Abstract—Deep neural networks (DNNs) are vulnerable to adversarial noises, which motivates the benchmark of model robustness. Existing benchmarks mainly focus on evaluating defenses, but there are no comprehensive studies of how architecture design and training techniques affect robustness. Comprehensively benchmarking their relationships is beneficial for better understanding and developing robust DNNs. Thus, we propose RobustART, the first comprehensive Robustness investigation benchmark on ImageNet regarding Architecture design (49 human-designed off-the-shelf architectures and 1200+ networks from neural architecture search) and Training techniques (10+ techniques, e.g., data augmentation) towards diverse noises (adversarial, natural, and system noises). Extensive experiments substantiated several insights for the first time, e.g., (1) adversarial training is effective for the robustness against all noises types for Transformers and MLP-Mixers; (2) given comparable model sizes and aligned training settings, CNNs > Transformers > MLP-Mixers on robustness against natural and system noises; Transformers > MLP-Mixers > CNNs on adversarial robustness; (3) for some light-weight architectures, increasing model sizes or using extra data cannot improve robustness. Our benchmark http://robust.art presents: (1) an open-source platform for comprehensive robustness evaluation; (2) a variety of pre-trained models to facilitate robustness investigation benchmark on ImageNet regarding architecture design and training techniques towards diverse noises; and (3) a new view to better understand the mechanism towards designing robust DNNs. We will continuously develop to this ecosystem for the community.

Index Terms—Model Robustness, Robustness Investigation Benchmark, Computer Vision.

1 INTRODUCTION

Deep neural networks (DNNs) have achieved remarkable performance across a wide range of applications [1], [2], [3]. However, DNNs are susceptible to adversarial examples [4], [5]; i.e., adding deliberately crafted perturbations imperceptible to humans could easily lead DNNs to wrong predictions, threatening both digital and physical deep learning applications [6], [7], [8], [9], [10], [11]. Besides, some prior works show that DNNs are also vulnerable to natural noises [12], [13], [14], [15]. These phenomena demonstrate that deep learning systems are not inherently secure and robust.

Since DNNs have been integrated into various safety-critical scenarios (e.g., autonomous driving, face recognition) [16], [17], [18], [19], improving model robustness and further constructing robust deep learning systems in practice is now growing in importance. Benchmarking the robustness of deep learning models paves a critical path to better understanding and further improving model robustness [20], [21], [22], [23]. Existing benchmarks focus on evaluating the performance of commonly used adversarial defense methods [24], [25], [26], [27], however, there are no comprehensive studies of how architecture design and general training techniques affect robustness. These factors reflect the inherent nature of model robustness, and slight differences may override the gains from the defenses [28], [29]. Thus, a comprehensive benchmark and study of the influence of architecture design and training techniques on robustness are highly important for understanding and improving the robustness of deep learning models.

In this work, we propose RobustART, the first comprehensive robustness benchmark on ImageNet regarding architecture design and training techniques towards diverse noise types. We systematically study over a thousand model architectures (49 prevalent human-designed off-the-shelf model architectures including CNNs [30], [31], [32], Transformers [33], [34], [35], and MLP-Mixers [36]; 1200+ architectures generated by Neural Architecture Search [37], [38], [39], [40], [41]) and 10+ mainstream training techniques (e.g., data augmentation, adversarial training, weight averaging, label smoothing, optimizer choices). To thoroughly study robustness against noises from different sources, we evaluate diverse noise types including adversarial noises [3], [24], natural noises (e.g., ImageNet-C [12], -P [12], -A [14], and -O [14]), and system noises [42] (see Table 1 for the top-5 robust architectures against different noises). Our large-scale experiments revealed several insights with respect to general model design for the first time: (1) for Transformers and MLP-Mixers, adversarial training is universally effective for improving the robustness against all types of noises (adversarial, natural, and system noises); (2) given comparable model sizes and aligned training settings, CNNs (e.g., ResNet) perform stronger on natural and system noises, while Transformers (e.g., ViT) are more robust on adversarial noises; and (3) for almost all model families, increasing model
capacity improves model robustness; however, increasing model sizes or adding extra data cannot improve robustness for some lightweight architectures.

Our contributions are as follows.

- **Comprehensive benchmark.** We provide the first comprehensive robustness benchmark on ImageNet, regarding architecture design and general training techniques. We investigate more than one thousand model architectures and 10+ training techniques on multiple noise types (adversarial, natural, and system noises).

- **Open-source framework.** We open-source our whole framework, which consists of a model zoo (100+ pre-trained models), an open-source toolkit, and all datasets (i.e., ImageNet with different noise types). The framework provides an open platform for the community, enabling comprehensive robustness evaluation.

- **In-depth analyses.** Based on extensive experiments, we revealed and substantiated several insights that reflect the inherent relationship between robustness and architecture design with different training techniques.

Our benchmark [http://robust.art/](http://robust.art/) provides an open-source platform and framework for comprehensive evaluations, better understanding of DNNs, and robust architectures design. Together with existing benchmarks on defenses, we could build a more comprehensive robustness benchmark and ecosystem involving more perspectives.

## 2 Background and Related Work

In this section, we provide a brief overview of existing work on adversarial attacks and defenses, as well as robustness benchmark and evaluation.

### 2.1 Adversarial attacks and defenses

Adversarial examples are inputs intentionally designed to mislead DNNs [4, 5]. Given a DNN $f_\Theta$ and an input image $x \in \mathbb{X}$ with the ground truth label $y \in \mathbb{Y}$, an adversarial example $x_{adv}$ satisfies

$$f_\Theta(x_{adv}) \neq y \quad \text{s.t.} \quad \|x - x_{adv}\| \leq \epsilon,$$

where $\| \cdot \|$ is a distance metric. Commonly, $\| \cdot \|$ is measured by the $f_p$-norm ($p \in [1, \infty]$).

In particular, adversarial attacks can be divided into two types: (1) white-box attacks, in which adversaries have the complete knowledge of the target model and can fully access it; and (2) black-box attacks, in which adversaries do not have full access to the target model and only have limited knowledge of it, e.g., can only obtain its prediction without knowing the architecture and weights. A plethora of work has been devoted to performing adversarial attacks [5, 43, 44, 45, 46, 47, 48]. Goodfellow et al. [5] first proposed the Fast Gradient Sign Method (FGSM) which leverages the gradient information of input image to craft adversarial examples efficiently. Madry et al. [24] proposed the Project Gradient Descent (PGD) attack that is similar with FGSM but iterates more steps to generate adversarial examples, after each step it projects noises to the $\epsilon$-ball around input images. Carlini & Wagner (C&W) attack [49] is an optimization-based attack that aims to find adversarial perturbations to minimize the specific object function. It transforms a general constrained optimization problem into minimizing an empirically-chosen object function. Universal Adversarial Perturbation (UAP) [50] aims to find the input-agnostic noises that could cause model misclassification when added on input images from various classes. AutoAttack [45] is one of the state-of-the-art adversarial attacks that combine four different attacks to form a parameter-free and computationally affordable attack to test adversarial robustness. It includes two extensions of PGD attack (APGD-CE and APGD-DLR) and two existing adversarial attacks (FAB attack [51] and Square Attack [52]) to further boost the strength of attack.

On the other hand, various defense approaches have been proposed to improve model robustness against adversarial examples [5, 24, 27, 53, 54, 55, 56, 57]. Specifically, adversarial training minimizes the worst case loss within some perturbation region for classifiers, by augmenting the training set $\{x^{(i)}, y^{(i)}\}_{i=1..n}$ with adversarial examples. Defensive Distillation [53] uses the change of softmax temperature to obfuscate the gradient information of model outputs and thus prevents the white-box attack from using gradient to generate adversarial examples. Zhang et al. [25] stated the trade-off between robustness and accuracy and proposed TRADES to defend adversarial attacks. TRADES introduces a regularization term to induce a shift of the decision boundaries away from the training data points. Kannan et al. proposed Adversarial Logit Pairing (ALP) [59] which not only minimizes the model prediction error on adversarial examples but also tries to minimize the distance of model logits between clean examples and the corresponding adversarial examples.

### 2.2 Robustness benchmark and evaluation

A number of works have been proposed to evaluate the robustness of deep neural networks [20, 21, 23, 60, 61, 62, 63, 64, 65, 66]. Su et al. [67] first investigated the adversarial robustness of 18 models on ImageNet. DEEPSPEC [21] is a platform for adversarial robustness analysis, which incorporates 16 adversarial attacks, 13 adversarial defenses, and several utility metrics. Carlini et al. [20] discussed the methodological foundations, reviewed commonly accepted best practices, and the suggested checklist for evaluating adversarial defenses. RealSafe [23] is another benchmark for evaluating adversarial robustness on image classification tasks (including 15 attacks and 16 defenses). Pang et al. [62] conducted a thorough empirical study of the training tricks of representative adversarial training methods to improve the robustness on CIFAR-10. More recently, RobustBench [68] is developed to track and evaluate the state-of-the-art adversarial defenses on CIFAR-10 and CIFAR-100.

Compared to existing benchmarks, our benchmark has the following characteristics: (1) comprehensive evaluation of different model architectures under aligned training settings and general training schemes over different architectures, while prior works focus on training schemes specialized for improving the performance against limited noise types, e.g., defenses against adversarial examples or common corruptions; (2) all noise types are based on ImageNet, while prior benchmarks mainly focus on image datasets of much smaller sizes, e.g., CIFAR-10 and CIFAR-100; and (3) systematic study of diverse noise types, while prior benchmarks mainly focus on evaluating adversarial robustness.
TABLE 1
Top-5 robust model architectures on ImageNet for different noises. For fair comparisons, we keep the aligned training settings for all architectures.

| Noise Type       | Datasets / Attacks | No.1                  | No.2                  | No.3                  | No.4                  | No.5                  |
|------------------|--------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Clean Images     | ImageNet           | ResNeXt-101           | WideResNet-101        | RegNetX-6400M         | ResNet-152            | Swin-B                |
| Adversarial Noises | AutoAttack-$\ell_\infty$ | VITAE-S              | VIT-B/32              | DeIT-B                | VIT-B/16              | VITAE-T               |
|                  | Worst-Case Adv     | VIT-B/32              | VITAE-S              | DeIT-B                | VIT-B/16              | MLP-Mixer L/16        |
| Natural Noises   | ImageNet-C         | ResNeXt-101           | WideResNet-101        | ResNet-152            | ResNet-101            | RepVGG-B3             |
|                  | ImageNet-P         | ResNeXt-101           | WideResNet-101        | ResNet-152            | RepVGG-B3             | ResNet-101            |
|                  | ImageNet-A         | Swin-B                | ResNeXt-101           | Swin-S                | RegNetX-6400M         | ResNet-152            |
|                  | ImageNet-O         | ResNeXt-101           | Swin-B                | Swin-T                | VITAE-S               | Swin-S                |
| System Noises    | ImageNet-S         | EfficientNet-B4       | DenseNet-201          | ResNeXt-50            | ResNeXt-101           | ResNet-152            |

3 ROBUSTNESS BENCHMARK ON ARCHITECTURE DESIGN AND TRAINING TECHNIQUES

Existing robustness benchmarks mainly evaluate adversarial defenses, and lack a comprehensive study of the effect of architecture design and general training techniques on robustness. These factors reflect the inherent nature of the model, and comprehensively benchmarking their effects on robustness lays the foundation for building robust DNNs. Therefore, we propose the first comprehensive robustness benchmark on ImageNet considering architecture design and training techniques.

3.1 Factors affecting robustness

Our main goal is to investigate the effects of two orthogonal factors on robustness, which are architecture design and training techniques. Therefore, we build a comprehensive repository containing: (1) models with different architectures, but trained with the same (aligned) techniques; and (2) models with the same architecture, but trained with different techniques. These fine-grained ablation studies enable a better understanding of how the core model design choices contribute to the robustness.

3.1.1 Architecture design

To conduct a thorough evaluation and explore the robustness trends of different architecture families, our repository tends to cover as many architectures as possible. As for the CNNs, we choose the classical large architectures including ResNet-series (ResNet, ResNeXt, WideResNet) and DenseNet, the lightweight ones including ShuffleNetV2 and MobileNetV2, the reparameterized architecture RepVGG, the NAS models including RegNet, EfficientNet and MobileNetV3, and sub-networks sampled from the BigNAS [39] supernet. As for the recently prevalent Vision Transformers, we reproduce ViT, DeIT, ViTAE, and Swin Transformer. Besides, we also include the MLP based architecture MLP-Mixer. All the models available are listed in Table 2. In total, we collect 49 human-designed off-the-shelf model architectures and sampled 1200 subnet architectures from the supernets. For fair comparisons of robustness, as for all human-designed off-the-shelf models we keep the aligned training technique setting (e.g., the same data augmentation techniques).

3.1.2 Training techniques

An increasing number of techniques have been proposed in recent years to train deep learning models with higher accuracy. Some of them have been proved to be influential for model robustness by previous literature [87], [88], [89], e.g., data augmentation. However, with investigations only on limited architectures and noise types, these conclusions might not be able to unveil the intrinsic nature behind. Besides, there are broader training techniques but their relationships with robustness are still ambiguous. To give more exact answers about the influence on robustness, we summarize 10+ mainstream training techniques into five different categories (see Table 3) and systematically benchmark their effects on robustness. The relevant pre-trained models using different training techniques are open-sourced.

3.2 Evaluation strategies

3.2.1 Dataset

For all of our experiments, we use the large-scale ImageNet-1K dataset [90], which contains 1,000 classes of colored images of size 224 * 224 with 1,281,167 training examples and 50,000 test instances.

3.2.2 Noise types

There exist various noise types in the real-world scenarios but most papers only consider a fraction of them (e.g., adversarial noises), which may fail to fully benchmark model robustness. This inspires us to collect diverse noise sources for a more comprehensive robustness profiling. As shown in Table 4, we categorize the noise format into three types: adversarial noise, natural noise, and system noise. The robustness of a model should take all these noises into consideration.

Adversarial noises. This type of noise is designed to attack DNNs. We choose 9 commonly-used adversarial attacks involving while-box attacks and black-box attacks with various $\ell_p$ perturbation types, including: FGSM [5], PGD-$\ell_\infty$ [24], AutoAttack-$\ell_\infty$ [91], MIM-$\ell_\infty$ [92], PGD-$\ell_2$ [24], DDN-$\ell_2$ [93], C&W-$\ell_\infty$ [99], PGD-$\ell_1$ [24] and transfer-based attack [94]. Each attack has 3 different perturbation magnitudes (small $\epsilon$, middle $\epsilon$, and large $\epsilon$). Specifically, for $\ell_1$ attacks we set large $\epsilon=1600.0$, middle $\epsilon=400.0$ and small $\epsilon=100.0$; for $\ell_2$ attacks we set large $\epsilon=8.0$, middle $\epsilon=2.0$ and small $\epsilon=0.5$; for $\ell_\infty$ attacks we set large $\epsilon=8/255$, middle...
### Table 2: Architecture repository.

| Category | Arch. Family | Archs |
|----------|--------------|-------|
| CNN      | ResNet [30]  | ResNet-18, ResNet-34, ResNet-50, ResNet-101, ResNet-152 |
|          | ResNetXNet [31] | ResNeXt-50-32x4d, ResNeXt-101-32x8d |
|          | WideResNet [32] | WRN-50-2, WRN-101-2 |
|          | DenseNet [33] | DenseNet-121, DenseNet-169, DenseNet-201 |
|          | ShuffleNetV2 [34] | ShuffleNetV2-x0.5, ShuffleNetV2-x1.0, ShuffleNetV2-x1.5, ShuffleNetV2-x2.0 |
|          | MobileNetV2 [35] | MobileNetV2-x0.5, MobileNetV2-x0.75, MobileNetV2-x1.0, MobileNetV2-x1.4 |
|          | RepVGG [36] | RepVGG-A0, RepVGG-B3 |
|          | RegNetX [37] | RegNetX-400M, RegNetX-800M, RegNetX-1600M, RegNetX-3200M, RegNetX-6400M |
|          | EfficientNet [38] | EfficientNet-B0, EfficientNet-B1, EfficientNet-B2, EfficientNet-B3, EfficientNet-B4 |
|          | MobileNetV3 [39] | MobileNetV3-x0.35, MobileNetV3-x0.5, MobileNetV3-x0.75, MobileNetV3-x1.0, MobileNetV3-x1.4 |
| Transformer | ViT [40] | ViT-B/16, ViT-B/32 |
|          | DeiT [41] | DeiT-Ti, DeiT-S, DeiT-B |
|          | ViTAE [42] | ViTAE-T, ViTAE-S |
|          | Swin Transformer [43] | Swin-T, Swin-S, Swin-B |
| MLP      | MLP-Mixer [44] | Mixer-B/16, Mixer-L/16 |

### Table 3: General training techniques.

| Category | Factors |
|----------|---------|
| Training Supervision | Knowledge Distillation [45], Self-supervised Training [46] |
| Weight Adjustment | Weight Averaging [47], Weight Re-parameterization [48] |
| Regularization | Label Smoothing [49], Dropout [50] |
| Training Data | Data Augmentation [51], Adversarial Training [52], Large-scale Pre-training [53] |
| Optimizer | SGD [54], AdamW [55] |

### Table 4: Characteristics of noise types.

| Noise Types | Adversarial Noise | Natural Noise | System Noise |
|-------------|-------------------|---------------|--------------|
| Model Dependent | ✓                  | x             | x            |
| Human Perceivable | x                  | ✓             | x            |
| Occurrence Frequency | Low               | High          | High         |
| Image Agnostic | x                  | ✓             | ✓            |
| Computational Cost | High              | Middle        | Low          |

$\epsilon=2/255$ and small $\epsilon=0.5/255$. See Section [E.3] and [F.3] in the supplementary materials for more details.

**Natural noises.** There are many formats of natural noises in the real world, and we choose four typical natural noise datasets (i.e., ImageNet-C, ImageNet-P, ImageNet-A, and ImageNet-O). See Section [E.3.2] in the supplementary materials for more details.

**System noises.** Besides, there always exists system noises in the training or inference stages for models deployed in the industry. Slight differences in pre-processing operations may cause different model performances. For example, different decoders (i.e., RGB and YUV) or resize modes (i.e., bilinear, nearest, and cubic scheme) would introduce system noises and in turn influence model robustness. Thus, we use the ImageNet-S dataset [42] to evaluate model robustness for system noises, which consists of 10 different industrial operations. See Section [E.3.3] in the supplementary materials for more details.

### 3.2.3 Metrics

**Adversarial Noise Robustness.** To evaluate the robustness against specific adversarial attacks, we use Adversarial Robustness (AR), which is based on commonly used Attack Success Rate (ASR) [55], [56], [57] and calculated by $1 - \text{ASR}$ (higher indicates stronger model). To evaluate the adversarial robustness under the union of different attacks, we use the Worst-Case Attack Robustness (WCAR), which indicates the lower bound of adversarial robustness against multiple adversarial attacks (higher indicates stronger model). The formal definitions are shown in Section [E.4.1] of the supplementary materials.

**Natural Noise Robustness.** For ImageNet-C, prior works [12] usually adopt mean Corruption Error (mCE) to measure model errors, thus we use $1 - \text{mCE}$ to measure the robustness for ImageNet-C (we call it ImageNet-C Robustness). For ImageNet-P, we follow the mean Flip Probability defined in [12] and take the negative of it (Negative mean Flip Probability, NmFP) as our metric. For ImageNet-A, we simply use the classification accuracy of models. For ImageNet-O, we follow [14] and use Area Under the Precision-Recall (AUPR). For the above 4 metrics, higher indicates a stronger model. Formal definitions are shown in Section [E.4.2] of the supplementary materials.

**System Noise Robustness.** For system noises, we use the accuracy to measure the robustness to different decode and resize modes. To further evaluate the model stability with different decode and resize methods, we use the standard deviation of accuracy across all combinations of these modes and take the negative of it (Negative Standard Deviation, NSD). The higher NSD of a model indicates the better tolerance of facing various combinations of system noises. See Section [E.4.3] of the supplementary materials for more details.

### 3.3 Framework

Our benchmark is built as a modular framework, which consists of 4 core modules (Models, Training, Noises, and Evaluation) and provides them in an easy-to-use way (see Figure 1). All the modules contained are highly extendable.
Fig. 1. Our benchmark is built as a modular framework, in which four core modules are provided for users in an easy-to-use way.

for users through API docs on our website. The benchmark is built on PyTorch [98] including necessary libraries such as Foolbox [99] and ART [100].

Models. We have collected 49 human-designed off-the-shelf models and their corresponding checkpoints (100+ pre-trained models in total), including ResNets, ViTs, MLP-Mixers, etc. Users could flexibly add their model architecture files, load weight configurations, and register their models in the framework to further study the robustness of the customized model architectures.

Training. We provide the implementations and interfaces of all training techniques mentioned in this paper. Users are also able to add customized training techniques to evaluate the robustness.

Noises. As for adversarial noises we provide 9 adversarial attacks including PGD-\(\ell_\infty\), AutoAttack-\(\ell_\infty\), FGSM, PGD-\(\ell_2\), MIM-\(\ell_\infty\), PGD-\(\ell_1\), DDN-\(\ell_2\), C&W-\(\ell_2\), and transfer-based attack; for natural datasets we provide ImageNet-C, ImageNet-P, ImageNet-O, and ImageNet-A; for system noises, we provide ImageNet-S. Users could simply generate corresponding perturbed images through our noise generation APIs. Moreover, users are also recommended to register new noise attack methods.

Evaluation. We provide various evaluation metrics, including WCAR, NmFP, mCE, AUPR, etc. Users are also recommended to add their own customized metrics through our APIs.

To sum up, based on our open-sourced benchmark, users could (1) conveniently use the source files to reproduce all the proposed results and conduct deeper analyses; (2) add new models, training techniques, noises, and evaluation metrics into the benchmark to conduct additional experiments through our APIs; (3) use our pre-trained checkpoints and research results for other downstream applications or as a baseline for comparisons.

4 EXPERIMENTS AND ANALYSES

4.1 Architecture design towards robustness

In this section, we first study the influence of architecture design on robustness. In particular, we divide this part into the analysis of human-designed off-the-shelf model architectures, and networks sampled by the neural architecture search.

4.1.1 Setup

Human-designed off-the-shelf architectures To conduct fair and rigorous comparisons among different model architectures, we keep the aligned training techniques for each human-designed off-the-shelf architecture. For optimizers, we use SGD [85] for all model families except for ViTs, DeiTs, ViTAEs, Swin Transformers, and MLP-Mixers; we use AdamW [86] for the rest of model families since Transformers and MLP-Mixers are highly sensitive to optimizers (using SGD would cause the failure of training [34]). For scheduler, we use cosine scheduler [101] with maximum training epoch=100 for all models. For data pre-processing, we use standard ImageNet training augmentation, which consists of the random resized crop, random horizontal flip, color jitter, and normalization. See Section F.1.1 of the supplementary materials for details.

Architectures sampled from NAS supernets We choose MobileNetV3, ResNet (basic block architecture), and ResNet (bottleneck block architecture) as the three typical NAS architectures to train the supernets using BigNAS. For optimizer,
we use SGD for all supernets; for scheduler, we use the cosine scheduler with maximum training epoch=100; for data preprocessing, we follow the settings for human-designed off-the-shelf architectures and use standard ImageNet training augmentation. For other hyper-parameters, we use label smooth and set batch size=512. More details are shown in Section 4.1.2 of the supplementary materials.

4.1.2 Human-designed off-the-shelf architectures
To study the effect of human-designed off-the-shelf model architectures on robustness, we choose 49 models from 15 most commonly used architecture families and keep the aligned training settings for each individual model. We report the model robustness against different noise types and standard performance (i.e., clean accuracy) w.r.t. model architectures. We use classical model floating-point operations (FLOPs) and model parameters (Params) to measure model sizes. For more results about the robustness and transferability maps with more attack magnitudes, please refer to Figure 16 and 17 in the supplementary material. As shown in Figure 16 and 17, we can draw observations as follows.

- **Model size (↑↓).** For most of the model families (e.g., ResNets, RegNetX), with the increase of the model size (e.g., FLOPs and Params), robustness for adversarial, natural, and system noises improves, and clean accuracy also increases. This indicates the positive influence of model capacity on robustness and task performance within the same model family. However, for some lightweight models such as MobileNetV2, MobileNetV3, and ShuffleNetV2, this conclusion does not entirely hold (i.e., larger models are not necessarily more robust than smaller models). It is even surprising that for EfficientNets, with the increase of the model size, the adversarial robustness decreases. We conjecture it may be due to the increase of input size (for EfficientNet family, the input size monotonically increases from EfficientNet-B0 to B7, e.g., the input size of EfficientNet-B0 is 224, B1 is 240, and B2 is 260).

- **Model architecture (↑↓).** Based on our large-scale experiments, we can find that the model architecture is a highly significant factor for robustness.

From a coarse-grained perspective, with comparable model sizes and aligned training settings, different model architectures yield significantly different robustness for the same noise. For example, WRN-101-2 and RepVGG-B3 have almost the same Params and clean accuracy performance, whereas their adversarial robustness differs to a large extent (e.g., 9.6 vs. 4.1 for worst-case attack robustness, 36.6 vs. 23.7 for PGD-$\ell_\infty$ robustness with $\epsilon=0.5/255$).

Specifically, we observe that when compared under the aligned training settings, ViT, ViTAE, and DeiT rank top-3 for worst-case attack robustness; for natural noise robustness, ResNeXt, WideResNet, ResNet rank top-3; for system noises, EfficientNet, DenseNet, ResNeXt rank top-3. Therefore, we could empirically reach the conclusion that with comparable sizes and aligned training settings, CNNs (e.g., ResNet) perform stronger on natural and system noises, while Transformers and MLP-Mixers are more robust against adversarial noises.

Moreover, it is interesting to find that although Swin Transformers are mainly based on the self-attention mechanism like ViTs and DeiTs, their robustness performance is more like CNNs. In other words, in contrast to ViTs, Swin Transformers are comparatively more robust to natural and system robustness, and less robust towards adversarial noises. Some mechanisms in Swin Transformers draw on properties of CNNs, such as window attention (introduce the locality like convolution kernel) and hierarchical architecture, thus we conjecture this might be the reason for the special robustness performance of Swin Transformers. We hope all these observations could inspire more in-depth future studies.

- **Adversarial transferability.** According to the experimental results, we mainly divide the model architectures into three categories: common CNNs (ResNet, ResNeXt, WideResNet, DenseNet, RegNetX, and RepVGG), lightweight CNNs (MobileNetV2, MobileNetV3, and ShuffleNetV2), and non-CNNs (ViTs, DeiTs, and MLP-Mixers). In most cases, models in each category are more robust against attacks transferred from other categories while less robust against attacks transferred from themselves. Interestingly, Swin Transformers and ViTAEs show “moderate” robustness (i.e., in contrast to other ViTs, Swin Transformers and ViTAEs are more robust against attacks transferred from other model families, and attacks generated from them also have stronger transferability to all other model families. We speculate that the design of Swin Transformers and ViTAEs has drawn the architecture properties from both CNNs and classical Transformers (e.g., multi-head attention, hierarchical architecture, feature pyramid).

- **Evaluation diversity.** The evaluation diversity plays an important role in evaluating robustness, and different evaluation noises may lead to different robustness evaluation results. For example, different noise types may yield different model robustness (e.g., Swin Transformer > ViT on natural noises, while Swin Transformer < ViT on adversarial noises); for the same noise type, different adversarial attacks may yield different robustness (e.g., ViT > ResNet on AutoAttack, but ViT < ResNet on FGSM); even given the same adversarial attack, different perturbation norms or budgets may still cause different results (e.g., for PGD-$\ell_\infty$ attack, DeiT > ResNetX when $\epsilon=0.5/255$, while DeiT < ResNetX when $\epsilon=2.0/255$; for EfficientNets under PGD attack, adversarial robustness increases with model size when the perturbation norm is $\ell_1$ and $\ell_2$, while decreases when the perturbation norm is $\ell_\infty$). See Figure 7 to 15 in the supplementary materials for more results.

4.1.3 Architectures sampled from NAS supernets
We then study the robustness of models sampled from BigNAS [39] supernet. Due to the flexibility of sampled subnets, we first study the effect of model size on robustness (we totally sampled 600 subnets from 3 supernets) and then dig into the detailed factors that affect robustness in a more fine-grained manner. Specifically, for each detailed factor (input size, convolution kernel size, model depth, and expand ratio), we fix other model factors and sample 50 subnets from each of the 3 supernets to evaluate robustness (600 subnets in total). As shown in Figure 16, we highlight the key findings below.

---

1. ↑ indicates that this factor has a positive correlation with model robustness, while ↓ indicates the opposite.
Fig. 2. Robustness on human-designed off-the-shelf architectures. (first line) from left to right: clean accuracy on standard ImageNet, WCAR (small magnitude) under all adversarial attacks, AR under PGD-ℓ∞ attack with ɛ=0.5/255, 1-mCE on ImageNet-C; (second line) from left to right: NmFP on ImageNet-P, accuracy on ImageNet-A, AUPR on ImageNet-O, and NSD on ImageNet-S. Results of different FLOPS are in Section G.7 of the supplementary materials. Results for different adversarial attacks with different magnitudes are shown in Figure G.8 to G.15 in the supplementary material.

Fig. 3. Transferability heatmap of human-designed off-the-shelf architectures under FGSM attack, ɛ=8/255. Values mean attack success rates (ASR) from a source model to a target model.

- **Model size** (↑). Within a specific supernet, increasing model size improves model robustness on adversarial (except for the lightweight supernet MobileNetV3, which is similar to conclusions in the human-designed model study) and natural noises, but there is no apparent effect on system noises. We hypothesize that for lightweight models, simply increasing their capacities cannot improve robustness.

- **Model depth** (↑). In all supernets, increasing the depth of the last stage (i.e., the number of layers in the subnets’ deepest block) could improve the adversarial robustness of the sampled subnets, which shows the deepest stage is of great importance for model robustness in NAS-sampled network. However, for the depth of other stages or the whole network, the relationship is still ambiguous.

- **Input size** (↓). In all supernets, when increasing the input size of sampled subnets, their adversarial robustness decreases. This observation is similar to the study on EfficientNets in Sec 4.1.2 indicating that networks with larger input sizes might be less robust against adversarial attacks. However, the effects of input size on robustness for natural and system noises are ambiguous.

- **Convolution kernel size** (↑). For sampled subnets,
increasing the total number of convolution kernel sizes in all stages could improve the adversarial robustness of subnets, while the effects on natural and system noises are unclear. For each stages’ convolution kernel size, there seems no correlation with model robustness.

To sum up, we found that the architecture design has a huge impact on robustness (especially the sizes and families). Meanwhile, the noise diversity is highly important to robustness evaluation (slight differences would cause opposite observations), we therefore recommend researchers to use more comprehensive and diverse noises when evaluating model robustness.

4.2 Training techniques towards robustness

4.2.1 Setup

In total, we choose 11 different training techniques, including weight averaging, label smoothing, ImageNet-21K pre-training, Mixup, Augmix, Dropout, weight re-parameterization, knowledge distillation, MOCO v2 self-supervised training, PGD-ℓ∞ adversarial training, and AdamW optimizer. In particular, for large-scale pre-training, we adopt ImageNet-21K as the pre-training data; for data augmentation, we select Mixup [85] and Augmix [82]; for adversarial training, we follow [60], [102] and adversarially train models with PGD-ℓ∞ attacks [24]; for self-supervised training, we use MoCo [28]. Due to the huge time consumption of training all models with or without these 11 training techniques on ImageNet, we choose several typical and widely-used architectures for each training technique (e.g., ResNet-50, RegNetX-3200M, RepVGG-A0, RepVGG-B3, ShuffleNetV2-x2.0, MobileNetV3-xl4, Vit-B/16, and Mixer-B/16). For each training technique, we either apply or disable this training technique for different model architectures with all other training settings being the same. We defer more details to Section 7 in the supplementary materials.

4.2.2 Results and analysis

We list some of the representative results in Figure 5, and well as the robustness against ImageNet-C and system we adopt ImageNet-21K as the pre-training data; for data augmentation, we select Mixup and Augmix for adversarial training, we follow [60], [102] and adversarially train models with PGD-ℓ∞ attacks; for self-supervised training, we use MoCo. Due to the huge time consumption of training all models with or without these 11 training techniques on ImageNet, we choose several typical and widely-used architectures for each training technique (e.g., ResNet-50, RegNetX-3200M, RepVGG-A0, RepVGG-B3, ShuffleNetV2-x2.0, MobileNetV3-xl4, Vit-B/16, and Mixer-B/16). For each training technique, we either apply or disable this training technique for different model architectures with all other training settings being the same. We defer more details to Section 7 in the supplementary materials.

4.3 Discussions

In contrast to existing studies that evaluate adversarial defenses, this paper aims to conduct a comprehensive and
fair robustness investigation of different architectures and training techniques. For architectures, we align different model architectures (including CNNs, Transformers, and MLP-Mixers) with the same training settings (without extra training techniques) for a fair comparison, which is often ignored by most existing literature. For training techniques, instead of studying one specific training technique with all its implementation tricks, we summarize and evaluate 10+ training techniques over several architectures to help better understand how training techniques will influence model robustness. Through extensive ablation studies (including eliminating the extra variables with an aligned training setting for comparing different model architectures), we comprehensively demonstrate how different model architectures and training techniques impact the robustness. Based on large-scale experiments and fair comparisons, we have obtained a wide variety of observations. In this section, we offer some of the most important and consistent ones and provide further discussions and analyses on them.

4.3.1 Adversarial training is universally effective for the robustness of Transformers and MLP-Mixers

During our analysis for the impact of training techniques on robustness in Sec 4.2, we follow the classical PGD-$\ell_\infty$ adversarial training scheme in [60], [102] and only feed adversarial examples into models in each mini-batch to conduct training. Based on this adversarial training scheme, we find that in contrast to CNNs, adversarially trained ViTs
and MLP-Mixers have a smaller clean accuracy drop and larger robustness improvement (even the natural and system robustness are improved), which indicates ViTs and MLP-Mixers perform better with adversarial training than CNNs.

To further investigate this observation, we follow [103] and use another PGD-$\ell_\infty$ adversarial training scheme to train models and evaluate their robustness. Specifically, we simultaneously feed clean examples and their corresponding adversarial examples in each mini-batch into models with a ratio of 1:1 (we call this scheme Half Adversarial Training). From the results in Table 5, we find that Half Adversarial Training could also largely increase the robustness of Transformers and MLP-Mixers towards all types of noises (i.e., adversarial, natural, and system noises). More importantly, we find that this adversarial training scheme could improve the accuracy of Transformers and MLP-Mixers on clean examples. However, Half Adversarial Training also decreases the accuracy of CNNs on clean examples, which indicates that adversarial training can be treated as a special technique for Transformers and MLP-Mixers to universally improve model performance if harnessed properly. We defer more results about Half Adversarial Training scheme in Figure 29 in the supplementary materials.

Note that, for all the above experiments for adversarial training, ViTs are adversarially trained based on our aligned training settings (i.e., without using extra training techniques, e.g., AutoAugment or Dropout). Therefore, we further evaluate the effect of adversarial training for ViTs under the optimal ViT training settings [54] (e.g., with Mixup, AutoAugment, etc.). In particular, we conduct Half Adversarial Training on a ViT-B/16 using the optimal setting and compare its robustness with another vanilla trained ViT-B/16 model under the same optimal setting. From the results in Table 6, we could reach similar observations, namely this adversarial training scheme could largely boost the robustness of ViT on all types of noises. In fact, we also conduct the standard PGD adversarial training (only feed adversarial examples into models in each mini-batch) for ViT-B/16 under the optimal settings, however, we observe that the model cannot converge. We speculate that it is too difficult for the model to fit the augmented adversarial examples since there have been various data augmentations in the optimal ViT training procedure [104].

Overall, to the best of our knowledge, we are the first to propose this conclusion through extensive experiments on ImageNet that adversarial training is universally effective for the robustness of Transformers and MLP-Mixers. We highly advocate researchers to use adversarial training to robustify their Transformers and MLP-Mixers in practice and further investigate the nature behind.

### 4.3.2 Vision transformers are more robust against adversarial noises while less robust against natural noises compared to CNNs under aligned settings

Some of the recent works [63], [64], [65], [66], [105] have already studied the adversarial or natural robustness of vision transformers, and reached various conclusions. For adversarial robustness, [63] shows that individual vision transformers are just as vulnerable as their CNN counterparts to white-box adversaries, while [65] and [64] both demonstrates that ViTs possess better adversarial robustness when compared with CNNs. For robustness against natural noises, [105] shows that a ViT with comparable parameters is more robust to image corruptions than the CNN trained with augmentations, and [65] shows that ViTs are more robust than CNNs under corruptions and OOD distributions.

However, as we can see from the above studies, some of their conclusions and observations are contradictory to others. We attribute this phenomenon to the unfair experimental settings and incomplete noises evaluation. For instance, most of the ViTs used in these works are trained with the standard settings for ViTs which consists of various specially-designed data augmentation techniques (e.g., AutoAugment and RandAugment), while they are not used for CNNs. Studies in [32] have revealed that data augmentation techniques could reduce adversarial robustness and improve natural robustness in most cases, therefore it will interfere with the correctness of model robustness evaluation when data augmentation techniques are introduced.

Therefore, in Sec. 4.1.2, we fairly evaluate the robustness of ViTs and other architectures (e.g., CNNs) under the aligned

| Architecture | Training Settings | Clean Accuracy | WCAR (large $\ell_\infty$) | WCAR (middle $\ell_\infty$) | WCAR (small $\ell_\infty$) | ImageNet-A Accuracy | ImageNet-O AUPR | ImageNet-C Robustness | ImageNet-P NmFP | ImageNet-S NSD |
|--------------|-------------------|----------------|--------------------------|--------------------------|--------------------------|---------------------|-----------------|----------------------|----------------|----------------|
| ViT-B/16     | Vanilla           | 66.662         | 0.000                    | 0.063                    | 22.259                   | 3.866               | 18.490          | 29.997               | -0.099          | -0.652         |
| ViT-B/16     | +Half AdvTrain    | 69.960         | 7.624                    | 22.335                   | 51.703                   | 5.040               | 20.670          | 42.344               | -0.047          | -0.385         |
| Mixer-B/16   | Vanilla           | 62.598         | 0.000                    | 0.063                    | 19.857                   | 2.706               | 17.580          | 26.648               | -0.107          | -0.618         |
| Mixer-B/16   | +Half AdvTrain    | 68.296         | 7.151                    | 13.485                   | 32.447                   | 3.853               | 19.780          | 38.396               | -0.065          | -0.407         |

| Architecture | Training Settings | Clean Accuracy | WCAR (large $\ell_\infty$) | WCAR (middle $\ell_\infty$) | WCAR (small $\ell_\infty$) | ImageNet-A Accuracy | ImageNet-O AUPR | ImageNet-C Robustness | ImageNet-P NmFP | ImageNet-S NSD |
|--------------|-------------------|----------------|--------------------------|--------------------------|--------------------------|---------------------|-----------------|----------------------|----------------|----------------|
| ViT-B/16     | Vanilla           | 75.132         | 0.000                    | 0.035                    | 18.693                   | 6.470               | 20.910          | 41.520               | -0.066          | -0.407         |
| ViT-B/16     | +Half AdvTrain    | 74.684         | 0.002                    | 0.134                    | 17.934                   | 6.573               | 19.471          | 48.457               | -0.038          | -0.378         |
training settings with diverse noises. Through our comprehensive empirical studies, we finally reach the conclusion that under aligned training settings, vision transformers and MLP-Mixers are more robust against adversarial noises while less robust against natural noises compared to CNNs.

4.3.3 Architecture is highly important for robustness

Previous works [67], [106] have demonstrated that model architecture is a more critical factor to robustness than model size. However, there exist two drawbacks of these works: on the one hand, they do not take the effect of training techniques into account, which may overestimate the robustness of model architectures; on the other hand, the numbers of models and noises used in the evaluation are comparatively small, which make the evaluation incomprehensive. Therefore, this paper keeps the aligned training settings when comparing the robustness of different model architectures, without introducing the influence of training techniques. Through our large-scale studies, we empirically demonstrate the significance of model architecture to robustness, and we hereby provide several interesting phenomena:

(1) Different architectures show different robustness. Generally, CNNs are more robust to natural and system noises while Transformers and MLP-Mixers are more robust to adversarial noises.

(2) As one of the Transformers architectures, Swin Transformer shows better robustness against natural noises while less robustness against adversarial noises, which is more like CNNs rather than other Transformers.

(3) Slight modifications in the structure (input size, depth, etc) of subnets sampled from supernets would affect their adversarial robustness.

To improve the robustness, besides designing new defense methods, robust architectures could also be taken into consideration. For example, Transformers are more robust for adversarial noises, and CNNs are more robust for natural and system noises.

4.3.4 There does not exist a “once-for-all” training technique for improving robustness

Previous works [15], [29], [88], [107] have studied the influence of some specific training techniques (e.g., label smoothing) on model robustness. In this work, we summarize and evaluate 10+ training techniques over several architectures to help better understand how training techniques will influence the robustness. We suggest that for fair evaluation, the training settings for different models should be aligned. Although according to our evaluation results, there does not exist a “once-for-all” training technique for improving robustness, we still draw several representative conclusions for researchers to improve their models’ robustness which is listed as follows:

(1) When training lightweight networks like ShuffleNetV2, MobileNetV2, and MobileNetV3, we highly recommend researchers use AdamW optimizer instead of SGD.

(2) When training Transformers or MLP-Mixers, adversarial training is universally effective for model robustness against all types of noises.

(3) When training MLP-Mixer, label smoothing could largely improve the adversarial robustness.

(4) When training Transformers, we recommend researchers use Dropout, which could largely boost the robustness against natural and system noises.

4.3.5 Noise diversity has huge influences on robustness evaluation

Some studies [20] have mentioned the fact that researchers should improve the diversity of attacks when evaluating adversarial defenses. However, there still exists no comprehensive empirical studies to study the effect of noise diversities on robustness evaluation. Through large-scale experiments and analysis, we safely conclude that models demonstrate different robustness facing different noise types (e.g., ViT-B/16 > ResNetXt-101 on AutoAttack, while ViT-B/16 < ResNeXt-101 on ImageNet-C). For the same noise type, different attack methods or norms may also result in different robustness evaluation results (e.g., from EfficientNet-B0 to B4, the robustness against PGD-$\ell_2$ increases while the robustness against PGD-$\ell_{\infty}$ decreases). Even for the same attack methods, different perturbation budgets may still influence the robustness evaluation (e.g., as for PGD-$\ell_{\infty}$ attack, DeiTs > ResNeXts when $\epsilon=0.5/255$, while DeITs < ResNeXts when $\epsilon=2/255$). Thus, we suggest researchers improve noise diversities for a more comprehensive robustness evaluation.

5 Conclusions

We propose RobustART, the first comprehensive Robustness benchmark on ImageNet regarding ARCHitecture design (49 human-designed off-the-shelf architectures and 1200 networks constructed by the neural architecture search) and Training techniques (10+ general techniques including training data augmentation) towards diverse noises (adversarial, natural, and system noises). In contrast to existing studies that focus on defense methods, RobustART aims to conduct a comprehensive and fair comparison of different architectures and training techniques towards robustness. Besides discovering several new findings, our benchmark is highlighted for fertilizing the community by providing: (a) an open-source platform for researchers to use and contribute; (b) 100+ pre-trained models publicly available to facilitate robustness evaluation; and (c) new observations to better understand the mechanism towards robust DNN architectures. We welcome community researchers to join us together to continuously contribute to building this ecosystem to better understand deep learning. We will credit contributions from researchers who are not the authors of this paper on the project website.

References

[1] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. Imagenet classification with deep convolutional neural networks. In International Conference on Neural Information Processing Systems, 2012.

[2] Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio. Neural machine translation by jointly learning to align and translate. arXiv preprint arXiv:1409.0473, 2014.

[3] Geoffrey Hinton, Li Deng, Dong Yu, George E. Dahl, Abdelrahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, and Tara N. Sainath. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. IEEE Signal Processing Magazine, 2012.
defenses to adversarial examples. In *International Conference on Machine Learning*, 2018.

[44] Jonathan Uesato, Brendan O'Donoghue, Aaron van den Oord, and Pushmeet Kohli. Adversarial risk and the dangers of evaluating against weak attacks. In *International Conference on Machine Learning*, 2018.

[45] Francesco Croce and Matthias Hein. Reliable evaluation of adversarial robustness with an ensemble of diverse parameter-free attacks. In *International Conference on Machine Learning*, 2020.

[46] Konda Reddy Mopuri, Aditya Ganeshan, and Raj K Venkatesh Babu. Generalizable data-free objective for crafting universal adversarial perturbations. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, 41(10):2452–2465, 2018.

[47] Hongqiu Wang, Guanbin Li, Xiaobai Liu, and Liang Lin. A hamiltonian monte carlo method for probabilistic adversarial attack and learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020.

[48] Yinpeng Dong, Shuyu Cheng, Tianyu Pang, Hang Su, and Jun Zhu. Query-efficient black-box adversarial attacks guided by a transfer-based prior. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, (01):1–1, 2021.

[49] Nicholas Carlini and David Wagner. Towards evaluating the robustness of neural networks. In *IEEE Symposium on Security and Privacy*, 2017.

[50] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. Universal adversarial perturbations. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1765–1773, 2017.

[51] Francesco Croce and Matthias Hein. Minimally distorted adversarial examples with a fast adaptive boundary attack. In *International Conference on Machine Learning*, 2020.

[52] Maksym Andriushchenko, Francesco Croce, Nicolas Flammarion, and Matthias Hein. Square attack: a query-efficient black-box adversarial attack via random search. In *European Conference on Computer Vision*, 2020.

[53] Nicolas Papernot, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami. Distillation as a defense to adversarial perturbations against deep neural networks. *arXiv preprint arXiv:1511.04508*, 2015.

[54] Cihang Xie, Jianyu Wang, Zhishuai Zhang, Zhou Ren, and Alan Yuille. Mitigating adversarial effects through randomization. In *International Conference on Learning Representations*, 2018.

[55] Fangzhong Liao, Ming Liang, Yinpeng Dong, Tianyu Pang, Xiaolin Hu, and Jun Zhu. Defense against adversarial attacks using high-level representation guided denoiser. In *IEEE Conference on Computer Vision and Pattern Recognition*, 2018.

[56] Moustapha Cisse, Piotr Bojanowski, Edouard Grave, Yann Dauphin, and Nicolas Usunier. Parseval networks: Improving robustness to adversarial examples. In *International Conference on Machine Learning*, 2017.

[57] Aamir Mustafa, Salman H Khan, Munawar Hayat, Roland Goecke, Jianbing Shen, and Ling Shao. Deeply supervised discriminative learning for adversarial defense. *IEEE Transactions on Pattern Analysis & Machine Intelligence, (01):1–1, 2020.

[58] Rajkumar Thagorajan and Bir Bhanu. Privacy preserving defense for black box classifiers against on-line adversarial attacks. *IEEE Transactions on Pattern Analysis & Machine Intelligence, (01):1–1, 2020.

[59] Harini Kannan, Alexey Kurakin, and Ian Goodfellow. Adversarial logit pairing. *arXiv preprint arXiv:1803.06373*, 2018.

[60] Cihang Xie, Yuxin Wu, Laurens van der Maaten, Alan L. Yuille, and Kaiming He. Feature denoising for improving adversarial robustness. In *CVPR*, 2019.

[61] Cihang Xie, Mingxing Tan, Boqing Gong, Alan L. Yuille, and Quoc V. Le. Smooth adversarial training. *arXiv preprint arXiv:1806.04536*, 2020.

[62] Tianyu Pang, Xiao Yang, Yinpeng Dong, Hang Su, and Jun Zhu. Bag of tricks for adversarial training. In *International Conference on Learning Representations*, 2021.

[63] Kalee Mahmood, Rigel Mahmood, and Marten van Dijk. On the robustness of vision transformers to adversarial examples. *CoRR*, abs/2105.11595, 2021.

[64] Rulin Shao, Zhouxing Shi, Jinfeng Yi, Pin-Yu Chen, and Cho-Jui Hsieh. On the adversarial robustness of visual transformers. *CoRR*, abs/2103.15670, 2021.

[65] Sayak Paul and Pin-Yu Chen. Vision transformers are robust learners. *CoRR*, abs/2105.07581, 2021.

[66] Ahmed Aldahdooh, Wassim Hamidouche, and Olivier Déforges. Reveal of vision transformers robustness against adversarial attacks. *CoRR*, abs/2106.03734, 2021.

[67] Dong Su, Huan Zhang, Hongge Chen, Jinfeng Yi, Pin-Yu Chen, and Yupeng Gao. Is robustness the cost of accuracy? A comprehensive study on the robustness of 18 deep image classification models. 2018.

[68] Francesco Croce, Maksym Andriushchenko, Vikash Shewag, Edoardo Debenedetti, Nicolas Flammarion, Mung Chiang, Prateek Mittal, and Matthias Hein. Robustbench: a standardized adversarial robustness benchmark. *arXiv preprint arXiv:2010.09670*, 2020.

[69] Saining Xie, Ross Girshick, Piotr Dollár, Zhouwen Tu, and Kaiming He. Aggregated residual transformations for deep neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1492–1500, 2017.

[70] Sergey Zagoruyko and Nikos Komodakis. Wide residual networks. *arXiv preprint arXiv:1605.07146*, 2016.

[71] Ningning Ma, Xiangyu Zhang, Hai-Tao Zheng, and Jian Sun. Shufflenet v2: Practical guidelines for efficient cnn architecture design. In *Proceedings of the European conference on computer vision (ECCV)*, pages 111–126, 2018.

[72] Mark Sandler, Andrew Howard, Menglong Zhu, Andrey Zhmoginov, and Liang-Chieh Chen. Mobilenetv2: Inverted residuals and linear bottlenecks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 4510–4520, 2018.

[73] Xiaohan Ding, Xiangyu Zhang, Ningning Ma, Jangun Hong, Guiguang Ding, and Jian Sun. Repvgg: Making vgg-style convnets great again. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 13733–13742, 2021.

[74] Ilija Radosavovic, Raj Prateek Kosaraju, Ross Girshick, Kaiming He, and Piotr Dollár. Designing network design spaces. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 10428–10436, 2020.

[75] Andrew Howard, Mark Sandler, Grace Chu, Liang-Chieh Chen, Bo Chen, Mingxing Tan, Weijun Wang, Yukun Zhu, Ruoming Pang, Vijay Vasudevan, et al. Searching for mobilenetv3. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 1314–1324, 2019.

[76] Yufei Xu, Qiming Zhang, Jing Zhang, and Dacheng Tao. Vitate: Vision transformer advanced by exploring intrinsic inductive bias. *arXiv preprint arXiv:2106.03348*, 2021.

[77] Geoffrey E. Hinton, Oriol Vinyals, and J. Dean. Distilling the knowledge in a neural network. *Neural Information Processing Systems: Workshop Deep Learning and Representation Learning Workshop*, 2014.

[78] Kaiming He, Haoqi Fan, Yuxin Wu, Saining Xie, and Ross Girshick. Momentum contrast for unsupervised visual representation learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.

[79] Pavel Izmailov, Dmitrii Podoprikhin, Timur Garipov, Dmitry P. Vetrov, and Andrew Gordon Wilson. Averaging weights leads to great again. In *Proceedings of the International Conference on Learning Representations: Workshop*, 2017.

[80] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15(39):1929–1958, 2014.

[81] Dan Hendrycks, Norman Mu, Ekin D. Cubuk, Barret Zoph, Justin Gilmer, and Balaji Lakshminarayanan. Augmix: A simple data processing method to improve robustness and uncertainty. 2020.

[82] Hongyi Zhang, Moustapha Cisse, Yann Dauphin, and David Lopez-Paz. mixup: Beyond empirical risk minimization, 2018.

[83] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei. *ImageNet Large Scale Visual Recognition Challenge*. *International Journal of Computer Vision (IJCV)*, 115(3):211–252, 2015.

[84] Sebastian Ruder. An overview of gradient descent optimization algorithms, 2017.

[85] Ilya Loshchilov and Frank Hutter. Decoupled weight decay regularization. In *International Conference on Learning Representations*, 2019.
**APPENDIX A**

**LIMITATIONS AND BROADER IMPACTS**

RobustART has several limitations, and we list them as follows. (1) Although we have included a large number of architectures and training techniques, due to the rapid emergence of new approaches, there might still exist relevant ones that are not evaluated. (2) We focus on image classification tasks in the first version of our benchmark, and we will continuously develop the benchmark to include more challenging tasks, such as object detection. (3) We presented many intriguing phenomena in our large-scale experiments, but have not dived into some new findings to analyze their causes. We will conduct more thorough studies based on these observations in future work, and we believe that they will also attract broad interests from the community. We will keep the benchmark up-to-date, and hope the community can contribute together to make the ecosystem grows.

Our benchmark will facilitate the studies of deep learning robustness and a better understanding of model vulnerabilities to adversarial examples and other types of noises. We hope that this work will help in building robust model architectures for real-world applications.

**APPENDIX B**

**LICENSES**

The code of RobustART is released under Apache License 2.0. Most model architectures are added to the code with the license chosen by the original author. All pre-trained model checkpoints we provided are produced using our RobustART code and are under Apache License 2.0 as well. The ImageNet-1K, ImageNet-21K, ImageNet-A, ImageNet-O, ImageNet-P, ImageNet-S datasets we use are downloaded from the official release. The ImageNet-C datasets we use are generated according to the official code release on GitHub.

**APPENDIX C**

**MAINTENANCE PLAN**

To make our RobustART benchmark energetic and sustainable, we will keep maintaining our benchmark in these following aspects.

*Maintain our website and leaderboard.* We host our website and leaderboard on our website [http://robust.art](http://robust.art). We will maintain and update our website and leaderboard to make it a sustainable resource center for robustness. At the same time, we will allow other researchers to upload their results on the leaderboard after review.

*Maintain our code base.* Our code base is an easy-to-use framework that includes the model, training, noises, and evaluation processes. The code of our framework is hosted on GitHub, we will keep maintaining and updating it.

*Maintain our pre-trained models.* We provide all pre-trained models in our cloud disk, which have taken more than 44GB of disk space. Every pre-trained model is able to download freely. Moreover, we will keep updating pre-trained models with different architectures and training techniques.

What’s more, we also plan to expand our benchmark to other tasks (i.e., object detection and semantic segmentation) and other datasets, making our RobustART a robust benchmark across major computer vision tasks and datasets.

**APPENDIX D**

**REPRODUCIBILITY AND RUN TIME**

We provide the code to run this benchmark on GitHub where everyone can download from freely. As for the setup steps and instructions about our code, we provided a detailed document which can be found on our website [http://robust.art](http://robust.art) Following the setup page of this document, users can easily install the required run time environment of this codebase.

Besides, there is a ‘Get Started’ page of this document. Users can experience most of the basic functions including model training, add noise and model evaluation of our code by following the instruction on page. For pro developers, we also provided a detailed API document. This API document explains the most important Python class and Python method of our code. Other developers can use this document to modify this code for their needs.

Since our benchmark experiments need us to train multiple models and evaluate them on different kinds of datasets, it needs a large amount of GPU resources. The total cost of our GPU resources to build this benchmark is about 20 GPU years. Most of our experiments are run on Nvidia GTX 1080Ti GPU, some experiments such as ImageNet-21K pre-training which needs more computing resources are run on Nvidia Tesla V100 GPU. For one training experiment, we run it on 16 GPUs parallel. For some training experiments such as ViT, we run it on 32 GPUs parallel to avoid out-of-memory problems.

**APPENDIX E**

**DETAILED INFORMATION**

**E.1 Datasets**

For all basic experiments we use ImageNet-1K dataset [90], which contains 1,000 classes of colored images of size 224 * 224 with 1,281,167 training examples and 50,000 test instances. We believe that different from small data sets such as MNIST and CIFAR-10, ImageNet is more like the application data in the real scene, and thus the robustness evaluation experiments under ImageNet are more valuable and meaningful.

**E.2 Training Techniques**

**Knowledge Distillation.** Knowledge distillation usually refers to the process of transferring knowledge from a large model (teacher) to a smaller one (student). While large models (such as very deep neural networks or ensembles of many models) have higher knowledge capacity than small models. In our experiments, we train a ResNet-18 model with a pre-trained ResNet-50 as a teacher for knowledge distillation.

**Self-Supervised Training.** Self-Supervised Training is proposed for utilizing unlabeled data with the success of supervised learning. In our experiments, we use MoCo v2 which is a classic momentum contrast self-supervised learning algorithm.

**Weight Averaging.** Stochastic Weight Averaging is an optimization procedure that averages multiple points along the trajectory of SGD, with a cyclical or constant learning rate. Weight averaging will lead to better results than
standard training. It was proved that weight averaging notably improves training of many state-of-the-art deep neural networks over a range of consequential benchmarks, with essentially no overhead.

Weight Re-parameterization. RepVGG realizes a decoupling of the training-time and inference-time architecture by structural re-parameterization technique so that the inference can be faster than training [79]. We set experiment of RepVGG with and without using re-parameterization to find out its influence on robustness.

Label smoothing. Label Smoothing is a regularization technique that introduces noise for the labels. This accounts for the fact that datasets may have mistakes in them. Assume for a small constant $\epsilon$ the training set label $y$ is correct with probability $1 - \epsilon$ and incorrect otherwise. Label Smoothing regularizes a model based on a softmax with $k$ output values by replacing the hard 0 and 1 classification targets with targets of $\frac{1}{k-1}$ and $1 - \epsilon$ respectively.

Dropout. Dropout is a regularization technique for neural networks that drops a unit (along with connections) at training time with a specified probability. To find out the influence of dropout on robustness, we trained and tested the models with and without dropout.

Data Augmentation. The performance of neural networks often improves with the amount of training data. Data augmentation is a technique to artificially create new training data from existing training data. We use Mixup and Augmix as two kinds of data augmentation methods to find out their influences.

Large-Scale Pre-training. It has been proved that pre-training using a large-scale dataset can improve the performance of neural networks. To find out the influence of large-scale dataset, we set up experiments using pre-training with ImageNet-21K dataset, which consists of 14,197,122 images (about 14 times larger than ImageNet-1K), each tagged in a single-label fashion by one of 21,841 possible classes.

Adversarial Training. Adversarial training is one of the most effective defense methods towards adversarial noises. During training, it generates adversarial examples using some attacks and then feed these adversarial examples into the model to calculate the loss function and update model weights. The most commonly used adversarial training method is PGD adversarial training, which uses PGD attack to generate adversarial examples during training procedure.

SGD and AdamW. Optimizers are algorithms or methods used to minimize the loss function or to maximize the efficiency of production. To find out the influence of different optimizers, we use two kinds of commonly used optimizers in our experiments. Stochastic Gradient Descent (SGD) is the most basic form of gradient descent. SGD subtracts the gradient multiplied by the learning rate from the weights. Despite its simplicity, SGD has strong theoretical foundations. AdamW is a stochastic optimization method that modifies the typical implementation of weight decay in Adam, by decoupling weight decay from the gradient update.

E.3 Noises

E.3.1 Adversarial noises

Fast Gradient Sign Method (FGSM). The FGSM [5] attack is an early-proposed one-step adversarial attack with $\ell_\infty$ norm. It simply substitutes the class variables with the target type of smallest recognition probability in the adversarial perturbation, and then subtracts the perturbation from the original images. Although it yields comparably weak attack ability, the main characteristic of FGSM is its low computational cost.

Projected Gradient Descent (PGD). The PGD [24] attack is one of the most powerful first-order attacks in the adversarial literature. Instead of a single step of calculating gradients and doing the gradient descent, it iterates through multiple steps with a gradient projection after each step. With different perturbation norm types, there are mainly PGD-$\ell_1$, PGD-$\ell_2$ and PGD-$\ell_\infty$ attack. We use all of them to conduct a comprehensive robustness evaluation.

Momentum Iterative Method (MIM). The MIM [92] is an iterative adversarial attack based on PGD. It integrates the momentum term into the iterative process for attacks, which stabilizes update directions and can escape from poor local maxima during the iterations, resulting in more powerful attack ability and transferability. We use the widely considered MIM-$\ell_\infty$ in our evaluations.

Decoupled Direction and Norm attack (DDN). DDN [93] is an efficient $\ell_2$ norm adversarial attack. It optimizes cross-entropy loss and then changes the norm based on whether the sample is adversarial or not. Using this approach to decouple the direction and norm of the adversarial noise leads to fewer attack iterations, thus speed up the generation of adversarial examples.

AutoAttack. The AutoAttack [91] proposes two extensions of the PGD-attack: APGD-CE and APGD-DLR, which overcome failures due to suboptimal step size and problems of the objective function. It then combines the two novel attacks with two complementary existing attacks (whitebox FAB attack [51] and black-box square attack [52]) to form a parameter-free and computationally affordable attack. AutoAttack is powerful on many classifiers with various defense methods, thus becoming a good choice for evaluating model robustness in adversarial literature.

Carlini&Wagner attack (C&W). The C&W [19] attack is a family of optimization-based attacks for finding adversarial perturbations that minimize the given loss function. It proposes to transform a general constrained optimization problem into an unconstrained optimization formulation using an empirically chosen loss function. The C&W attack enables strong attack ability, while the whole optimization procedure is time-consuming.

E.3.2 Natural noises

ImageNet-A. ImageNet-A is a dataset of real-world adversarially filtered images that fool current ImageNet classifiers. To build this dataset, they first download numerous images related to an ImageNet class. Thereafter they delete the images that fixed ResNet-50 classifiers correctly predict. With the remaining incorrectly classified images, they manually select visually clear images and make this dataset [14].

ImageNet-O. ImageNet-O is a dataset of adversarially filtered examples for ImageNet out-of-distribution detectors. To create this dataset, they download ImageNet-22K and delete examples from ImageNet-1K. With the remaining ImageNet-22K examples that do not belong to ImageNet-1K
classes, they keep examples that are classified by a ResNet-50 as an ImageNet-1K class with high confidence [14].

**ImageNet-C.** The ImageNet-C dataset consists of 15 diverse corruption types applied to validation images of ImageNet. The corruptions are drawn from four main categories: noise, blur, weather, and digital. Each corruption type has five levels of severity since corruptions can manifest themselves at varying intensities. We use all four categories and five levels of severity of this dataset in our benchmark [12].

**ImageNet-P.** Like ImageNet-C, ImageNet-P consists of noise, blur, weather, and digital distortions. The dataset also has validation perturbations and difficulty levels. ImageNet-P departs from ImageNet-C by having perturbation sequences generated from each ImageNet validation image. Each sequence contains more than 30 frames [12].

### E.3.3 System noises

The ImageNet-S dataset [42] consists of 3 commonly used decoder types and 7 commonly used resize types. For the decoder, it includes the implementation from Pillow, OpenCV, and FFmpeg. For resize operation, it includes nearest, cubic, lanczos, area, box, and bilinear interpolation modes from OpenCV and Pillow tools.

During the process of evaluation, Pillow bilinear mode is set as the default resize method when testing the decoding robustness. This setting is also the default training setting in PyTorch [108] official code example. Similarly, Pillow is set as the default image decoding tool (same as PyTorch).

This dataset provides a validation set of ImageNet with different decoding and resize methods, and saves each image file after decoding and resizing it as a \(3 \times \text{width} \times \text{height}\) matrix in a .npy file instead of JPEG. According to the commonly used transform on ImageNet [90] test set, it implements pre-processing for images. This dataset provides a matrix of an image after the process of resizing to \(3 \times 256 \times 256\) then applied a center crop to \(3 \times 224 \times 224\).

## E.4 Metrics

### E.4.1 Metrics for adversarial noises

**Adversarial Robustness (AR).** As widely used in the literature [95], [96], [97], we choose Attack Success Rate (ASR) as the base evaluation metric. Considering that ASR mainly measures the attack effectiveness while we are about to measure model robustness, we simply modify it to get our adversarial robustness metric:

\[
AR(f, a, \mathbb{D}) = \frac{\sum_{(x_i, y_i, \sim \mathbb{D})} 1(f(x_i) = y_i) \cdot 1(a(x_i, y_i, f) = y_i)}{\sum_{(x_i, y_i, \sim \mathbb{D})} 1(f(x_i) = y_i)}
\]  

(2)

where \(f\) is the threat model, \(a\) is a certain adversarial attack like PGD-\(\ell_\infty\) that receives input images, label and threat model as input and returns the perturbed images, and \(\mathbb{D}\) is the clean dataset. \(1(\cdot)\) is the indicator function. This metric can effectively reveal the relevant accuracy drop of a specific model when facing noises with considering the original clean accuracy of the model. However, it is not enough to help us figure out the deeper conclusion of the model inherent robustness. Thus we design some new metrics.

**Worst-Case Attack Robustness (WCAR).** To aggregate the model adversarial robustness results under different attacks, we follow instructions in [20] and choose to use the per-example worst-case attack robustness:

\[
WCAR(f, A, \mathbb{D}) = \sum_{(x_i, y_i, \sim \mathbb{D})} \left\{ 1(f(x_i) = y_i) \cdot \prod_{a \in A} 1(f(a(x_i, y_i, f) = y_i) \right\} \sum_{(x_i, y_i, \sim \mathbb{D})} 1(f(x_i) = y_i)
\]

(3)

where \(f\) is the threat model, \(A\) is the attack set consisting of many different adversarial attacks, and \(\mathbb{D}\) is the clean dataset. \(1(\cdot)\) is the indicator function. WCAR means the lower bound adversarial robustness of a model under multiple different adversarial attacks, which is a better metric for aggregating the results of different adversarial attacks appropriately compared to some other methods like simple averaging. Further, we define three aggregating magnitudes of WCAR: WCAR (small \(\epsilon\)) means the WCAR under all adversarial attacks with small \(\epsilon\), WCAR (middle \(\epsilon\)) means the WCAR under all adversarial attacks with middle \(\epsilon\), and WCAR (large \(\epsilon\)) means the WCAR under all adversarial attacks with large \(\epsilon\).

### E.4.2 Metrics for natural noises

**Top-1 Accuracy.** We use top-1 accuracy as the metric for ImageNet-A dataset. It can reflect how good performance of this model when facing the images which fool commonly used ResNet-50.

**1-mCE.** We use 1-mCE as the metrics for ImageNet-C dataset. Firstly, we compute the top-1 accuracy of on each corruption type \(c\) at each level of severity \(s\) and then compute top-1 error rate denote by \(E^f_{c,s}\). After that we can compute the Corruption Error, with the formula \(CE^f_c = \sum_{s=1}^5 E^f_{c,s} / \sum_{s=1}^5 E^f_{c,s}\) [18]. Now we can average the 15 Corruption Error values and get meanCE or mCE for shot. Finally, we can compute \(1 - mCE\) to evaluate ImageNet-C robustness.

**AUPR.** We use the area under the precision-recall curve (AUPR) as the metrics for ImageNet-O dataset [14]. This metric requires anomaly scores. Our anomaly score is the negative of the maximum softmax probabilities from a model that can classify the 200 ImageNet-O classes.

**NmFP.** Denote \(m\) perturbation sequences with \(S = \{x_1, x_2, \ldots, x_n\}\) \(m\) where each sequence is made with perturbation \(p\). The "Flip Probability" of network \(f : X \rightarrow \{1, 2, \ldots, 1000\}\) on perturbation sequences \(S\) is

\[
\text{FP}_p = \frac{1}{m(n-1)} \sum_{i=1}^{n} \sum_{j=2}^{n} \left| \mathbb{P}_{x \sim S} (f(x_j) \neq f(x_j-1)) \right|
\]

(4)

For noise perturbation sequences, which are not temporally related, \(x_1^{(i)}\) is clean and \(x_j^{(i)}\) \((j > 1)\) are perturbed images of \(x_1^{(i)}\). Then the FP formula can be recast...
as \( FP_p = \frac{1}{m(n-1)} \sum_{i=1}^{m} \sum_{j=2}^{n} \mathbb{P}_{\tau \neq s} (f(x_i) \neq f(x_j)) \) where \( \mathbb{P}_{\tau \neq s} (f(x) \neq f(x) | j > 1) \). Averaging the Flip Probability across all perturbations and its negative number yields the Negative mean Flip Probability or NmFP [12].

### E.4.3 Metrics for system noises

**NSD**. We use Negative Standard Deviation (NSD) as the metrics for ImageNet-S system noise, which is the negative value of standard deviation across all accuracy on different decoders and resize methods. The formula of it can be written as \( NSD = -\sigma(A) \), where \( A = \{a_{\text{decoder}}^{\text{resize method}}\}. We use standard deviation because we want to know the stability of a model facing different decoders and resize methods, and we take the negative value of it since we want this value to increase with this model’s performance just like other metrics of this benchmark.

### APPENDIX F

#### EXPERIMENTAL SETUP

Here, we provide the details of the experimental settings of our robustness evaluation benchmark.

#### F.1 Settings for Architecture Design

##### F.1.1 Human-designed off-the-shelf architectures

To conduct fair and rigorous comparisons among different models, we keep the aligned training techniques as much as possible for each human-designed off-the-shelf architecture. For optimizer, we use SGD [85] optimizer with nesterov momentum=0.9 and weight decay=0.0001 for all model families except for ViTs, DeiTs, Swin Transformers, ViTAEs and MLP-Mixers; instead for these five model families, we use AdamW [86] with weight decay=0.05 since Transformers and MLP-Mixers are highly sensitive to optimizers, using SGD would cause the failure of training [54]. For scheduler, we use cosine scheduler [101] with maximum training epoch=100 for all models, except for ViTs, DeiTs, Swin Transformers, ViTAEs and MLP-Mixers we use base learning rate (lr)=0.1, warm up lr=0.4, and minimal lr=0.0, and for these five model families we use a much smaller learning rate. For data pre-processing, we use standard ImageNet training augmentation, which consists of random resized crop, random horizontal flip, color jitter, and normalization. For other hyper-parameters, we use label smoothing with \( \epsilon=0.1 \) and batch size=512.

When we study the model size towards robustness, we randomly sample 200 subnets without any factor fixing from each supernet and evaluate subnets’ robustness towards adversarial, natural, and system noises. When we study the influence of a certain factor \( i.e. \), input size, convolution kernel size, model depth, or expand ratio, we first fix all other factors, ensuring they are the same in all sampled subnets, then we randomly sample 50 subnets and evaluate their robustness.

##### F.2 Settings for Training Techniques

In total, we choose 11 different training techniques, including weight averaging, label smoothing, ImageNet-21K pre-training, Mixup, Augmix, Dropout, weight re-parameterization, knowledge distillation, MOCO v2 self-supervised training, PGD-\( \infty \) adversarial training, and AdamW optimizer. Due to the huge time consumption of training all 49 human-designed off-the-shelf architectures with or without these 11 training techniques and evaluating their robustness under various noises on ImageNet, we only choose several architectures for each training technique. For Mixup, Augmix, weight averaging, label smoothing, and PGD-\( \infty \) adversarial training, we choose ResNet-50, RegNetX-3200M, ShuffleNetV2-x2.0, MobileNetV3-x1.4, ViT-B/16 and Mixer-B/16, covering large CNNs, light-weight CNNs, and ViTs. For knowledge distillation, we only choose ResNet-18 due to time consumption. For MOCO v2 self-supervised training, we choose ResNet-50 since it is the most commonly used architecture in self-supervised training. For ImageNet-21K pre-training we only choose ResNet-50 and ViT-B/16 due to time consumption. For AdamW optimizer, we choose ResNet-50, RegNetX-3200M, ShuffleNetV2-x2.0 and MobileNetV3-x1.4. For weight re-parameterization, we choose RepVGG-A0 and RepVGG-B3 since this technique is well supported by this model architecture. For Dropout, we choose EfficientNet-B0, MobileNetV3-x1.4, ViT-B/16, and Mixer-B/16.

For the chosen networks of each training technique, we select to apply or disable this training technique during training with all other training settings being the same. For weight averaging, we set decay=0.9999. For label smoothing, we set \( \epsilon=0.1 \). For ImageNet-21K pre-training, we train the model on ImageNet-21K dataset for 100 epochs, then finetune it on ImageNet-1K for 30 epochs with a small learning rate (0.01 base learning rate and 0.04 warm up learning rate). For Mixup, we set \( \alpha=0.2 \). For Augmix, we use the same default config as the original paper. For Dropout, we train one kind of model with the default dropout rate while still train the other kind of model without dropout \( i.e. \) set the dropout rate to 0. For weight re-parameterization, we use the model of RepVGG-A0 and RepVGG-B3 with and without weight re-parameterization respectively. The process of weight re-parameterization is done following by the guide of paper of RepVGG [85]. For knowledge distillation, we use the baseline ResNet-50 model as the teacher model, and the ResNet-18 model as the student model. We train it on ImageNet-1K for
100 epochs. For MOCO v2 self-supervised training, we first train it using the unsupervised method for 200 epochs, then finetune it for 100 epochs. For PGD-$\ell_\infty$ adversarial training, we set attack iteration=20, step size=0.002 and $\epsilon$=8/255. For AdamW optimizer, we use cosine decay learning rate schedule setting, base learning rate as $1e^{-5}$ and warm up learning rate as $5e^{-4}$.

F.3 Settings for Noises

**Adversarial noises.** For all adversarial attacks, we use three different perturbation magnitudes (small, middle and large). Specifically, for $\ell_1$ attacks we set large $\epsilon$=1600.0, middle $\epsilon$=400.0 and small $\epsilon$=100.0; for $\ell_2$ attacks we set large $\epsilon$=8.0, middle $\epsilon$=2.0 and small $\epsilon$=0.5; for $\ell_\infty$ attacks we set large $\epsilon$=8/255, middle $\epsilon$=2/255 and small $\epsilon$=0.5/255. As for other hyper-parameters, for PGD-$\ell_1$, PGD-$\ell_2$ and PGD-$\ell_\infty$ attack we set attack iteration=20, step size=$\frac{\epsilon}{40}$ and enable random restart; for MIM-$\ell_\infty$ we set attack iteration=20, step size=$\frac{\epsilon}{47}$, and decay factor=1.0; for DDN-$\ell_2$ we set optimization steps=10 and factor $\gamma$=0.05; for AutoAttack-$\ell_\infty$ we simply follow its original hyper-parameters since it is a parameter-free attack; for C&W attack we set binary search steps=5, optimization steps=100 and optimization step size=0.001.

**Natural noises.** For natural noises, we simply follow the standard settings in ImageNet-C, ImageNet-P, ImageNet-A, and ImageNet-O datasets.

**System noises.** For system noises, we use the standard setting of ImageNet-S dataset, which can be found in Section E.3.3.

APPENDIX G

ADDITIONAL RESULTS

G.1 Architecture Design Towards Robustness

We first report the model robustness and standard performance under the view of FLOPs in Figure 5. For almost all model architectures, the robustness results are the same as those using Params to measure model size. Then we report the detailed results of model robustness under various magnitudes of different adversarial noises in Figure 6, 7, 8, 9, 10, 11, 12, 13, 14, 15. There are 2 model size measurements (FLOPs and Params) and 3 perturbation magnitudes (small, middle and large), resulting in total 6 figure for each attack. In addition, we also report the heatmap of different model architectures under transfer-based adversarial attacks under more perturbation magnitudes in Figure 16, 17. We can see the model robustness results under transfer-based attack with $\epsilon$=0.5/255 and $\epsilon$=2/255 are almost the same as those under attack with $\epsilon$=8/255.

G.2 Training Techniques Towards Robustness

We report the results for the influence of all training techniques studied towards model robustness under various noises in Figure 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28. For each training technique we choose 24 metrics to show its influence on model accuracy and robustness. More results can be found on our website.
Fig. 6. Robustness on human-designed off-the-shelf architectures under the view of FLOPs.

Fig. 7. Worst-case attack robustness of human-designed off-the-shelf architectures under 3 different $\epsilon$ magnitudes.
Fig. 8. Adversarial robustness of human-designed off-the-shelf architectures under DDN-\(\ell_2\) attack with 3 different \(\epsilon\) magnitudes.

Fig. 9. Adversarial robustness of human-designed off-the-shelf architectures under FGSM attack with 3 different \(\epsilon\) magnitudes.
Fig. 10. Adversarial robustness of human-designed off-the-shelf architectures under MIM-$\ell_\infty$ attack with 3 different $\epsilon$ magnitudes.

Fig. 11. Adversarial robustness of human-designed off-the-shelf architectures under PGD-$\ell_1$ attack with 3 different $\epsilon$ magnitudes.
Fig. 12. Adversarial robustness of human-designed off-the-shelf architectures under PGD-$\ell_2$ attack with 3 different $\epsilon$ magnitudes.

Fig. 13. Adversarial robustness of human-designed off-the-shelf architectures under PGD-$\ell_{\infty}$ attack with 3 different $\epsilon$ magnitudes.
Fig. 14. Adversarial robustness of human-designed off-the-shelf architectures under AutoAttack-$\ell_{\infty}$ attack with 3 different $\epsilon$ magnitudes.

Fig. 15. Adversarial robustness of human-designed off-the-shelf architectures under C&W-$\ell_{2}$ attack with 3 different $\epsilon$ magnitudes.
Fig. 16. Transferability heatmap of human-designed off-the-shelf architectures under FGSM attack, $\epsilon=2/255$.

Fig. 17. Transferability heatmap of human-designed off-the-shelf architectures under FGSM attack, $\epsilon=0.5/255$. 
Fig. 18. The influence of ImageNet-21K pre-training towards model robustness under various noises.
Fig. 19. The influence of AdamW optimizer towards model robustness under various noises.
Fig. 20. The influence of adversarial training towards model robustness under various noises.
Fig. 21. The influence of Augmix data augmentation towards model robustness under various noises.
Fig. 22. The influence of Dropout towards model robustness under various noises.
Fig. 23. The influence of knowledge distillation towards model robustness under various noises.
Fig. 24. The influence of label smoothing towards model robustness under various noises.
Fig. 25. The influence of Mixup data augmentation towards model robustness under various noises.
Fig. 26. The influence of self-supervised training towards model robustness under various noises.
Fig. 27. The influence of weight averaging towards model robustness under various noises.
Fig. 28. The influence of weight re-parameterization towards model robustness under various noises.
Fig. 29. The influence of Half Adversarial Training scheme towards model robustness under various noises.