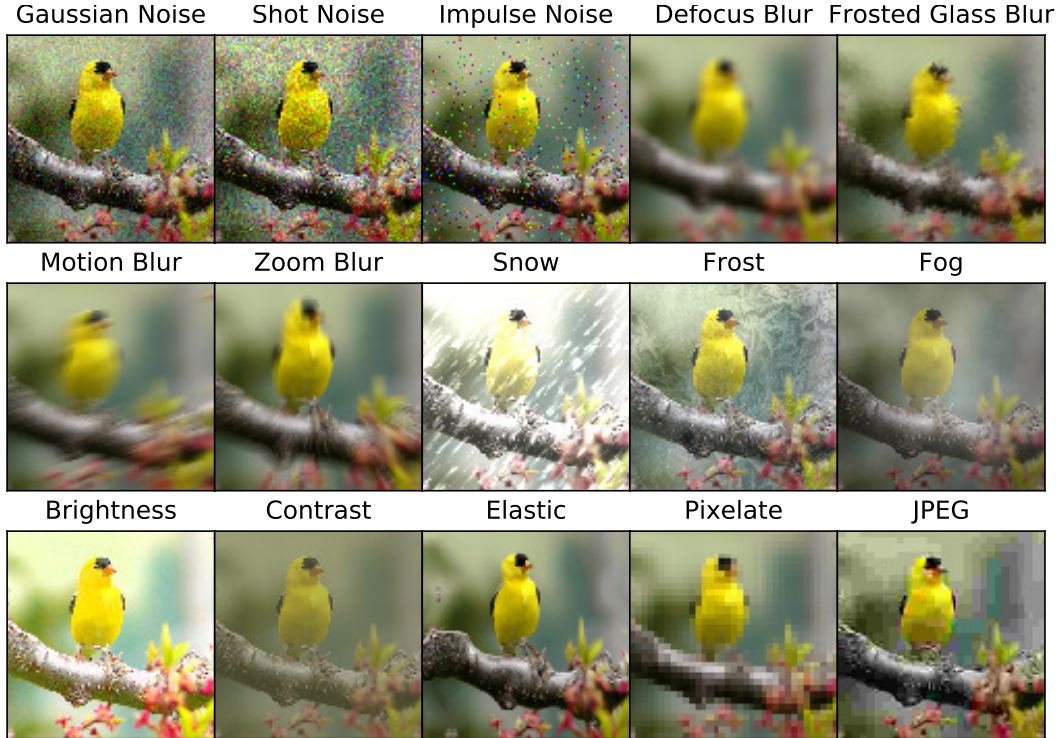


Figure 1: Our IMAGENET-C dataset consists of 15 types of algorithmically generated corruptions from noise, blur, weather, and digital categories. Each type of corruption has five levels of severity, resulting in 75 distinct corruptions. See different severity levels in the Supplementary Materials.

that applying these corruptions to 32×32 images and benchmarking on such small images is not predictive of corruption robustness on larger images. Overall, the dataset IMAGENET-C consists of 15 corruption types, each with five different severities, all applied to ImageNet validation images for testing a pre-existing network.

Common Corruptions. The first IMAGENET-C corruption is *Gaussian noise*. This corruption can appear in low-lighting conditions. *Shot noise*, also called Poisson noise, is electronic noise caused by the discrete nature of light itself. *Impulse noise* is a color analogue of salt-and-pepper noise and can be caused by bit errors. *Defocus blur* occurs when an image is out of focus. *Frosted Glass Blur* appears with “frosted glass” windows or panels. *Motion blur* appears when a camera is moving quickly. *Zoom blur* occurs when a camera moves toward an object rapidly. *Snow* is a visually obstructive form of precipitation. *Frost* forms when lenses or windows are coated with ice crystals. *Fog* shrouds objects and is rendered with the diamond-square algorithm. *Brightness* varies with daylight intensity. *Contrast* can be high or low depending on lighting conditions and the photographed object’s color. *Elastic* transformations stretch or contract small image regions. *Pixelation* occurs when upsampling a low-resolution image. *JPEG* is a lossy image compression format that increases image pixelation and introduces artifacts. Each corruption type is tested with depth due to its five severity levels, and this broad range of corruptions allows us to test model corruption robustness with breadth.

3.2 Metric and Setup

Mean and Relative Corruption Error. Common corruptions such as Gaussian noise can be benign or destructive depending on their severity. In order to *comprehensively* evaluate a classifier’s robustness to a given type of corruption, we score the classifier’s performance across five corruption severity levels and aggregate its scores. The first evaluation step is to take a pre-existing classifier here notated “Network,” which has not and will not train on IMAGENET-C, and then compute the clean dataset top-1 error rate. Denote this error rate $E_{\text{Clean}}^{\text{Network}}$. This same classifier will then test on an IMAGENET-C corruption type notated “Corruption.” Let top-1 error rate for the Network classifier on Corruption with severity level s ($1 \leq s \leq 5$) be written $E_{s, \text{Corruption}}^{\text{Network}}$. The classifier’s aggregate

performance across the five severities of the corruption type Corruption is the Corruption Error, computed with the formula

$$CE_{\text{Corruption}}^{\text{Network}} = \sum_{s=1}^5 E_{s,\text{Corruption}}^{\text{Network}} / \sum_{s=1}^5 E_{s,\text{Corruption}}^{\text{AlexNet}}.$$

Different corruptions pose different levels of difficulty. For example, fog corruptions often obscure an object’s class more than Brightness corruptions. Thus to make Corruption Errors comparable across corruption types, we adjust for the difficulty by dividing by AlexNet’s errors. Now with commensurate Corruption Errors, we can summarize model corruption robustness by averaging the 15 Corruption Error values ($CE_{\text{Gaussian Noise}}^{\text{Network}}, CE_{\text{Shot Noise}}^{\text{Network}}, \dots, CE_{\text{JPEG}}^{\text{Network}}$). This results in the *mean CE* or *mCE* for short.

We now introduce a more nuanced corruption robustness measure. Consider a classifier that withstands most corruptions, so that the gap between the mCE and the clean data error is minuscule. Contrast this with a classifier with a low clean error rate that does not cope well with corruptions, which corresponds to a large gap between the mCE and clean data error. It is possible the former classifier has a larger mCE than the latter, despite the former degrading more gracefully in the presence of corruptions. The amount that the classifier declines on corrupted inputs is given by the formula

$$\text{Relative } CE_{\text{Corruption}}^{\text{Network}} = \left(\sum_{s=1}^5 E_{s,\text{Corruption}}^{\text{Network}} - E_{\text{Clean}}^{\text{Network}} \right) / \left(\sum_{s=1}^5 E_{s,\text{Corruption}}^{\text{AlexNet}} - E_{\text{Clean}}^{\text{AlexNet}} \right).$$

Averaging these 15 Relative Corruption Errors results in the *Relative mCE*. In short, the Relative mCE measures the relative robustness or the performance degradation when encountering corruptions.

Preserving Metric Validity. The goal of ImageNet-C is to evaluate the robustness of machine learning algorithms to novel forms of corruption. Humans are able to generalize to novel corruptions quite well. For example, they can easily deal with new Instagram filters. Hence, we propose the following protocol. The image recognition network should be trained on the ImageNet training set and on whatever other training sets the investigator wishes to include. However, the network should not be trained on any of the 75 corruptions that were used to generate IMAGENET-C. Then the resulting trained model should be evaluated on IMAGENET-C and the above metrics computed. We provide a separate set of additional corruptions that can be employed for training or validation prior to testing on IMAGENET-C (see Supplementary Materials).

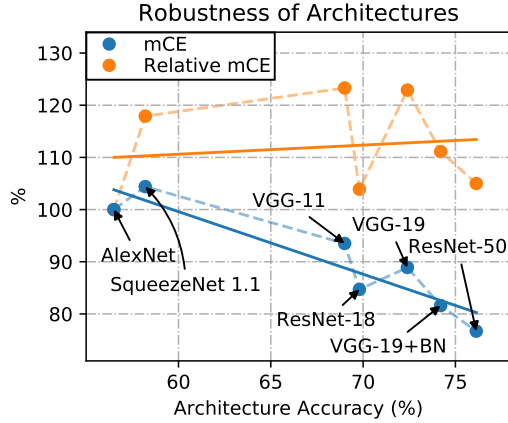


Figure 2: Robustness (mCE) and Relative mCE IMAGENET-C values. Relative mCE values suggest robustness in itself declined from AlexNet to ResNet. “BN” abbreviates Batch Normalization.

3.3 Architecture Robustness

How robust are current methods and has progress in computer vision been achieved at the expense of robustness? As seen in Figure 2, as architectures improve, so too does the mean Corruption Error (mCE). By this measure, architectures have become progressively more successful at generalizing to corrupted distributions. All Corruption Error values are in 1. Note that models with similar clean error rates have fairly similar CEs, and there are no large shifts in a corruption type’s CE. Consequently, it would seem that architectures have slowly and consistently improved their representations over time. However, it appears that robustness improvements are mostly explained by accuracy improvements. Recall that the Relative mCE tracks a classifier’s accuracy decline in the presence of corruptions. Figure 2 shows that the Relative mCE is worse than that of AlexNet [34]. In consequence, from AlexNet to ResNet [18], robustness in itself has barely changed. Relative robustness remains near AlexNet-levels and therefore below human-level, which shows that our “superhuman” classifiers are decidedly subhuman. We now apply IMAGENET-C to evaluate several methods for attempting to improve robustness to image corruption.

Network	Error	mCE	Noise			Blur				Weather				Digital			
			Gauss.	Shot	Impulse	Defocus	Glass	Motion	Zoom	Snow	Frost	Fog	Bright	Contrast	Elastic	Pixel	JPEG
AlexNet	43.5	100.0	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
SqueezeNet	41.8	104.4	107	106	105	100	103	101	100	101	103	97	97	98	106	109	134
VGG-11	31.0	93.5	97	97	100	92	99	93	91	92	91	84	75	86	97	107	100
VGG-19	27.6	88.9	89	91	95	89	98	90	90	89	86	75	68	80	97	102	94
VGG-19+BN	25.8	81.6	82	83	88	82	94	84	86	80	78	69	61	74	94	85	83
ResNet-18	30.2	84.7	87	88	91	84	91	87	89	86	84	78	69	78	90	80	85
ResNet-50	23.9	76.7	80	82	83	75	89	78	80	78	75	66	57	71	85	77	77

Table 1: Corruption Error and mCE values of different corruptions and architectures on IMAGENET-C. The mCE value is the mean Corruption Error of the corruptions in Noise, Blur, Weather, and Digital columns. All models are trained on clean ImageNet images, not IMAGENET-C images. Here “BN” abbreviates Batch Normalization [28].

3.4 Informative Robustness Enhancement Attempts

Stability Training. Stability training is a technique to improve the robustness of deep networks [53]. The method’s creators found that training on images corrupted with noise can lead to underfitting, so they instead propose minimizing the cross-entropy from the noisy image’s softmax distribution to the softmax of the clean image. The authors evaluated performance on images with subtle differences and suggested that the method provides additional robustness to JPEG corruptions. We fine-tune a ResNet-50 with stability training for five epochs. For train time corruptions, we corrupt images with uniform noise, where the maximum and minimum of the uniform noise is tuned over $\{0.01, 0.05, 0.1\}$, and the stability weight is tuned over $\{0.01, 0.05, 0.1\}$. Across all noise strengths and stability weight combinations, the models with stability training tested on IMAGENET-C had a larger mCEs than the baseline ResNet-50’s mCE. Even on unseen noise corruptions, stability training did not increase robustness. An upshot of this failure is that benchmarking robustness-enhancing techniques requires a diverse test set.

Image Denoising. An approach orthogonal to modifying model representations is to improve the inputs using image restoration techniques. Although *general* image restoration techniques are not yet mature, denoising restoration techniques are not. We thus attempt restore an image with the denoising technique called non-local means [4]. The amount of denoising applied is determined by the noise estimation technique of Donoho and Johnstone [1993]. Therefore clean images receive nearly no modifications from the restoration method, while noisy images should undergo considerable restoration. We found that denoising increased the mCE from 76.7% to 82.1%. A plausible account is that the non-local means algorithm slightly smoothed images even when images lacked noise, despite having the non-local means algorithm governed by the noise estimate. Therefore, the gains in noise robustness were wiped away by subtle blurs to images with other types of corruptions, showing that targeted image restoration can prove harmful for robustness.

Smaller Models. All else equal, “simpler” models often generalize better, and “simplicity” frequently translates to model size. Accordingly, smaller models may be more robust. We test this hypothesis with CondenseNets [24]. A CondenseNet attains its small size via sparse convolutions and pruned filter weights. An off-the-shelf CondenseNet ($C = G = 4$) obtains a 26.3% error rate and a 80.8% mCE. On the whole, this CondenseNet is slightly less robust than larger models of similar accuracy. Even more pruning and sparsification yields a CondenseNet ($C = G = 8$) with both deteriorated performance (28.9% error rate) and robustness (84.6% mCE). Here again robustness is worse than larger model robustness. Though models fashioned for mobile devices are smaller and in some sense simpler, this does not improve robustness.

3.5 Successful Corruption Robustness Enhancements

Histogram Equalization. Histogram equalization successfully standardizes speech data for robust speech recognition [50, 17]. For images, we find that preprocessing with Contrast Limited Adaptive Histogram Equalization [44] is quite effective. Unlike our previous image denoising attempt, CLAHE reduces the effect of some corruptions while not worsening performance on most others, thereby improving the mCE. We demonstrate CLAHE’s net improvement by taking a pre-trained ResNet-50 and fine-tuning the whole model for five epochs on images processed with CLAHE. The ResNet-50 has a 23.87% error rate, but ResNet-50 with CLAHE has an error rate of 23.55%. On nearly

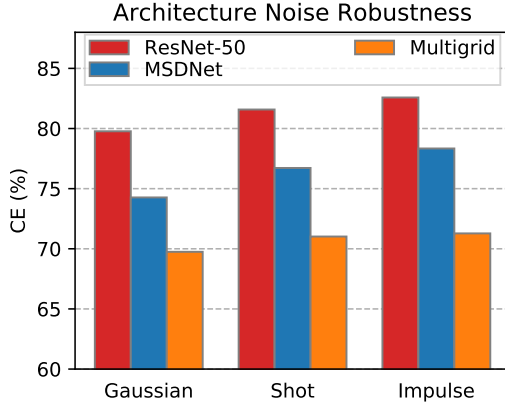


Figure 3: Architectures like Multigrid networks and DenseNets resist noise corruptions more effectively than ResNets.

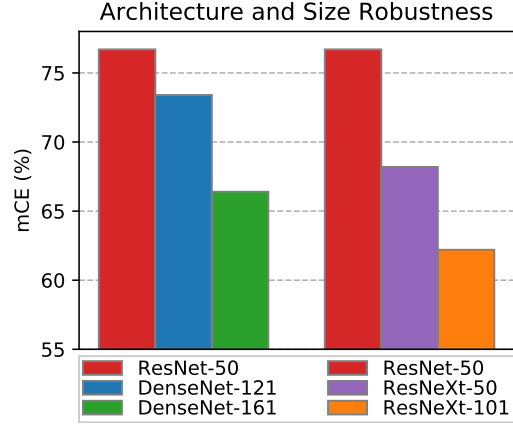


Figure 4: Larger feature aggregating networks achieve robustness gains that substantially outpace their accuracy gains.

all corruptions, CLAHE slightly decreases the Corruption Error. The ResNet-50 without CLAHE preprocessing has an mCE of 76.7%, while with CLAHE the ResNet-50’s mCE decreases to 74.5%.

Multiscale, Feature Aggregating, and Larger Networks. Multiscale architectures achieve greater robustness by propagating features across scales at each layer rather than slowly gaining a global representation of the input as in typical convolutional neural networks. Some multiscale architectures are called Multigrid Networks [31]. Multigrid networks each have a pyramid of grids in each layer which enables the subsequent layer to operate across scales. Along similar lines, Multi-Scale Dense Networks (MSDNets) [26] use information across scales. MSDNets bind network layers with DenseNet-like [25] skip connections. These two different multiscale networks both enhance robustness. Before comparing mCE values, we first note the Multigrid network has 24.6% top-1 error, as does the MSDNet, while the ResNet-50 has 23.9% top-1 error. On noisy inputs, Multigrid networks noticeably surpass ResNets and MSDNets, as shown in Figure 3. Since multiscale architectures have high-level representations processed in tandem with fine details, the architectures appear better equipped to suppress otherwise distracting pixel noise. When all corruptions are evaluated, ResNet-50 has an mCE of 76.7%, the MSDNet has an mCE of 73.6%, and the Multigrid network has an mCE of 73.3%.

Some recent models enhance the ResNet architecture by increasing what is called feature aggregation. Of these, DenseNets [25] and ResNeXts [52] are most prominent. Each purports to have stronger representations than ResNets, and the evidence is largely a hard-won ImageNet error-rate downtick. Interestingly, the IMAGENET-C mCE clearly indicates that DenseNets and ResNeXts have superior representations. Accordingly, a switch from a ResNet-50 (23.9% top-1 error) to a DenseNet-121 (25.6% error) decreases the mCE from 76.7% to 73.4%. More starkly, switching from a ResNet-50 to a ResNeXt-50 (22.9% top-1) drops the mCE from 76.7% to 68.2%. Results are summarized in Figure 4. This shows that corruption robustness may be a better way to measure future progress in object recognition than the clean dataset top-1 error rate.

Some of the greatest and simplest robustness gains sometimes emerge from making recent models more monolithic. Apparently more layers, more connections, and more capacity allow these massive models to operate more stably on corrupted inputs. We saw earlier that making models smaller does the opposite. Swapping a DenseNet-121 (25.6% top-1) with the larger DenseNet-161 (22.9% top-1) decreases the mCE from 73.4% to 66.4%. In a similar fashion, a ResNeXt-50 (22.9% top-1) is less robust than the a giant ResNeXt-101 (21.0% top-1); the mCEs are 68.2% and 62.2% respectively. Both model size and feature aggregation results are summarized in Figure 4. Consequently, future models with more depth, width, and feature aggregation may attain further robustness.

4 Surface Variation Robustness

An important goal for machine learning is to learn the essential structural elements of a class while being robust to unimportant surface variation. Whereas corruptions degrade the entirety of an image,



Figure 5: Image samples are from 12 of the 50 ICONS-50 classes. These images showcase the dataset’s high image quality, interclass and intraclass diversity, and its many styles.

surface variations cleanly alter the surface of an object and preserve the fundamental structure of the class. We developed the ICONS-50 dataset to test robustness to two forms of surface variation: style variation and subtype variation. Style variation is variation in artistic style that leaves the fundamental structure unchanged. Subtype variation is variation within a broad class (e.g., types of cats within the broad class of “cat”) where the subtypes all share essential characteristics of the broad class.

4.1 The ICONS-50 Dataset

The ICONS-50 dataset consists of 10,000 images belonging to 50 classes of icons (e.g., people, food, activities, places, objects, symbols, etc.) collected from different technology companies and platforms (e.g., Apple, Samsung, Google, Facebook, etc.). A full list of ICONS-50 classes is in the Supplementary Materials, and the dataset can be downloaded at <https://github.com/hendrycks/robustness>. A subset of ICONS-50 classes is shown in Figure 5. Each class has icons with different styles. For instance, icons with the thick, black outlines (like the bottom right “Drink” icon) are created by Microsoft. Other styles in the ICONS-50 dataset are from Apple, Samsung, Google, Facebook, and other platforms. The ICONS-50 dataset provides more icons per class (mean of 200) and more classes (50) than the logo datasets of Romberg et al. [2011] (32 classes, 70 logos per class) and of Joly and Buisson [2009] (37 classes and 53 logos per class).

We propose two protocols for evaluating surface variation robustness using the ICONS-50 dataset. For style robustness, the icons from one source (e.g., Microsoft) should be held out and the network trained on the remaining icons. Then the ability to generalize to the held out source can be measured by the classification accuracy of the held out icon source. For subtype robustness, we construct a training set by holding out 50 subtypes from ICONS-50. For example, we hold out the “duck” icons from the broad “Bird” class. Entire broad classes are not withheld, only a fraction of the subtypes within ICON-50’s 50 broad classes are withheld. The network is trained on the remaining icons and learns to classify broad classes. We evaluate the classifier’s subtype robustness by computing the broad class accuracy on the held out subtypes. These experiments are in the following section, and auxiliary experiments are in the Supplementary Materials.

4.2 Surface Variation Robustness Experiments with ICONS-50

Style Robustness. The ICONS-50 dataset has several styles like Microsoft’s flat vector graphics style and Apple’s realistic style. We aim to test the model’s robustness to an unseen style. To that end, we train a network on ICONS-50 while holding out Microsoft-styled icons. Microsoft-styled icons appear in all 50 classes, so each class is tested. Here, the metric for style robustness is simply the classifier’s accuracy on Microsoft-styled icons after the classifier trains on all other styles. That said,

we train a 20 layer ResNet, a 40 layer DenseNet ($L = 40, k = 24$), and a 29 layer ResNeXt ($8 \times 32d$) for 50 epochs with the cosine learning rate schedule [38] and Nesterov momentum. Icons are resized to 32×32 images. Like others, we use image mirroring and image cropping data augmentation. What we find is that the networks lack style robustness—the ResNet only obtains 58.3% accuracy on the held out Microsoft-styled icons, and the DenseNet and ResNeXt do worse with 48.5% and 51.8% accuracy, respectively. Clearly DenseNets and ResNeXts do not necessarily outperform ResNets as they did in the corruption robustness benchmark.

These results are not symptomatic of a training data shortage, rather a lack of robustness. The networks perform well if we instead use ICONS-50 for traditional classification rather than surface variation robustness. To do this, we hold out one version or rendition of icons that have multiple versions. For example, we hold out one version of the many Google-stylized “football” icons which have appeared across different versions of Android. By holding out one version for icons with many versions, the ResNeXt achieves 98.0% accuracy, the DenseNet obtains 97.3% accuracy, and the ResNet 97.2% accuracy. Thus the networks have enough data. With sub-60% accuracy on held out Microsoft-styled icons, the networks demonstrate a clear lacking in style robustness.

Subtype Robustness. Each ICONS-50 class has many subtypes, so we can treat each class as a broad class. We hold out 50 subtypes, train the classifier on the remaining subtypes to predict the broad class, and test the classifier’s accuracy on the held out subtypes. Then, we train a ResNet, DenseNet, and ResNeXt with the same training scheme from the style robustness experiment. After training, we find that classifier accuracies on these held out subtypes are again meager and that style robustness and subtype robustness indeed test different forms of robustness. This time the ResNet is worst, as it obtains only 57.5% accuracy on the held out subtypes. Meanwhile the DenseNet has 58.7% accuracy, and the ResNeXt has 60.0% accuracy. This indicates that the classifiers have wide room for subtype robustness improvement.

Enhancing Surface Variation Robustness. Multiscale networks can improve surface variation robustness not just corruption robustness. MSDNets [26] can process the whole image structure early in the forward pass, so that when the style changes while the fundamental structure is preserved, MSDNets can persevere better than other networks. In comparison to DenseNets, the network type most similar to MSDNets as both use dense connections, the MSDNet obtains 65.1% accuracy on the style robustness task while the DenseNet obtains only 48.5% accuracy. However, for subtype robustness, both networks differ by only a fraction of a percent in performance.

A method to improve both aspects of surface variation robustness is Shake-Shake regularization [14]. Shake-Shake regularization stochastically modulates the influence of each ResNeXt branch, so that the network can cope with unusual representations. Note we could not test shake-shake regularization’s effect on corruption robustness since contemporary GPUs do not have enough memory for shake-shake regularization applied to networks processing large-scale images. Now, the vanilla ResNeXt has 51.8% style robustness accuracy, but a ResNeXt with shake-shake regularization jumps to 76.0% accuracy. Subtype robustness also improves appreciably; the ResNeXt has 60.0% accuracy while the ResNeXt with shake-shake regularization has 63.6% accuracy. Clearly subtype robustness can be harder to improve than style robustness, but shake-shake regularization can improve both.

5 Conclusion

In this paper, we introduced what are to our knowledge the first benchmarks for corruption robustness and surface variation robustness. This was made possible by introducing two new datasets, IMAGENET-C and ICONS-50, the first of which showed that many years of architectural advancements corresponded to minuscule changes in relative robustness. Therefore benchmarking and improving robustness deserves attention, especially as top-1 accuracy nears its ceiling. We found that some methods harm corruption robustness, while methods such as histogram equalization, multiscale architectures, and larger models improve corruption robustness. Afterward, we opened research in surface variation robustness by defining style and subtype robustness. Here we found modern models to be fragile, but we also found that multiscale networks and highly regularized networks can noticeably enhance surface variation robustness. In this work, we had several findings, introduced novel experiments, and created new datasets for the rigorous study of model robustness, a pressing necessity as models are unleashed into safety-critical real-world settings.

References

- [1] Ossama Abdel-Hamid et al. “Applying Convolutional Neural Networks concepts to hybrid NN-HMM model for speech recognition.” In: *ICASSP* (2013).
- [2] Aharon Azulay and Yair Weiss. “Why do deep convolutional networks generalize so poorly to small image transformations?” In: *arXiv preprint* (2018).
- [3] Osbert Bastani et al. “Measuring Neural Net Robustness with Constraints”. In: *Advances in Neural Information Processing Systems* 29. Ed. by D. D. Lee et al. 2016.
- [4] Antoni Buades and Bartomeu Coll. “A non-local algorithm for image denoising”. In: *CVPR*. 2005.
- [5] Nicholas Carlini and David Wagner. *Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods*. 2017.
- [6] Nicholas Carlini and David Wagner. *Defensive Distillation is Not Robust to Adversarial Examples*. 2016.
- [7] Nicholas Carlini and David Wagner. *Towards Evaluating the Robustness of Neural Networks*. 2016.
- [8] Nicholas Carlini et al. *Ground-Truth Adversarial Examples*. 2017.
- [9] Jia Deng et al. “ImageNet: A Large-Scale Hierarchical Image Database”. In: *CVPR* (2009).
- [10] Samuel Dodge and Lina Karam. *A Study and Comparison of Human and Deep Learning Recognition Performance Under Visual Distortions*. 2017.
- [11] Samuel Dodge and Lina Karam. *Quality Resilient Deep Neural Networks*. 2017.
- [12] David Donoho and Iain Johnstone. “Ideal Spatial Adaptation by Wavelet Shrinkage”. In: *Biometrika* (1993).
- [13] Ivan Evtimov et al. *Robust Physical-World Attacks on Deep Learning Models*. 2017.
- [14] Xavier Gastaldi. “Shake-Shake Regularization”. In: *ICLR Workshop* (2017).
- [15] Leon Gatys, Alexander Ecker, and Matthias Bethge. “Image Style Transfer Using Convolutional Neural Networks”. In: *CVPR* (2016).
- [16] Robert Geirhos et al. *Comparing deep neural networks against humans: object recognition when the signal gets weaker*. 2017.
- [17] Mark Harvilla and Richard Stern. *Histogram-based subband powerwarping and spectral averaging for robust speech recognition under matched and multistyle training*. 2012.
- [18] Kaiming He et al. “Deep Residual Learning for Image Recognition”. In: *CVPR* (2015).
- [19] Dan Hendrycks and Kevin Gimpel. *Early Methods for Detecting Adversarial Images*. 2017.
- [20] Dan Hendrycks et al. “Using Trusted Data to Train Deep Networks on Labels Corrupted by Severe Noise”. In: *arXiv preprint arXiv:1802.05300* (2018).
- [21] Hans-Günter Hirsch. *Aurora-5 Experimental Framework for the Performance Evaluation of Speech Recognition in Case of a Hands-free Speech Input in Noisy Environments*. 2007.
- [22] Hans-Günter Hirsch and David Pearce. “The Aurora Experimental Framework for the Performance Evaluation of Speech recognition Systems Under Noisy Conditions”. In: *ISCA ITRW ASR2000* (2000).
- [23] Hossein Hosseini, Baicen Xiao, and Radha Poovendran. *Google’s Cloud Vision API Is Not Robust To Noise*. 2017.
- [24] Gao Huang et al. “CondenseNet: An Efficient DenseNet using Learned Group Convolutions”. In: *arXiv preprint* (2017).
- [25] Gao Huang et al. “Densely connected convolutional networks”. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2017.
- [26] Gao Huang et al. “Multi-Scale Dense Networks for Resource Efficient Image Classification”. In: *ICLR* (2018).
- [27] Xun Huang and Serge Belongie. “Arbitrary Style Transfer in Real-time with Adaptive Instance Normalization”. In: *ICCV* (2017).
- [28] Sergey Ioffe and Christian Szegedy. “Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift”. In: *JMLR* (2015).
- [29] Alexis Joly and Olivier Buisson. “Logo Retrieval with A Contrario Visual Query Expansion”. In: *ACM International Conference on Multimedia Retrieval* (2009).

- [30] Guy Katz et al. “Towards Proving the Adversarial Robustness of Deep Neural Networks”. In: *arXiv preprint* (2017).
- [31] Tsung-Wei Ke, Michael Maire, and Stella X. Yu. *Multigrid Neural Architectures*. 2017.
- [32] Chanwoo Kim and Richard M. Stern. “Power-normalized Cepstral Coefficients (PNCC) for Robust Speech Recognition”. In: *IEEE/ACM Trans. Audio, Speech and Lang. Proc.* 24.7 (July 2016), pp. 1315–1329. ISSN: 2329-9290.
- [33] Alex Krizhevsky. *Learning multiple layers of features from tiny images*. Tech. rep. 2009.
- [34] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. “ImageNet Classification with Deep Convolutional Neural Networks”. In: *NIPS* (2012).
- [35] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. “Adversarial Machine Learning at Scale”. In: *ICLR* (2017).
- [36] Jinyu Li et al. “An Overview of Noise-Robust Automatic Speech Recognition”. In: vol. 22. IEEE – Institute of Electrical and Electronics Engineers, 2014, pp. 745 –777.
- [37] Fu-Hua Liu et al. “Efficient Cepstral Normalization for Robust Speech Recognition”. In: *Proc. of DARPA Speech and Natural Language Workshop*. 1993.
- [38] Ilya Loshchilov and Frank Hutter. *SGDR: Stochastic Gradient Descent with Warm Restarts*. 2017.
- [39] Jiajun Lu et al. *Standard detectors aren’t (currently) fooled by physical adversarial stop signs*. 2017.
- [40] Aleksander Madry et al. *Towards Deep Learning Models Resistant to Adversarial Attacks*. 2018.
- [41] Jan Hendrik Metzen et al. *On Detecting Adversarial Perturbations*. 2017.
- [42] Vikramjit Mitra et al. *Robust features in Deep Learning based Speech Recognition*. 2017.
- [43] Nicolas Papernot et al. *Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks*. 2017.
- [44] Stephen M. Pizer et al. “Adaptive histogram equalization and its variations”. In: *Computer Vision, Graphics, and Image Processing* (1987).
- [45] Jonas Rauber, Wieland Brendel, and Matthias Bethge. *Foolbox v0.8.0: A Python toolbox to benchmark the robustness of machine learning models*. 2017.
- [46] Benjamin Recht et al. “Do CIFAR-10 Classifiers Generalize to CIFAR-10?” In: *arXiv preprint* (2018).
- [47] Stefan Romberg et al. “Scalable Logo Recognition in Real-World Images”. In: *ACM International Conference on Multimedia Retrieval 2011* (2011).
- [48] Jacob Steinhardt, Pang Wei Koh, and Percy Liang. “Certified Defenses for Data Poisoning Attacks”. In: *NIPS* (2017).
- [49] Christian Szegedy et al. *Intriguing properties of neural networks*. 2014.
- [50] Ángel de la Torre et al. “Histogram equalization of speech representation for robust speech recognition”. In: *IEEE Signal Processing Society* (2005).
- [51] Igor Vasiljevic, Ayan Chakrabarti, and Gregory Shakhnarovich. *Examining the Impact of Blur on Recognition by Convolutional Networks*. 2016.
- [52] Saining Xie et al. “Aggregated Residual Transformations for Deep Neural Networks”. In: *CVPR* (2016).
- [53] Stephan Zheng et al. *Improving the Robustness of Deep Neural Networks via Stability Training*. 2016.

A Example of IMAGENET-C Severities



Figure 6: Pixelation modestly to markedly corrupts a fish, showing our benchmark’s varying severities.

In Figure 6, we show the Pixelation corruption type in its five different severities. Clearly, IMAGENET-C corruptions can range from negligible to pulverizing. Because of this, the benchmark comprehensively assesses each corruption type.

B Extra IMAGENET-C Corruptions

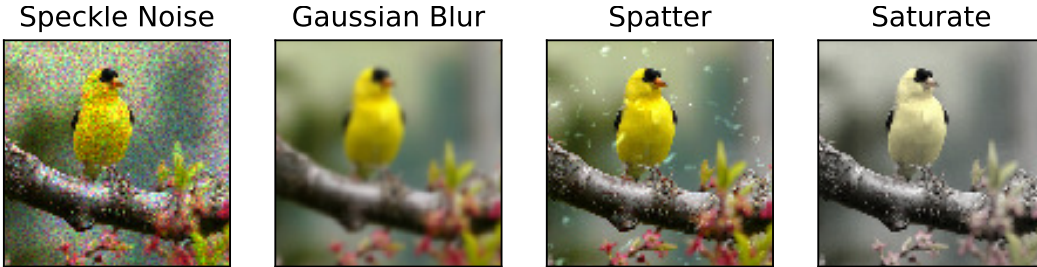


Figure 7: Extra IMAGENET-C corruption examples are available for model validation and sounder experimentation.

Directly fitting the types of IMAGENET-C corruptions is worth avoiding, as it would cause researchers to overestimate a model’s robustness. Therefore, it is incumbent on us to simplify model validation. For this reason, we provide extra corruptions that are available for download <https://github.com/hendrycks/robustness>. There is one corruption type for each noise, blur, weather, and digital category. The first corruption type is *speckle noise*, an additive noise where the noise added to a pixel tends to be larger if the original pixel intensity is larger. *Gaussian blur* is a low-pass filter where a blurred pixel is a result of a weighted average of its neighbors, and farther pixels have decreasing weight. *Spatter* can occlude a lens in the form of rain or mud. Finally, *saturate* is common in edited images where images are made more or less colorful. See Figure 7 for instances of each corruption type.

C Full Corruption Robustness Results

IMAGENET-C corruption relative robustness results are in Table 2. Since we use AlexNet errors to normalize Corruption Error values, we now specify the value $\frac{1}{5} \sum_{s=1}^5 E_{s, \text{Corruption}}^{\text{AlexNet}}$ for each corruption type. Gaussian Noise: 88.6%, Shot Noise: 89.4%, Impulse Noise: 92.3%, Defocus Blur: 82.0%, Glass Blur: 82.6%, Motion Blur: 78.6%, Zoom Blur: 79.8%, Snow: 86.7%, Frost: 82.7%, Fog: 81.9%, Brightness: 56.5%, Contrast: 85.3%, Elastic Transformation: 64.6%, Pixelate: 71.8%, JPEG: 60.7%, Speckle Noise: 84.5%, Gaussian Blur: 78.7%, Spatter: 71.8%, Saturate: 65.8%.

D 10-Crop Classification Fails to Enhance Robustness

Viewing an object at several different locations may give way to a more stable prediction. Having this intuition in mind, we perform 10-crop classification. 10-crop classification is executed by cropping all four corners and cropping the center of an image. These crops and their horizontal mirrors are

Network	Error	Rel. mCE	Noise			Blur				Weather				Digital			
			Gauss.	Shot	Impulse	Defocus	Glass	Motion	Zoom	Snow	Frost	Fog	Bright	Contrast	Elastic	Pixel	JPEG
AlexNet	43.5	100.0	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
SqueezeNet	41.8	117.9	118	116	114	104	110	106	105	106	110	98	101	100	126	129	229
VGG-11	31.0	123.3	122	121	125	116	129	121	115	114	113	99	86	102	151	161	174
VGG-19	27.6	122.9	114	117	122	118	136	123	122	114	111	88	82	98	165	161	172
VGG-19+BN	25.8	111.1	104	105	114	108	132	114	119	102	100	79	68	89	165	125	144
ResNet-18	30.2	103.9	104	106	111	100	116	108	112	103	101	89	67	87	133	97	126
ResNet-50	23.9	105.0	104	107	107	97	126	107	110	101	97	79	62	89	146	111	132

Table 2: Relative Corruption Errors and Relative mCE values of different corruptions and architectures on IMAGENET-C. All models are trained on clean ImageNet images, not IMAGENET-C images. Here “BN” abbreviates Batch Normalization.

processed through a network to produce 10 predicted class probability distributions. We average these distributions to compute the final prediction. Of course, a prediction informed by 10-crops rather than a single central crop is more accurate. Ideally, this revised prediction should be more robust too. However, the gains in mCE do not outpace the gains in accuracy on a ResNet-50. In all, 10-crop classification is a computationally expensive option which contributes to classification accuracy but not noticeably to robustness.

E Auxiliary Surface Variation Robustness Experiments

We repurpose the CIFAR-100 [33] and ImageNet-22K datasets for a closer investigation into subtype robustness. Both datasets have hierarchical taxonomies, so they have subtypes. Then we consider an inferior but informative synthetic test for style robustness.

CIFAR-100. The CIFAR-100 dataset has 20 broad classes, each with five subtypes. For this experiment, we hold out 1, 2, 3, or 4 subtypes from each broad class, train the classifier on the remaining subtypes while predicting the broad class, then test the classifier’s broad class accuracy on the held out subtypes. The classifier is a 40-2 Wide ResNet. We find the classifier broad class prediction error rate when we hold out 1, 2, 3, or 4 subtypes, and then we average these error rates. The average broad class prediction error rate with held out subtypes as inputs is 59.7%. In sharp contrast, the average broad class prediction error rate on subtypes known to the classifier is 13.2%. Like before there is a dearth of subtype robustness.

ImageNet-22K. Another natural image dataset with many classes but more data is ImageNet-22K, an ImageNet-1K superset. To define this subtype robustness experiment, we manually select 25 broad classes from ImageNet-22K, listed with their WordNet IDs in the Supplementary Materials. Each broad class has many subtypes. We call a subtype “seen” if and only if it is in ImageNet-1K and a subtype of one of the 25 broad classes. The subtype is “unseen” if and only if it is a subtype of the 25 broad classes and is from ImageNet-22K but not ImageNet-1K. Fortunately, pre-trained ImageNet-1K classifiers are readily available and have not trained on subtypes which should remain unseen. Therefore, we test subtype robustness by fine-tuning several pre-trained ImageNet-1K classifiers on seen subtypes so that they predict one of 25 broad classes. Their “seen” and “unseen” accuracies are shown in Figure 8, while the ImageNet-1K classification accuracy before fine-tuning is on the horizontal axis. Despite only having 25 classes and having trained on millions of images, these classifiers demonstrate a subtype robustness performance gap that should be far less pronounced.

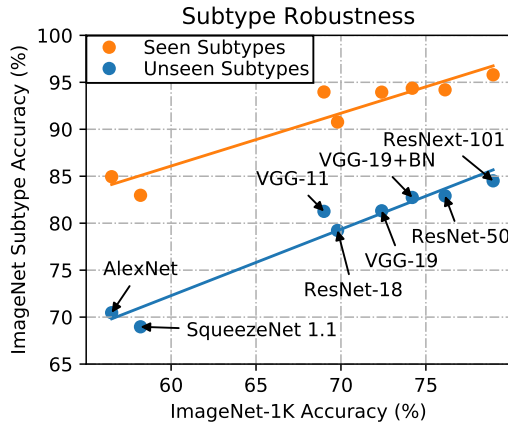


Figure 8: ImageNet classifiers and their robustness to unseen subtypes. Unseen subtypes of known broad classes are noticeably harder for classifiers.

For completeness, we list the 25 broad classes which we selected from ImageNet. Amphibian (n01627424), Appliance (n02729837), Aquatic Mammal (n02062017), Bird (n01503061), Bear (n02131653), Beverage (n07881800), Big cat (n02127808), Building (n02913152), Cat (n02121620), Clothing (n03051540), Dog (n02084071), Electronic Equipment (n03278248), Fish (n02512053), Footwear (n03380867), Fruit (n13134947), Fungus (n12992868), Geological Formation (n09287968), Hoofed Animal (n02370806), Insect (n02159955), Musical Instrument (n03800933), Primate (n02469914), Reptile (n01661091), Utensil (n04516672), Vegetable (n07707451), Vehicle (n04576211).

Style Transfer. Now we supplement our style robustness results with a lower quality, synthetic, yet informative experiment. Style transfer [15] provides a synthetic way to test style robustness by algorithmically and artificially recomposing the image in the style of another image. We test robustness to style transfer in the same way we tested robustness in our IMAGENET-C corruption benchmark. Therefore we corrupt ImageNet validation images with the style transfer method of Huang and Belongie [27]. Images are corrupted at five different severities where higher severities preserve less content and more strictly adhere to a randomly chosen target style. Improving style transfer robustness proves to be more difficult than improving IMAGENET-C performance. From AlexNet to ResNet-50, the mCE of IMAGENET-C distortions went from 100% to 76.7%, but the Corruption Error for style transfer only decreased from 100% to 92%. In fact, the ResNet-50 style transfer Corruption Error is higher than all IMAGENET-C Corruption Errors, and this holds for nearly all architectures tested. This again shows that current classifiers are not yet suited to surface variations such as stylization.

F Classes in ICONS-50

The 50 classes of ICONS-50 are as follows: Airplane, Arrow Directions, Ball, Biking, Bird, Blade, Boat, Books, Building, Bunny Ears, Cartwheeling, Clock, Cloud, Disk, Drink, Emotion Face, Envelope, Family, Fast Train, Feline, Flag, Flower, Footwear, Golfing, Hand, Hat, Heart, Holding Hands, Japanese Ideograph, Kiss, Lock, Mailbox, Marine Animal, Medal, Money, Monkey, Moon, Mountain, Numbers, Phone, Prohibit Sign, Star, Surfing, Tree, Umbrella, Vehicle, Water Polo, Worker, Wrestling, Writing Utensil.