Learning Instance-Specific Data Augmentations

Ning Miao¹  Emile Mathieu¹  Yann Dubois²  Tom Rainforth¹
Yee Whye Teh¹  Adam Foster³  Hyunjik Kim⁴

Abstract

Existing data augmentation methods typically assume independence between transformations and inputs: they use the same transformation distribution for all input instances. We explain why this can be problematic and propose InstaAug, a method for automatically learning input-specific augmentations from data. This is achieved by introducing an augmentation module that maps an input to a distribution over transformations. This is simultaneously trained alongside the base model in a fully end-to-end manner using only the training data. We empirically demonstrate that InstaAug learns meaningful augmentations for a wide range of transformation classes, which in turn provides better performance on supervised and self-supervised tasks compared with augmentations that assume input–transformation independence. Codes are available at https://github.com/NingMiao/InstaAug.

1 Introduction

Data augmentation is ubiquitous in deep learning [34]. It can be seen as a regularization technique [14], as well as a means to incorporate inductive biases and invariances into models [5, 26]. Data augmentations are particularly useful in computer vision, where they are an essential component of modern supervised [30, 22, 11, 28] and self-supervised [1, 6, 39] training pipelines.

Algorithmically, data augmentations consists in applying a random transformation \( \tau : \mathcal{X} \to \mathcal{X} \), \( \tau \sim p(\tau) \), to each input data point \( x \in \mathcal{X} \), before feeding this augmented data into the base model. These transformations are resampled each time the data point is used (e.g. at each training epoch), effectively populating the training set with additional samples. A particular augmentation is defined by the choice of the transformation distribution \( p(\tau) \), whose construction thus forms the key design choice. Good transformation distributions will induce substantial and wide-ranging changes to the input, while preserving key information relevant to the task at hand.

Data augmentation necessarily relies on exploiting problem-specific expertise: though aspects of \( p(\tau) \) can be learned from data [2], trying to learn \( p(\tau) \) from the set of all possible transformation distributions is not only unrealistic, but actively add odds with our core motivations of regularization and inductive biases. To incorporate domain-specific knowledge, one, therefore, restricts \( \tau \) to transformations that reflect how we desire our model to generalize, such as affine transformations, cropping, or color jitter for image data.

Current approaches [10, 24, 2] generally sample the transformation, \( \tau \), independently of the input. That is, they use a distribution \( p(\tau) \) with no dependence on \( x \). For example, one samples a rotation angle independently of the image being rotated.

We argue that this independence assumption can be a severe limitation when \( \tau \) (and by extension \( p(\tau) \)) is restricted, as is always the case in practice. Taking color jittering for instance, changing the color of a leaf from yellow to green would likely preserve its label, yet the same transformation would change a lemon to a lime (see Figure 1b). This color transformation thus cannot be usefully applied as a global augmentation, i.e. independently of the input \( x \), even though it is a useful augmentation for the specific input instance of a leaf. Similar examples regularly occur for rotation and cropping, as illustrated in Figure 1.

¹Department of Statistics, University of Oxford. ²Stanford University. ³Microsoft Research. ⁴DeepMind, UK. Corresponding to Ning Miao <ning.miao@stats.ox.ac.uk>.
Figure 1: Different inputs require different augmentations. In (a), the digit ‘0’ is invariant to any rotation, but rotating the digit ‘6’ by more 90° makes it a ‘9’. In (b), a similar phenomenon is observed for color jittering applied to a leaf and a lemon/lime. The red dashed lines in (a) and (b) are boundaries between different classes. In (c), the same effect is shown for cropping. Solid rectangles represent the patches that preserve the labels of the original images ([left] grass, [right] cattle), while dashed rectangles represent patches with different labels to the original images.

To address this shortfall, we propose InstaAug, a new augmentation method that learns instance-specific transformation distributions of the form \( p(\tau; \phi(x)) \), where \( \phi \) is a deep neural network that maps inputs to transformation distribution parameters. We refer to \( \phi \) as an augmentation module. We train \( \phi \) and the base model simultaneously in a fully end-to-end manner, using only the training data and a single objective function that minimizes the training error while maintaining augmentation diversity. As such, InstaAug allows one to directly learn powerful and general augmentations, without requiring access to additional annotations.

We evaluate InstaAug in supervised and self-supervised settings, focusing on image classification for the former, and contrastive learning for the latter. Our experimental results show that InstaAug learns meaningful augmentations that are consistent with human cognition, and that those augmentations improve model performance for various tasks compared with random and learned global augmentations.

2 Method: InstaAug

The ultimate aim of data augmentation can be thought of as instilling inductive biases into the model. Hence, \( p(\tau) \) must be restricted to particular classes of transformations that reflect our domain expertise. Existing approaches [10, 24, 2] further assume that \( \tau \) is generated independently of \( x \). For example, when augmenting images with rotated versions of themselves, \( p(\tau) \) is typically a uniform distribution over a fixed range of rotation angles.

For general classes of transformations, this assumption can be justified through the noise outsourcing lemma [19]. This tells us that any conditional distribution \( Y|X=x \) can be expressed as a deterministic function \( g: \mathcal{X} \times \mathbb{R}^n \to \mathcal{Y} \) of the input and some independent noise \( \varepsilon \sim \mathcal{N}(0, I) \). This result is the basis for reparameterization in VAEs [21, 33], and learning (conditional) generators from random noise in deep generative models [29, 35, 36].

However, for restricted transformation classes, this result no longer holds, and the independence assumption can cause severe restrictions. For example, sampling rotations independently to the input is equivalent to the unrealistic assumption that the labels of all images \( x \) are invariant to the same range of angles (cf. Figure 1a).

In order to remedy this problem, we propose InstaAug. InstaAug learns an input dependent transformation distribution \( p(\tau; \phi(x)) \) that actively makes use of the input \( x \), as opposed to learning a fixed global transformation distribution \( p(\tau) \). This generalizes the hypothesis class of transformation distributions, and significantly increases the flexibility and expressivity of the augmentations we can learn, without undermining our ability to carefully control the inductive biases that are imparted.

We train InstaAug so that the augmentations fulfill two properties. First, the transformations should preserve the information in \( x \) that is necessary for the task at hand. For example, in classification, transformations must preserve sufficient information to correctly classify \( \tau(x) \). Second, the set of augmentations needs to have sufficient ‘diversity’ to effectively augment the training data. We quantify diversity as the entropy of the transformation distribution \( p(\tau; \phi(x)) \). For classification, our aim can thus be thought of as minimizing cross-entropy under the constraint of maintaining large transformation entropy. For simplicity, we describe InstaAug on the task of classification in the remainder of this section.
2.1 Model structure

As illustrated in Figure 2, InstaAug forms a simple plug-in module between the input \(x\) and the classifier \(f\). We assume a parametric family of distributions \(p(\tau; \cdot)\) over some transformation space. Given an input \(x\), the augmentation module \(\phi\), which is a trainable neural network, predicts the parameters \(\phi(x)\) of the transformation distribution. During training, we sample a transformation \(\tau \sim p(\tau; \phi(x))\), which is applied to \(x\) to generate an augmented sample \(\tau(x)\), before feeding this into the classifier \(f\). Taking the example of rotations as the space of transformations, the augmentation module outputs \(\phi(x) = (\theta_{\min}, \theta_{\max})\) which represents the maximum and minimum values of a uniform distribution over the angle \(\theta\) of 2D rotations. We then rotate the input image \(x\) by an angle uniformly sampled from the predicted interval: \(x \mapsto \tau(x) = R(\theta) \cdot x\), with \(\theta \sim U(\theta_{\min}, \theta_{\max})\).

2.2 Objective function

Good augmentations should induce substantial changes to the input \(x\) in order to capture the maximum possible invariance. At the same time, they should preserve key information from the input \(x\) relevant to the task at hand, e.g. such that class labels are preserved. Figure 3a illustrates the tension between these two objectives. Wider ranging transformations are generally beneficial for generalization, but ‘excessive’ transformations will generate samples that will be incorrectly classified. In Figure 3a we see this in the red area, where the augmentations for a pair of data points have started to overlap, creating ambiguity and inevitably misclassifications. The cross-entropy loss of the classifier naturally applies pressure to avoid this behavior, but optimizing the loss alone is unlikely to produce diverse augmentations. The augmentation module could indeed simply learn to induce a Dirac distribution at the identity function, which would not affect the loss.

A key design in our method is therefore to constrain the ‘diversity’ of augmented samples, which we quantify via the average entropy of the transformations \(E_{x \sim p_{\text{data}}} [H[p(\tau; \phi(x))]]\). By properly parameterizing \(p(\tau; \phi(x))\) in Section 2.3, we can write down its entropy in closed form. We can then formulate the problem as the following constrained optimization problem:

\[
\begin{align*}
\min_{f, \phi} & \quad E_{x, y \sim p_{\text{data}}} \left[ E_{\tau \sim p(\tau; \phi(x))} \left[ L(f(\tau(x)), y) \right] \right], \\
\text{s.t.} & \quad E_{x, y \sim p_{\text{data}}} \left[ H[p(\tau; \phi(x))] \right] \in [H_{\min}, H_{\max}],
\end{align*}
\]

(1a)

(1b)

where \(L\) is the cross-entropy loss. This objective can be interpreted as the usual cross-entropy minimization for classification while ensuring that augmentation diversity is maintained within a certain range during training. The lower bound avoids \(p(\tau; \phi(x))\) degenerating to a delta function at the identity, while the upper bound prevents \(p(\tau; \phi(x))\) exploding at the start of training when the classifier is weak: without this we empirically find that the augmented samples from different classes rapidly overlap with each other in the initial phase of training, hindering the training of the classifier \(f\). \(H_{\min}\) and \(H_{\max}\) are hyper-parameters reflecting human preference for augmentation diversity.
The Lagrangian function, 
\[ \mathbb{E}_{x,y \sim p_{data}} \left[ \mathbb{E}_{\tau \sim p(\tau; \phi(x))} \left[ L(f(\tau(x)); y) \right] \right] - \lambda \mathbb{E}_{x,y \sim p_{data}} \left[ H[p(\tau; \phi(x))] \right], \]
can be used to solve this constrained optimization, where \( \lambda \) is the Lagrangian multiplier. In practice, we initialize \( \lambda \) with a small positive value, and increase (decrease) \( \lambda \) when the average entropy drops below \( H_{\text{min}} \) (exceeds \( H_{\text{max}} \)). This method can also be extended to regression or self-supervised learning by substituting the loss function \( L \) (cf. Appendix B).

### 2.3 Parameterization of augmentations and model training

Due to the varied characteristics of different image transformations, we design two different parameterization methods for \( p(\tau; \phi(x)) \). We focus on transformations that are frequently used in computer vision, although our framework can easily be extended to other domains.

**Uniform parameterization.** For transformations acting on the whole image, such as rotation or color jittering, we find that a uniform distribution is suitable for parameterizing \( p(\tau; \phi(x)) \). For example, we assume that 2D rotations’ angles are uniformly distributed on the interval \( \phi(x) = (\theta_{\text{min}}, \theta_{\text{max}}) \), where \( \theta_{\text{max}} \) and \( \theta_{\text{min}} \) are the outputs of the augmentation module \( \phi \). To compose multiple transformations \( \tau_k \) (such as hue, saturation and brightness in color jittering), we make a mean field assumption that the joint distribution \( p(\tau_1, \ldots, \tau_K; \phi(x)) \) factorises along each transformation \( \tau_k \).

**Location-related parameterization.** It is less straightforward to parameterize local transformations such as cropping. Using independent uniform distributions on the centers and sizes of the crop has two failure modes. First, the distribution of ‘good’ patches may be multi-modal, since label information may exist in different parts of an image. Second, the center coordinates and patch sizes are highly correlated, which goes against a mean-field assumption. For example, smaller sizes are sufficient for patches around the head of an animal than its torso.

To parametrize cropping transformations, we consider a categorical distribution over a finite number of patches of various sizes. We do so by applying a CNN to the input image and relating every feature from every layer of that CNN to a corresponding patch. We then flatten and concatenate the intermediate and final layer features of the CNN to form a vector of unnormalized log probabilities over desired patches, as shown at the top of Figure 4. Our parametrization is designed so that each logit corresponds to the patch from which it receives information, i.e., its receptive field. Feature-patch pairs are shown by the same color in Figure 4. Features at a given layer of the CNN, therefore, correspond to patches of the same size with different locations, and features from different layers represent patches of different sizes. To extend the support of \( p(\tau; \phi(x)) \) from this finite set of square patches defined by the CNN, we further perturb the positions and sizes of samples generated from the categorical distribution with small i.i.d. uniform noise. Though we describe this parameterization on cropping, it can be directly applied to other local transformations, such as masking, local blurring, pixel-wise perturbation, and local color jittering.

**Model training.** In InstaAug, the augmentation module and base model are trained simultaneously by solving the optimization problem (1). Unlike nested training algorithms in meta-learning based methods, InstaAug only has a single forward pass and a single backward pass; it is trained end-to-end via gradient descent. In order to estimate gradients of the loss through the random samples \( \tau \sim p(\tau; \phi(x)) \) of the transformation distributions and use them to update the augmentation module \( \phi \), we rely respectively on the reparameterization trick [21, 2] for uniform distributions and the REINFORCE estimator [40, 31] for categorical distributions. The entropies can be computed directly in closed form in both cases.
3 Related Work

Hard-coded invariance. Much recent work has been devoted to hard-coding invariance in neural networks. For example, various models have been designed to be invariant to translation [4, 46], rotation [42, 50, 27], scaling [41, 37] or other group actions [9, 43]. Although very effective in low-data settings, these methods have two main differences from our method. Firstly, they require the set of invariant transformations to be closed under composition (to form a group), leaving out many practical transformations that do not form a group, such as cropping. Secondly, all inputs have the same global invariance, thus these works do not allow instance-specific invariance.

Learning augmentations. In order to address the shortcomings of random augmentation and hard-coded invariance, there have been prior works that automatically learn augmentations and invariance from data. AutoAugment [10] uses reinforcement learning to find augmentation strategies that increase classification accuracy on a separate validation set. Subsequent works such as Fast AutoAugment [24], PBA [17], Faster AutoAugment [15] and DADA [23] improve the efficiency of AutoAugment with similar test performance. RandAugment [11] further speeds up training using a reduced search space. DeepAA [47] builds more flexible augmentations by stacking more transformation layers. Adversarial Det-AdvProp [7] attacks the predictive network by adversarial augmentations, which encourages the predictive network to learn more robust features. Zhou et al. [48] learn symmetries shared across several datasets through a meta-learning scheme.

In InstaAug, we focus on learning instance-specific augmentations, whereas the aforementioned methods apply the same global transformation distribution to every input, and often focus on relatively coarse augmentation parametrizations. We also developed a simple training scheme that only uses the training set, avoiding more complex, nested learning using a validation set. The learned augmentations of these methods correspond to some specific settings of the hyperparameters for global random augmentation. Therefore, rather than comparing with these methods directly in our experiments, we perform a sweep over all possible augmentation hyperparameter settings for global random augmentation, and benchmark our method against the best setting in Section 4. This thus forms an upper bound for the performance of any baseline that learns a global random augmentation policy.

Instance-specific augmentation. For the purpose of achieving sample-aware augmentation, MetaAugment [49] leverages a separate network to tune the probabilities of applying different transformations for each sample. In order to achieve class awareness, AdaAug [8] reuses features extracted by the classifier to predict augmentation policies. Unlike InstaAug, their search spaces for augmentation parameters are too coarse to allow subtle differences in the transformation parametrization for different inputs. Meanwhile, both methods rely on a validation set to train the augmentation network, which makes it difficult to quantitatively compare InstaAug with them.

Spatial transformer [18] also aims to learn instance-specific transformations. Their aim is to learn a single transformation rather than a distribution of transformations, making it distinct from data augmentation. More recently, Tamkin et al. [38] aim to learn instance-specific adversarial noise for self-supervised learning using the training set. They focus on the specific augmentation of additive noise (unlike InstaAug, which deals with more general and realistic augmentations). Luo et al. [25] also try to learn instance-specific augmentations. However, their application is mainly on the task of text recognition, because they rely on edit distance between text strings to measure the difficulty of augmentations, which is not available in more general cases that we consider.

Augerino. As an invariance-learning method, Augerino [2] is distinct from previous approaches in that it learns standard augmentations using a single training stage, without an extra validation set. InstaAug can be seen as a generalization of Augerino to allow instance-specific invariance and more flexible transformations such as crops. Augerino uses an objective that is similar to a Lagrangian relaxation of our objective, but we empirically found their approach to be unstable and highly dependent on initialization. See Appendix A for details of Augerino and direct comparisons.

4 Supervised Learning Experiments

In this section, we first construct several classification experiments so as to assess InstaAug’s ability to learn good instance-specific augmentations such as rotation, color jittering, and cropping. All experimental details can be found in Appendix C.
4.1 Rotated 2D images

First, we focus on a toy synthetic dataset proposed in Benton et al. [2]. The dataset contains four categories, (1) upright Mario; (2) upside-down Mario; (3) upright Iggy; and (4) upside-down Iggy. Each of the four base images is randomly rotated in the interval of $[-\pi/4, \pi/4]$ to form the training dataset. The task is to predict the correct character (Mario vs Iggy) and the orientation (up vs down). We assess whether InstaAug is able to learn the ‘best’ rotation range for each sample—i.e. the maximum range that avoids ‘up’ and ‘down’ classes from overlapping.

From Figure 5, we can see that InstaAug almost fully recovers the broadest range of rotations for each image while preserving labels. In contrast, Augerino only learns a subset of these ranges. For instance, for the bottom-right input image in Figure 5b showing an upright Mario rotated clockwise, we observe that InstaAug successfully learns an augmentation interval that is skewed towards anti-clockwise rotations. This is a consequence of the optimization problem Equation (1a) which tries to preserve the label while encouraging the diversity of rotations.

In contrast, Augerino learns a unique global augmentation distribution shared across all images. Thus, the learned invariance is overly conservative to avoid rotating images to the extent that their orientation (up/down) would be reversed. In particular, samples close to the $\pm\pi/4$ boundary force the learned augmentation distribution to have a maximum range of about $\pi/2$ to avoid transforming these boundary inputs into a region in which they would be misclassified.

4.2 Cropping

We now move to more realistic images and to the most common form of image augmentation: cropping. We use the Tiny-Imagenet (TinyIN) dataset at $64 \times 64$ resolution, as it inherits the image complexity of ImageNet, whilst being within our computational budget. TinyIN is a standard testbed for data augmentations that contains 100k images divided into 200 classes.

We benchmark our proposed model InstaAug alongside several augmentation baselines, including Augerino, no augmentation, and random resized crop (random augmentation). Random augmentation uniformly samples patch sizes and then randomly selects a patch inside the image. Since the effect of cropping crucially relies on scales of patches, we carefully tune this baseline by sweeping over all possible scale intervals between $[0, 1]$ with a stride of 0.1. We additionally compare to other prior works that have obtained competitive results on TinyIN [32, 44, 45]. Following prior works, we choose the PreActResNet-18 architecture [16] with width = 1 as the classifier for all methods, and we train models for 150 epochs with the same learning rate schedule.

![Figure 5: InstaAug learns a broader range of label preserving augmentations (longer green arcs) than Augerino on the Mario and Iggy dataset. The black circle represents the full rotational orbit of an image ($-\pi$ to $\pi$), whilst arcs in blue contain training samples. Green arcs show the learned transformation distributions for some examples.](image-url)

We benchmark our proposed model InstaAug alongside several augmentation baselines, including Augerino, no augmentation, and random resized crop (random augmentation). Random augmentation uniformly samples patch sizes and then randomly selects a patch inside the image. Since the effect of cropping crucially relies on scales of patches, we carefully tune this baseline by sweeping over all possible scale intervals between $[0, 1]$ with a stride of 0.1. We additionally compare to other prior works that have obtained competitive results on TinyIN [32, 44, 45]. Following prior works, we choose the PreActResNet-18 architecture [16] with width = 1 as the classifier for all methods, and we train models for 150 epochs with the same learning rate schedule.

| Method                | Instance | LRP | Accuracy (%) |
|-----------------------|----------|-----|--------------|
| MixMo [32]            | —        | —   | 64.80        |
| CutMix [44]           | —        | —   | 65.09        |
| Mixup [45]            | —        | —   | 63.74        |
| No augmentation       | ×        | ×   | 55.06±0.10   |
| Random augmentation   | ×        | ×   | 64.49±0.12   |
| Augerino [2]          | ×        | ×   | 55.02±0.29   |
| InstaAug (uniform param) | ✓      | ×   | 55.39±0.19   |
| InstaAug (global)     | ×        | ✓   | 63.20±0.12   |
| InstaAug              | ✓        | ✓   | 66.02±0.18   |
Figure 6: InstaAug (C) learns more sensible crops compared to random (A) and learned global (B) augmentations. Columns (a, b, e) show examples of random or learned cropping patches, where the relative probabilities of patches decrease as the color of their edges turn from red to yellow. Columns (c, f) are the density maps of the centers of medium-sized patches represented by the second layer of CNN in Figure 4, where bright color means higher probability; (d) and (g) are the learned proportions of medium (green) and large (red) patches for each image.

Table 1 shows the top-1 accuracy for each method. In agreement with prior work, we find that random cropping increases top-1 accuracy by 9.4% over no augmentation, which is achieved where cropping scale \( = [0.1, 1] \). InstaAug outperforms random cropping and the global version of InstaAug by 1.5% and 2.8% respectively, highlighting the effect of learning instance-specific augmentation. We also find model performance is generally not sensitive to the choice of the entropy interval \([H_{\text{min}}, H_{\text{max}}]\) in InstaAug. Any subinterval of \([3, 4]\) yields similar results as the best setting \((3.5, 4]\). But intervals below 3 or above 4 would lead to performance degradation because of insufficient or excessive augmentations. In order to ablate the effects of input-dependency and location-related parameterization on InstaAug, we additionally assess the performance of InstaAug (global) that also relies on the location-related parametrization (described in Figure 4) but shared across all inputs, and InstaAug (uniform param) which relies on the the same uniform parameterization as Augerino. We empirically observed that methods with mean-field uniform parameterization (including Augerino and InstaAug with uniform parameterization) are easily stuck in local minima with low cropping diversity, leading to similar performance as no augmentation. It shows the importance of location-related parameterization on cropping. Meanwhile, instance dependence allows InstaAug to outperform carefully tuned random augmentation.

Figure 6 shows the distribution of crops learned by InstaAug and baseline methods for a few samples. From columns (e-f) of rows (1-3), we find that InstaAug can successfully focus on the objects and generate informative cropping patches. However, in columns (b-c), global augmentation uses the same distribution to crop different images, which generates many patches focusing on the background, such as the sky or grassland. In row (4), we observe that InstaAug is able to learn a multi-modal distribution for 2 separate pieces of meat in the image, thanks to the location-related parameterization of the cropping distribution. From column (g), we observe that InstaAug learns a larger proportion of smaller patches than global augmentation, which is conservative and thus prefers larger patches, especially when the main object is small.
4.3 Color jittering on textures

Color jittering is another important type of data augmentation, which can help models generalize to various lighting conditions. We benchmark on the texture classification dataset RawFooT [3], a common testbed for color-related tasks. RawFooT includes 68 different samples of raw food and each sample has an image taken under each of 46 different lighting conditions. We crop the original images to create the train set and test set. For each original image with a resolution of 800 × 800, we randomly sample 200 different 200 × 200 patches in the upper half as training images. The same procedure is taken on the lower half to produce test images, giving a train set and a test set per lighting condition. To evaluate the generalization ability of each method to a broader range of lighting conditions, we evenly mix test images from all lighting conditions to form a general test set. See Figure C.1 for some examples of the dataset.

We first train on a single lighting condition D45 (4500K, daylight) resembling natural light. Table 2 shows that InstaAug outperforms all baselines with and without test time augmentation. In this task, we find that Augerino (with relaxed symmetry restrictions on learned intervals) underperforms random augmentation because its augmentation parameters $\phi$ are often stuck in a neighborhood around their initial values. We believe this is due to the conservative nature of using global augmentations (cf. Figure 3), where even a small change in the parameters may largely increase the training loss, which prohibits wide-ranging augmentations.

We also compare in-distribution and out-of-distribution generalization across different baselines by splitting the 46 test sets into two groups, according to the similarity of their lighting conditions to D45—see Appendix C.2 for the details on the splitting method. In Figure 7 we can see that above a certain in-distribution generalization performance, there exists a trade-off between in-distribution generalization and out-of-distribution generalization for different hyperparameter settings for random augmentation. InstaAug achieves superior performance in both metrics compared to almost all hyperparameter settings of the random augmentation baseline.

We can further vary the difficulty of the classification task by using different numbers of lighting conditions as training data. In Table 3, we randomly select a set number of lighting conditions to use as the training set for each baseline. As expected, the accuracy increases as we increase the number of lighting conditions for all methods. However, the effect of augmentation saturates: random augmentation performs similarly to no augmentation with 8 lighting conditions. In contrast, InstaAug always outperforms random augmentation. In Appendix C, we empirically show that this extra performance comes at very little computational overhead at both train and test time.

## 5 InstaAug for Contrastive Learning

Contrastive learning aims to learn features that are approximately invariant to certain augmentations. Typical contrastive learning methods, such as SimCLR [6, 12], first sample two independent transfor-
Table 3: InstaAug significantly outperforms baseline methods in general test accuracy (%) on different difficulty levels. For each difficulty level, we randomly sample lighting conditions used for training and repeat each experiment 10 times.

| Method / #Lighting conditions for training | 1          | 2          | 4          | 8          |
|------------------------------------------|------------|------------|------------|------------|
| No aug                                   | 68.5 ± 2.6 | 78.1 ± 1.8 | 84.8 ± 0.7 | 87.8 ± 0.5 |
| Random aug w/ test-time aug              | 72.7 ± 2.7 | 80.8 ± 1.3 | 85.9 ± 0.6 | 87.9 ± 0.3 |
| InstaAug w/ test-time aug                | **76.0 ± 2.5** | **83.6 ± 1.1** | **88.2 ± 0.5** | **89.6 ± 0.3** |

mations $\tau_1, \tau_2 \sim p(\tau)$, and apply them to an input image $x$ to generate two different views $x_1$ and $x_2$. Then they feed the transformed images to a neural encoder $f$ and train the encoder to maximize the relative similarity between $f(x_1)$ and $f(x_2)$, measured with a contrastive loss.

As the choice of augmentations directly influences the learned invariance of the encoder, it is a crucial ingredient of contrastive learning [1, 6, 39]. However, the current instance independent augmentations often introduce unrealistic assumptions. For example, if there are multiple entities in an image, such as grass and cattle in Figure 1c, contrastive learning with random cropping pulls features for different entities closer to each other. Consequently, we propose InstaAug as a more flexible instance-specific augmentation method for contrastive learning.

Applying InstaAug to contrastive learning is similar to the supervised case shown in Section 2. The main difference is, given an input $x$, we sample two $\tau$ independently from the input-specific distribution $p(\tau; \phi(x))$, before they are applied to $x$. The training objective is correspondingly changed to minimizing the contrastive loss while keeping the diversity in a reasonable range.

We again consider TinyIN and evaluate three methods: InstaAug, InstaAug with global augmentations, and random crop augmentation. We exclude methods with uniform parameterization, because of their poor performance in the simpler supervised setting. All experiments are based on the SimCLR framework and use the PreActResNet-18 network as the encoder. We train each model with a batch size of 512 for 500 epochs. We then train a linear classifier to evaluate feature quality. We use test time augmentation—over 10 sampled cropped patches—as it has been shown to improve performance [13].

From Table 4, we see that InstaAug outperforms random and InstaAug with global augmentation. We observe from the examples shown in Figure 8 that InstaAug focuses on the salient features containing important information. We also notice that the sizes of learned patches are correlated to the sizes of the main objects in images. We see that InstaAug is able to learn sensible instance-specific augmentations from the contrastive loss signal in a fully unsupervised setting.

Table 4: Representations learned by InstaAug perform better in the downstream linear classification task than baselines.

| Method            | Accuracy (%) |
|-------------------|--------------|
| Random aug        | 51.63 ± 0.30 |
| InstaAug (global) | 54.20 ± 0.23 |
| InstaAug          | **55.05 ± 0.21** |

6 Discussion

In this paper we introduced InstaAug, a method for learning instance-specific data augmentations. We highlighted the limitations of existing augmentation methods that rely on both instance independent and restricted classes of transformations. We introduced an augmentation module that parametrizes a distribution over transformations whose samples are used to augment the training data on the fly. The main benefits of our method stem from its applicability to a wide range of settings, its ease of use, and crucially its capacity to learn meaningful augmentations that in turn improve performance. Empirically, we demonstrated these benefits on a range of tasks—supervised and unsupervised—and several classes of transformations—rotation, color jittering, and cropping.
References

[1] Philip Bachman, R Devon Hjelm, and William Buchwalter. Learning representations by maximizing mutual information across views. Advances in neural information processing systems, 32, 2019.

[2] Gregory Benton, Marc Finzi, Pavel Izmailov, and Andrew Gordon Wilson. Learning invariances in neural networks. Advances in Neural Information Processing Systems, 2020.

[3] Simone Bianco, Claudio Cusano, Paolo Napoletano, and Raimondo Schettini. Improving cnn-based texture classification by color balancing. Journal of Imaging, 3(3):33, 2017.

[4] Anadi Chaman and Ivan Dokmanic. Truly shift-invariant convolutional neural networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3773–3783, 2021.

[5] Shuxiao Chen, Edgar Dobriban, and Jane H Lee. Invariance reduces variance: Understanding data augmentation in deep learning and beyond. 2019.

[6] Ting Chen, Simon Kornblith, Mohammad Norouzi, and Geoffrey Hinton. A simple framework for contrastive learning of visual representations. In International conference on machine learning, pp. 1597–1607. PMLR, 2020.

[7] Xiangning Chen, Cihang Xie, Mingxing Tan, Li Zhang, Cho-Jui Hsieh, and Boqing Gong. Robust and accurate object detection via adversarial learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 16622–16631, 2021.

[8] Tsz-Him Cheung and Dit-Yan Yeung. Adaaug: Learning class- and instance-adaptive data augmentation policies. In International Conference on Learning Representations, 2022. URL https://openreview.net/forum?id=rWXfFogxRJN.

[9] Taco Cohen and Max Welling. Group equivariant convolutional networks. In International conference on machine learning. PMLR, 2016.

[10] Ekin D Cubuk, Barret Zoph, Dandelion Mane, Vijay Vasudevan, and Quoc V Le. Autoaugment: Learning augmentation policies from data. Conference on Computer Vision and Pattern Recognition, 2018.

[11] Ekin D Cubuk, Barret Zoph, Jonathon Shlens, and Quoc V Le. Randaugment: Practical automated data augmentation with a reduced search space. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp. 702–703, 2020.

[12] Aleksandr Ermolov, Aliaksandr Siarohin, Enver Sangineto, and Nicu Sebe. Whitening for self-supervised representation learning. In International Conference on Machine Learning, pp. 3015–3024. PMLR, 2021.

[13] Adam Foster, Rattana Pukdee, and Tom Rainforth. Improving transformation invariance in contrastive representation learning. In International Conference on Learning Representations, 2021.

[14] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. Deep learning. MIT press, 2016.

[15] Ryuichi Hataya, Jan Zdenek, Kazuki Yoshizoe, and Hideki Nakayama. Faster autoaugment: Learning augmentation strategies using backpropagation. In European Conference on Computer Vision, pp. 1–16. Springer, 2020.

[16] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Identity mappings in deep residual networks. In European conference on computer vision, pp. 630–645. Springer, 2016.

[17] Daniel Ho, Eric Liang, Xi Chen, Ion Stoica, and Pieter Abbeel. Population based augmentation: Efficient learning of augmentation policy schedules. In International Conference on Machine Learning, pp. 2731–2741. PMLR, 2019.

[18] Max Jaderberg, Karen Simonyan, Andrew Zisserman, et al. Spatial transformer networks. Advances in neural information processing systems, 28, 2015.
[19] Olav Kallenberg and Olav Kallenberg. Foundations of modern probability, volume 2. Springer, 1997.

[20] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. In ICLR (Poster), 2015.

[21] Diederik P Kingma and Max Welling. Auto-encoding variational bayes. In International Conference on Learning Representations, 2014.

[22] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems, 25, 2012.

[23] Yonggang Li, Guosheng Hu, Yongtao Wang, Timothy Hospedales, Neil M Robertson, and Yongxin Yang. Dada: differentiable automatic data augmentation. arXiv preprint arXiv:2003.03780, 2020.

[24] Sungbin Lim, Ildoo Kim, Taesup Kim, Chiheon Kim, and Sungwoong Kim. Fast autoaugment. Advances in Neural Information Processing Systems, 2019.

[25] Canjie Luo, Yuanzhi Zhu, Lianwen Jin, and Yongpan Wang. Learn to augment: Joint data augmentation and network optimization for text recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 13746–13755, 2020.

[26] Clare Lyle, Mark van der Wilk, Marta Kwiatkowska, Yarin Gal, and Benjamin Bloem-Reddy. On the benefits of invariance in neural networks. arXiv preprint arXiv:2005.00178, 2020.

[27] Diego Marcos, Michele Volpi, Nikos Komodakis, and Devis Tuia. Rotation equivariant vector field networks. In Proceedings of the IEEE International Conference on Computer Vision, 2017.

[28] Agnieszka Mikołajczyk and Michał Grochowski. Data augmentation for improving deep learning in image classification problem. In 2018 international interdisciplinary PhD workshop (IIPhDW). IEEE, 2018.

[29] Mehdi Mirza and Simon Osindero. Conditional Generative Adversarial Nets. CoRR, abs/1411.1784, 2014. URL http://arxiv.org/abs/1411.1784.

[30] Luis Perez and Jason Wang. The effectiveness of data augmentation in image classification using deep learning. arXiv preprint arXiv:1712.04621, 2017.

[31] Jan Peters and Stefan Schaal. Policy gradient methods for robotics. In 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 2219–2225. IEEE, 2006.

[32] Alexandre Ramé, Rémy Sun, and Matthieu Cord. Mixmo: Mixing multiple inputs for multiple outputs via deep subnetworks. In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 823–833, 2021.

[33] Danilo Jimenez Rezende, Shakir Mohamed, and Daan Wierstra. Stochastic backpropagation and approximate inference in deep generative models. In International conference on machine learning, pp. 1278–1286. PMLR, 2014.

[34] Connor Shorten and Taghi M Khoshgoftaar. A survey on image data augmentation for deep learning. Journal of big data, 6(1):1–48, 2019.

[35] Kihyuk Sohn, Honglak Lee, and Xinchen Yan. Learning structured output representation using deep conditional generative models. In C. Cortes, N. Lawrence, D. Lee, M. Sugiyama, and R. Garnett (eds.), Advances in Neural Information Processing Systems, volume 28. Curran Associates, Inc., 2015. URL https://proceedings.neurips.cc/paper/2015/file/8d5a249e6baa5c06772297520da2051-Paper.pdf.

[36] Yang Song, Jascha Sohl-Dickstein, Diederik P Kingma, Abhishek Kumar, Stefano Ermon, and Ben Poole. Score-based generative modeling through stochastic differential equations. In International Conference on Learning Representations, 2021. URL https://openreview.net/forum?id=FzTIG12RRH5.
[37] Ivan Sosnovik, Michał Szmaja, and Arnold Smeulders. Scale-equivariant steerable networks. In *International Conference on Learning Representations*, 2019.

[38] Alex Tamkin, Mike Wu, and Noah Goodman. Viewmaker networks: Learning views for unsupervised representation learning. In *International Conference on Learning Representations*, 2020.

[39] Yonglong Tian, Chen Sun, Ben Poole, Dilip Krishnan, Cordelia Schmid, and Phillip Isola. What makes for good views for contrastive learning? *Advances in Neural Information Processing Systems*, 33:6827–6839, 2020.

[40] Ronald J Williams. Simple statistical gradient-following algorithms for connectionist reinforcement learning. *Machine learning*, 8(3):229–256, 1992.

[41] Daniel Worrall and Max Welling. Deep scale-spaces: Equivariance over scale. *Advances in Neural Information Processing Systems*, 2019.

[42] Daniel E Worrall, Stephan J Garbin, Daniyar Turmukhambetov, and Gabriel J Brostow. Harmonic networks: Deep translation and rotation equivariance. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2017.

[43] Jin Xu, Hyunjik Kim, Thomas Rainforth, and Yee Teh. Group equivariant subsampling. *Advances in Neural Information Processing Systems*, 2021.

[44] Sangdoo Yun, Dongyoon Han, Seong Joon Oh, Sanghyuk Chun, Junsuk Choe, and Youngjoon Yoo. Cutmix: Regularization strategy to train strong classifiers with localizable features. In *Proceedings of the IEEE/CVF international conference on computer vision*, pp. 6023–6032, 2019.

[45] Hongyi Zhang, Moustapha Cisse, Yann N Dauphin, and David Lopez-Paz. mixup: Beyond empirical risk minimization. In *International Conference on Learning Representations*, 2018.

[46] Richard Zhang. Making convolutional networks shift-invariant again. In *International Conference on Learning Representations*, 2019.

[47] Yu Zheng, Zhi Zhang, Shen Yan, and Mi Zhang. Metaaugment: Sample-aware data augmentation policy learning. *Thirty-Fifth AAAI Conference on Artificial Intelligence*, 2021.

[48] Allan Zhou, Tom Knowles, and Chelsea Finn. Meta-learning symmetries by reparameterization. *arXiv preprint arXiv:2007.02933*, 2020.

[49] Fengwei Zhou, Jiawei Li, Chuanlong Xie, Fei Chen, Lanqing Hong, Rui Sun, and Zhenguo Li. Metaaugment: Sample-aware data augmentation policy learning. *Thirty-Fifth AAAI Conference on Artificial Intelligence*, 2021.

[50] Yanzhao Zhou, Qixiang Ye, Qiang Qiu, and Jianbin Jiao. Oriented response networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2017.
Appendix A Details of Augerino

As a method to learn invariance, Augerino [2] is quite different from the previous approaches, which no longer require an extra validation set. The basic idea behind Augerino is to use a few parameters ($\theta$) to control the transformation distribution on input images and learn these parameters with the training loss of the classifier. Specifically, it minimizes the loss

$$L_{\lambda}(x; y) \triangleq \mathbb{E}[L(x; y)] + \lambda \cdot R(\theta), \quad (A.1a)$$

where $L(x; y)$ is the cross-entropy loss and $R(\theta)$ is a regularization function on the volume of the support of the distribution weighted by the hyper-parameter $\lambda$.

Comparison with InstaAug. InstaAug shares with Augerino the idea of tuning augmentation parameters by the classifier loss, but they are different in the following aspects. The most significant difference is that InstaAug is instance-specific, while Augerino learns global augmentations. Besides, Augerino uses a single scalar $\theta$ to parameterize a symmetric uniform distribution ($U(-\theta, \theta)$) over each type of transformations, which lacks the flexibility to model more complex augmentations, such as cropping.

In addition, Augerino uses a fixed weight $\lambda$ to balance the training loss and augmentation diversity. However, we find that, in more complicated settings, this is quite impractical. Specifically, we need different $\lambda$ in different stages of training. If we use a large $\lambda$ from the start of training, the diversity will quickly diverge to maximum, because the classifier is very weak and the loss is consequently dominated by the diversity term. This will block the training of the classifier because transformed samples from different classes are quite mixed with each other. Otherwise, if we choose a small $\lambda$, the diversity will converge to zero after a few epochs, yielding similar results as the vanilla model without augmentation. In neither of the case can we learn a useful augmentation. Consequently, InstaAug directly constrains the diversity to keep it stable during training.

Appendix B Method details

B.1 Regression and self-supervised learning

In Section 2, we use classification as an example to introduce InstaAug. However, InstaAug can be easily applied to other tasks including regression and self-supervised learning. For regression, the classifier (see Figure 2) is replaced by a regressor and the loss function $L$ in Equation (1a) is changed accordingly to absolute or square error. For self-supervised contrastive learning, we replace the classifier and cross-entropy loss with the feature extractor and contrastive loss (such as SimCLR loss [6]), respectively. In addition, the sampler samples 2 rather than 1 transformations to generate multiple views for an input $x$.

B.2 Implementation of location-related parameterization

As an example, we show how to implement location-related parameterization with a basic CNN structure in the following algorithm.

**Algorithm 1:** Location related parameterization

**Input:** Image $x$, channel numbers $M_i$, and layer number $n_{layer}$

**Output:** Probability of patches $p$

$F^0_0 = x$;

for ($i = 1; i \leq n_{layer}; i = i + 1$)

- $F^1_1 = \text{Conv2d}(F^1_{i - 1}, \text{kernel}=2, \text{stride}=1, \text{output}\_\text{channel}=M_i)$; \hspace{1cm} // CNN Operation
- $F^2_1 = \text{Pooling}(F^1_1, \text{kernel}=2)$; \hspace{1cm} // CNN Operation
- $F^3_1 = \text{Conv2d}(F^2_1, \text{kernel}=1, \text{stride}=1, \text{output}\_\text{channel}=1)$; \hspace{1cm} // To a single channel
- $\logit_i = \text{Flatten}(F^3_1)$; \hspace{1cm} // Logit vector at each level
- $\logits = \text{Concat}([\logit_i])$; \hspace{1cm} // Logit vector at all levels
- $p = \text{Normalize}(\text{Exp}(\logits))$; \hspace{1cm} // Probability after normalization
Appendix C Experimental details

C.1 Cropping

Supervised training Based on the Mixmo codebase\(^1\) [32], we use stochastic gradient descent (SGD) optimizer to train baselines and InstaAug. For the classifier, the initial learning rate is set to 0.2 (with momentum 0.9 and weight decay \(1e^{-4}\)). A scheduler is used to decrease the learning rate by a factor of 0.9 once validation accuracy doesn’t increase for 10 epochs. The learning rate of the augmentation module \(\phi\) is fixed at \(1e^{-5}\). Batch size is set to 100 and we pre-train InstaAug for 10 epochs without augmentation.

Contrastive training We directly apply InstaAug on the codebase\(^2\) from [12]. Because of the characteristics of contrastive learning, we set the batch size to 512. Same as the supervised case, we use SGD optimizer to train the augmentation module \(\phi\). Differently, we use Adam optimizer [20] (with learning rate \(1e^{-3}\) and weight decay \(1e^{-6}\)) to train the base model. We train each model for 500 epochs and decrease the learning rate by a factor of 0.8 at step 450 and 475.

C.2 Color jittering on textures

Training We use PreActResNet-18 (width = 1) on texture recognition task on RawFooT and train it with SGD optimizer. The learning rate is 0.02 (with momentum 0.9 and weight decay \(1e^{-4}\)) for the classifier and \(1e^{-5}\) for the augmentation module \(\phi\). We train each model for 50 epochs and learning rate schedulers are not necessary in this task.

Random augmentation baseline. We sweep over the variation range on each channel to find the best hyperparameters for the random augmentation baseline. For hue (h-jittering), we sweep between [0, 0.5] with stride 0.1, and for saturation (s-jittering) as well as brightness value (v-jittering), we sweep between [0, 1] with stride 0.2, which yields 216 different settings in total. The best accuracy shown in Table 2 is achieved where \(h, s, v = 0.0, 0.2, 0.8\).

\(^1\)https://github.com/alexrame/mixmo-pytorch.git, under Apache License v2.0.
\(^2\)https://github.com/htdt/self-supervised.git, under Apache License v2.0.
In-distribution vs. out-of-distribution generalization. To further investigate the effect of each augmentation method, we additionally split the 46 test sets into two equally-sized groups. The first group contains lighting conditions similar to D45, such as daylight with different temperatures, for which the vanilla model without augmentation trained on D45 has high test accuracy. The second group contains lighting conditions that are dramatically different from D45, for example, pure red light, which are more difficult for the vanilla method. Then the average accuracy on the first group can be regarded as a measure of in-distribution generalization, while the accuracy on the second group reflects out-of-distribution generalization.

C.3 Time complexity

We notice that InstaAug on color jittering has a similar training speed (0.37s/iter) as random augmentation (0.40s/iter) on a single Nvidia 1080Ti GPU, though it takes more epochs (about 40) compared with random augmentation, which usually converges after 25 epochs. We also find the speed for evaluation is very fast even with test time augmentation (sample number =10), which is about 0.004s/sample. However, the training speed of InstaAug on cropping (0.25s/iter) is slower than random augmentation (0.15s/iter) due to optimization issues on the more complex parameterization method. The evaluation speed is 0.011s/sample when sample number is set to 50 for test-time augmentation.

Appendix D Additional Results

D.1 RawFooT

Figure D.1 shows some examples of learned color jittering. Though it’s not easy to fully understand them, we can still find some patterns. For example, InstaAug tends to increase the brightness of darker images (row 1 and 3) and decrease the brightness of brighter images (row 4). Also InstaAug is more likely to change saturation compared with hue and brightness, which is consistent with the common belief that saturation contains less information than hue and brightness. InstaAug’s behavior is quite different on different samples. It even decides not to augment the H and V channels of the image in the second row. In comparison, Augerino adds or multiplies noise to each channel with the same distribution across all samples, which is harmful in many cases. For example, the input image in the last row is already very bright, but Augerino allows further increasing its brightness. Then brightness values of many pixels will be capped at 1.0, which leads to loss of information.

| Group   | Lighting id   |
|---------|---------------|
| Easy (1) | 1-4,10,14-31  |
| Hard (2) | 5-9, 11-13, 32-46 |

Figure D.1: Examples of learned color jittering. (a) Original image; (b, f) Average hue (H) of original image (blue dot) and learned hue jittering (red arc) for InstaAug and Augerino, respectively; (c) learned saturation (S) and brightness value (V) of original image (blue dot) and learned hue jittering (red line segment) for InstaAug and Augerino, respectively; (d) and (e) Examples of transformed images by InstaAug.