
Contrastive Learning with Adversarial Examples

Chih-Hui Ho Nuno Vasconcelos
Department of Electrical and Computer Engineering
University of California, San Diego
{chh279, nvasconcelos}@ucsd.edu

Abstract

Contrastive learning (CL) is a popular technique for self-supervised learning (SSL) of visual representations. It uses pairs of augmentations of unlabeled training examples to define a classification task for pretext learning of a deep embedding. Despite extensive works in augmentation procedures, prior works do not address the selection of challenging negative pairs, as images within a sampled batch are treated independently. This paper addresses the problem, by introducing a new family of adversarial examples for contrastive learning and using these examples to define a new adversarial training algorithm for SSL, denoted as CLAE. When compared to standard CL, the use of adversarial examples creates more challenging positive pairs and adversarial training produces harder negative pairs by accounting for all images in a batch during the optimization. CLAE is compatible with many CL methods in the literature. Experiments show that it improves the performance of several existing CL baselines on multiple datasets.

1 Introduction

Deep networks have enabled significant advances in many machine learning tasks over the last decade. However, this usually requires supervised learning, based on large and carefully curated datasets. Self-supervised learning (SSL) [25] aims to alleviate this limitation, by leveraging unlabeled data to define surrogate tasks that can be used for network training. Early advances in SSL were mostly due to the introduction of many different surrogate tasks [2, 51, 34, 78, 81, 33], including solving image [47, 27] or video [3] puzzles, filling image patches [51, 15, 44] or discriminating between image rotations [18]. Recently, there have also been advances in learning techniques specifically tailored to SSL, such as contrastive learning (CL) [78, 12, 22, 74, 63, 23, 55, 39], which is the focus of this paper. CL is based on a surrogate task that treats instances as classes and aims to learn an invariant instance representation. This is implemented by generating a pair of examples per instance, and feeding them through an encoder, which is trained with a contrastive loss. This encourages the embeddings of pairs generated from the same instance, known as positive pairs, to be close together and embeddings originated from different instances, known as negative pairs, to be far apart.

The design of positive pairs is one of the research focuses of CL [5]. These pairs can include data from one or two modalities. For single-modality approaches, a common procedure is to rely on data augmentation techniques. For example, instances from image datasets are frequently subject to transformations such as rotation, color jittering, or scaling [12, 78, 22, 74, 39] to generate the corresponding pairs. This type of data augmentation has been shown critical for the success of CL, with different augmentation approaches having a different impact on SSL performance [12]. For video datasets, positive pairs are usually derived from temporal coherence constraints [56, 21]. For multi-view data, augmentations can be more elaborate. For example, [63] considers augmentations of color channels, depth or surface normal and shows that the performance of CL improves as the augmentations increase in diversity. Multi-modal CL approaches tend to rely on audio and video from a common video clip to design positive pairs [52]. In general, CL benefits from definitions of positive pairs that pose a greater challenge to the learning of the invariant instance representation.

34th Conference on Neural Information Processing Systems (NeurIPS 2020), Vancouver, Canada.

Unlike the plethora of positive pair selection proposals, the design of negative pairs has received less emphasis in the CL literature. Since CL resembles approaches such as noise contrastive estimation (NCE) [20] and N-pair [59] losses, it can leverage hard negative pair mining schemes proposed for these approaches [7, 59]. However, because they treat each instance independently, previous SSL works do not consider CL algorithms that select difficult negative pairs within a batch. This is unlike CL methods based on metric learning [30, 59, 54, 62], which seek to construct batches with challenging negative samples.

In this work, we seek a general algorithm for the generation of diverse positive and challenging negative pairs. This is framed as the search for instance augmentation sets that induce the largest optimization cost for CL. A natural approach to synthesize these sets is to leverage adversarial examples [79, 10, 19, 11, 76, 76], which are crafted to attack the network and can thus be seen as the most challenging examples that it can process. We note that the goal is not to enhance robustness to adversarial attacks, but to produce a better representation for SSL. This is in line with recent studies in the adversarial literature, showing that adversarial examples can be used to improve supervised [75, 77] and semi-supervised [41] learning. We explore whether the same benefits can ensue for SSL. One difficulty is, however, that no attention has been previously devoted to the design of adversarial attacks for SSL, where no class labels are available. In fact, for SSL embeddings trained by CL, the classical definition of adversarial attack does not even apply, since CL operates on pairs of examples. We show, however, that it is possible to leverage the interpretation of CL as instance classification to produce a sensible generalization of classification attacks to the CL problem. The new attacks are then combined with recent techniques from the adversarial literature [75, 77], which treat adversarial training as multi-domain training, to produce more invariant representations for SSL.

Overall, the paper makes three contributions. First, we show that adversarial data augmentation can be used to improve the performance of SSL learning. Second, we propose a novel procedure for training *Contrastive Learning with Adversarial Examples (CLAE)* for SSL models. Unlike the attacks classically developed in the supervised learning literature, the new attacks produce pairs of examples that account for both the positive and negative pairs in a batch to maximize contrastive loss. To the best of our knowledge neither the use of attacks to improve SSL nor the design of adversarial examples with this property have been previously discussed in the literature. Finally, extensive experiments demonstrate that (1) adversarial examples can indeed be leveraged to improve CL, and (2) CLAE boosts the performance of several CL baselines across different datasets.

2 Related work

Since this work focuses on image classification tasks, our survey of previous work concentrates on contrastive learning (CL) and adversarial examples for image classification.

2.1 Contrastive learning

Contrastive learning has been widely used in the metric learning literature [13, 71, 54] and, more recently, for self-supervised learning (SSL) [68, 74, 78, 63, 22, 12, 39, 55, 23], where it is used to learn an encoder in the pretext training stage. Under the SSL setting, where no labels are available, CL algorithms aim to learn an invariant representation of each image in the training set. This is implemented by minimizing a contrastive loss evaluated on pairs of feature vectors extracted from data augmentations of the image. While most CL based SSL approaches share this core idea, multiple augmentation strategies have been proposed [74, 78, 63, 22, 12, 39]. Typically, augmentations are obtained by data transformation (i.e. rotation, cropping, random grey scale and color jittering) [78, 12], but there have also been proposals to use different color channels, depth, or surface normals as the augmentations of an image [63]. Another approach is to use an augmentation dictionary composed of the embedding vectors from the previous epoch [74] or obtained by forwarding an image through a momentum updated encoder [22]. This diversity of approaches to the synthesis of augmentations reflects the critical importance of using semantically similar example pairs in CL [5]. This has also been studied empirically in [12], showing that stronger data augmentations improve CL performance.

Despite this wealth of augmentation proposals for SSL, most CL algorithms fail to mine hard negative pairs or relate the image instances within a batch. While [70, 40, 12, 66] have mentioned the importance of selecting negative pairs, they do not propose a systematic algorithm to do this. Since

CL is inspired by the noise contrastive estimation (NCE) [20] and N-pair [59] loss methods from metric learning, it inherits the well known difficulties of hard negative mining in this literature [73, 59, 54, 62, 30, 58, 50, 60]. For metric learning methods [54, 60, 30, 59], the number of possible positive and negative pairs increases dramatically (for example, cubically when the triplet loss is used [54]) as the dataset increases. A solution used by NCE is to draw negative samples from a noise distribution that treats all negative samples equally [7, 8].

Unlike all these prior efforts, this work proposes to use “adversarial augmentations” as challenging training pairs that maximize the contrastive loss. However, unlike hard negative mining in metric learning, no class labels are provided in SSL. Hence, the consideration of how all images in the batch relate to each other is necessary for generating hard negative pairs.

2.2 Adversarial examples

Adversarial examples are created from clean examples to produce adversarial attacks that induce a network in error [79, 10, 19]. They have been used in many supervised learning scenarios, including image classification [19, 31, 48, 43, 9, 42, 61], object detection [11, 76, 16, 82] and segmentation [76, 4]. Typically, to defend against such attacks and increase network robustness, the network is trained with both clean and adversarial examples, a process referred as adversarial training [57, 65, 32, 35, 79, 77]. It is also possible to leverage SSL to increase robustness against unseen attacks [45]. While adversarial training is usually effective as a defense mechanism, there is frequently a decrease in the accuracy of the classification of clean examples [80, 64, 67, 75, 35].

This effect has been attributed to overfitting to the adversarial examples [35] but remains somewhat of a paradox, since the increased diversity of adversarial examples could, in principle, improve standard training [24], e.g. by enabling models trained on adversarial examples to generalize better to unseen data [69, 36]. In summary, while adversarial examples could assist learning, it remains unclear how to do this. Recently, [75, 77] have made progress along this direction, by introducing a procedure, denoted AdvProp, that treats clean and adversarial examples as samples from different domains, and uses a different set of batch normalization (BN) layers for each domain. This aims to align the statistics of the embedding of clean and adversarial samples, such that both can contribute to the network learning, and has been previously shown successful for multi-domain classification problems [6, 53].

The proposed framework CLAE is inspired by recent advances in the adversarial example literature, yet parallel to them. Unlike these methods, we aim to leverage the strength of adversarial example for SSL, where no labels are available, and the focus on pairs rather than single examples requires an altogether different definition of adversaries. Our aim is to use adversarial training to compensate the limitation of current CL algorithms, by both generating challenging positive pairs and mining effective hard negative pairs for the optimization of the contrastive loss. Note that the goal is to produce better embeddings for CL, rather than robustifying CL embeddings against attacks.

3 Leveraging adversarial examples for improved contrastive learning

In this section, we introduce the approach proposed to create adversarial examples for CL, and a novel training scheme CLAE that leverages these examples for improved contrastive learning (CL).

3.1 Supervised learning

A classifier maps example $x \in \mathcal{X}$ into label $y \in \{1, \dots, C\}$, where C is a number of classes. A deep classifier is implemented by the combination of an embedding $f_\theta(x)$ of parameters θ and a softmax regression layer that predicts the posterior class probabilities

$$P_{Y|X}(i|x) = \frac{e^{w_i^T f_\theta(x)}}{\sum_k e^{w_k^T f_\theta(x)}}, \quad (1)$$

where w_i is the vector of classification parameters of class i . Given a training set $\mathcal{D} = \{x_i, y_i\}$, the parameters θ and $\mathcal{W} = \{w_i\}_{i=1}^C$ are learned by minimizing the risk $\mathcal{R} = \sum_i L(x_i, y_i; \mathcal{W}, \theta)$ defined

by the cross-entropy loss

$$L_{ce}(x, y; \mathcal{W}, \theta) = -\log \frac{e^{w_y^T f_\theta(x)}}{\sum_k e^{w_k^T f_\theta(x)}}. \quad (2)$$

Given the learned classifier, the untargeted adversarial example x^{adv} of a clean example x is

$$x^{adv} = x + \delta \quad s.t. \quad \|\delta\|_p < \epsilon \text{ and } \arg \max_i w_i^T f_\theta(x) \neq \arg \max_i w_i^T f_\theta(x^{adv}), \quad (3)$$

where δ is an adversarial perturbation of L_p norm smaller than ϵ . The optimal perturbation for x is usually found by maximizing the cross-entropy loss, i.e.

$$\delta^* = \arg \max_{\delta} L_{ce}(x + \delta, y; \mathcal{W}, \theta) \quad s.t. \quad \|\delta\|_p < \epsilon, \quad (4)$$

although different algorithms [79, 10] use different strategies to solve this optimization.

3.2 Contrastive learning

In SSL, the dataset is unlabeled, i.e. $\mathcal{U} = \{x_i\}$, and each example x is mapped into an example pair (x^p, x^q) . In this work, we consider applications where x is an image and the pair is generated by data augmentation. This consists of applying a transformation p (q) in some set of transformations \mathcal{T} (e.g. spatial transformations, color transformations, etc.) to x , to produce the *augmentation* x^p (x^q). CL seeks to learn an invariant representation of image x_i by minimizing the risk defined by the loss

$$L_{cl}(x_i^{p_i}, x_i^{q_i}; \theta, \mathcal{T}) = -\log \frac{\exp(f_\theta(x_i^{p_i})^T f_\theta(x_i^{q_i})/\tau)}{\sum_{k=1}^B \exp(f_\theta(x_i^{p_k})^T f_\theta(x_i^{q_i})/\tau)}, \quad p_i, q_i \sim \mathcal{T} \quad (5)$$

where f is an embedding parameterized by θ , τ is the temperature, B is the batch size and $x_i^{p_i}, x_i^{q_i}$ are augmentations of x_i under transformations p_i, q_i randomly sampled from \mathcal{T} . Previous works on CL have considered many possibilities for the set of transformations \mathcal{T} . While [12] has shown that the choice of \mathcal{T} has a critical role on SSL performance, most prior works do not give much consideration to the **individual choice of p_i and q_i** , which are simply uniformly sampled over \mathcal{T} . In this work, we seek to go beyond this and select *optimal* transformations for each image x_i . More precisely, we seek augmentations that maximize the risk defined by the loss of (5), i.e.

$$\{p_i^*, q_i^*\} = \arg \max_{\{p_i, q_i\} \in \mathcal{T}} \sum_i L_{cl}(x_i^{p_i}, x_i^{q_i}; \theta, \mathcal{T}). \quad (6)$$

This is, in general, an ill-defined problem since, for each example x_i , what matters is the difference between the two transformations, not their absolute values.

3.3 Adversarial augmentation

This ambiguity can be eliminated by fixing one of the transformations of (5), i.e. solving instead

$$\{p_i^*\} = \arg \max_{\{p_i\} \in \mathcal{T}} \sum_i L_{cl}(x_i^{p_i}, x_i^{q_i}; \theta, \mathcal{T}), \quad q_i \sim \mathcal{T} \quad (7)$$

for a given set of $\{q_i\}$ sampled randomly from \mathcal{T} . However, it is usually difficult to search over the set \mathcal{T} efficiently. Instead, we proposed to replace $x_i^{p_i}$ by an adversarial perturbation of $x_i^{q_i}$, i.e. find

$$x_i^{r_i} = \arg \max_{x \in \mathcal{A}(x_i^{q_i})} L_{cl}(x, x_i^{q_i}; \theta, \mathcal{T}), \quad q_i \sim \mathcal{T} \quad (8)$$

where $\mathcal{A}(x_i^{q_i})$ is a set of adversarial perturbations of $x_i^{q_i}$, defined by

$$\mathcal{A}(x) = \{x' | x' = x + \delta, \|\delta\|_p < \epsilon\}. \quad (9)$$

In summary, given a set of transformations \mathcal{T} and a set of augmentations $x_i^{q_i}$, the goal is to learn the adversaries $x_i^{r_i} = x_i^{q_i} + \delta_i^*$, by finding the perturbations δ_i^* that lead to the most diverse positive pairs $(x_i^{r_i}, x_i^{q_i})$. The rationale is that the use of these pairs in (5) increases the challenge of unsupervised learning, encouraging the learning algorithm to produce a more **invariant representation**.

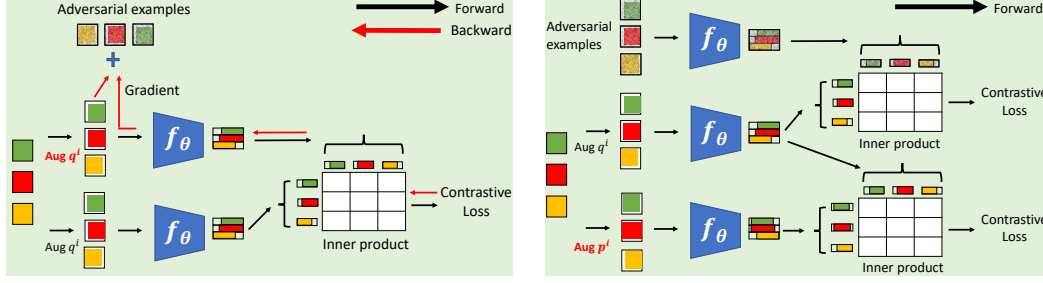


Figure 1: (Left) Generation of adversarial augmentations in step 4 of Algorithm 1 (Right) Adversarial training with contrastive loss in step 5 of Algorithm 1.

Algorithm 1 Pseudocode of contrastive learning with adversarial example (CLAE) in a batch

- 1: **Input** $\mathcal{X} = \{x_i\}_{i=1}^B$, $AUG :=$ Data Augmentation, Hyperparameter α
- 2: $\mathcal{W}^p = \{x_i^{p_i}\}_{i=1}^B = AUG(\mathcal{X})$
- 3: $\mathcal{W}^q = \{x_i^{q_i}\}_{i=1}^B = AUG(\mathcal{X})$
- 4: Compute (15) with $\{x_i^{q_i}\}_{i=1}^B$ and \mathcal{W}^q to obtain \mathcal{W}^*
- 5: Compute L_{aug} of (16) with $\{x_i^{q_i}\}_{i=1}^B$ and \mathcal{W}^p , and L_{adv} of (16) with $\{x_i^{q_i}\}_{i=1}^B$ and \mathcal{W}^*
- 6: Minimize (16) with hyperparameter α

To optimize (8), we start by noting that the contrastive loss of (5) can be written as the cross-entropy loss of (2)

$$L_{cl}(x_i^{p_i}, x_i^{q_i}; \theta, \mathcal{T}) = -\log \frac{\exp(w_i^T f_\theta(x_i^{q_i}))}{\sum_{k=1}^B \exp(w_k^T f_\theta(x_i^{q_i}))} = L_{ce}(x_i^{q_i}, i; \mathcal{W}^p, \theta) \quad (10)$$

by defining the classifier parameters \mathcal{W}^p as $w_k = f_\theta(x_k^{p_k})/\tau$. As above, we can replace each $x_i^{p_i}$ by the optimal adversarial perturbation $x_i^{r_i} \in \mathcal{A}(x_i^{q_i})$, to obtain an optimal set of perturbed parameters $\mathcal{W}^* = \{f_\theta(x_k^{r_k})/\tau\}$ by solving

$$\{x_k^{r_k}\} = \arg \max_{\{x_k \in \mathcal{A}(x_k^{q_k})\}} \sum_i L_{ce}(x_i^{q_i}, i; \{f_\theta(x_k)/\tau\}, \theta), \quad q_i \sim \mathcal{T}. \quad (11)$$

Note that this requires the determination of the optimal adversarial perturbation $x_i^{r_i}$ for the augmentation $x_i^{q_i}$ of each example x_i in the batch. Using the definition of adversarial set of (9) in (11), results in the optimization

$$\{\delta_k^*\} = \arg \max_{\{\delta_k\}} \sum_i L_{ce}(x_i^{q_i}, i; \{f_\theta(x_k^{q_k} + \delta_k)/\tau\}, \theta) \quad s.t. \quad \|\delta_k\|_p < \epsilon, \quad q_i \sim \mathcal{T}. \quad (12)$$

This is an optimization similar to (4), but with a significant difference. While in (4) δ is a perturbation of the classifier input, in (12) it is a perturbation of the classifier weights. This implies that δ_k appears in the denominator of (10) for all $x_i^{q_i}$ in the batch and forces the optimization to account for all images simultaneously. In result, the embedding is more strongly encouraged to bring together the positive pairs $(x_i^{r_i}, x_i^{q_i})$ and separate all perturbations of different examples, i.e. the optimization seeks both challenging positive and negative pairs, performing hard negative mining as well.

3.4 FSGM attacks for unsupervised learning

The optimization of (12) can be performed for any set of transformations \mathcal{T} . Hence, the procedure can be applied to most CL methods in the literature. The optimization can also be implemented with most adversarial techniques in the literature. In this work, we rely on untargeted attacks with the popular fast gradient sign method (FGSM) [19]. For supervised learning, an untargeted FGSM attack consists of

$$x^{adv} = x + \delta = x + \epsilon \text{sign}(\nabla_x L_{ce}(x, y; \mathcal{W}, \theta)) \quad \|\delta\|_2 < \epsilon, \quad (13)$$

where L_{ce} is the cross-entropy loss of (2). Similarly, to obtain δ_k^* of (12), the first order derivative of (12) is computed at $x_k^{q_k}$ to obtain $x_k^{r_k}$ with

$$x_k^{r_k} = x_k^{q_k} + \delta_k^* = x_k^{q_k} + \epsilon \text{sign} \left(\nabla_{x_k^{q_k}} \sum_i L_{ce}(x_i^{q_i}, i; \{f_\theta(x_k^{q_k})/\tau\}, \theta) \right) \quad (14)$$

$$= x_k^{q_k} + \epsilon \text{sign} \left(\nabla_{x_k^{q_k}} \sum_i L_{ce}(x_i^{q_i}, i; \mathcal{W}^q, \theta) \right), \quad \|\delta_k\|_2 < \epsilon \quad (15)$$

Note that, due to this, the optimal set of adversarial augmentations $\mathcal{W}^* = \{f_\theta(x_k^{r_k})/\tau\}$ takes into consideration the relationship between all instances within the sampled batch.

3.5 Adversarial training with contrastive loss

To perform adversarial training, we adopt the training scheme of AdvProp [75], which uses two separate batch normalization (BN) layers for clean and adversarial examples. Unlike [75, 77], we set the momentum for the two BN layers differently. The momentum of the BN layer associated with clean examples is fixed to the value used by the original CL algorithm, while a larger momentum is used empirically for the BN layer associated with adversarial examples. The overall loss function is obtained by combining (10) and (15),

$$\arg \min_{\theta} \sum_{i=1}^B L_{ce}(x_i^{q_i}, i; \mathcal{W}^p, \theta) + \alpha \sum_{i=1}^B L_{ce}(x_i^{q_i}, i; \mathcal{W}^*, \theta) = \arg \min_{\theta} L_{aug} + \alpha L_{adv}, \quad (16)$$

where α balances between contrastive loss L_{aug} parametrized with \mathcal{W}^p and L_{adv} parametrized with \mathcal{W}^* . The proposed procedure for CLAE is summarized in Algorithm 1 and visualized in Fig.1. Given augmentations $x_i^{q_i}$, adversarial examples are created by backpropagating the gradients of the contrastive loss to the network input. Contrastive loss terms are then computed for standard augmentation pairs and pairs composed by the augmentations $x_i^{q_i}$ and their adversarial examples, and combined with (16) to train the network.

3.6 Generalization to other contrastive learning approaches

While Algorithm 1 is based on the plain contrastive loss of (5), CLAE can be generalized to many other CL approaches in the literature. For example, UEL [78] uses an extra objective function to discourage different images from being recognized as the same instance. SimCLR [12] uses a projection head to avoid loss of information during pretext training and discards the projection head when optimizing the downstream task. To generalize Algorithm 1 to these approaches, it suffices to replace the plain contrastive loss with the loss functions on which they are based.

4 Experiments

In this section, we discuss an experimental evaluation of adversarial contrastive learning.

4.1 Setup

Experiments are performed on CIFAR10 [29], CIFAR100 [29] or tinyImagenet [1], using three different contrastive loss baselines: the loss of (5) (denoted as "Plain"), UEL [78] and SimCLR [12]. Unless otherwise noted, a Resnet18 encoder is trained using Algorithm 1 with $\alpha = 1$, standard Pytorch augmentation, and an adversarial batchnorm momentum of 0.01¹. Two evaluation protocols are used, both based on a downstream classification task using features extracted by the learned encoder. These are implemented with a $k = 200$ nearest neighbor (kNN) classifier, and a logistic regression layer (LR). The encoder is trained with batch size 256 (128) and LR is trained for 1000 (200) epochs for CIFAR10 and CIFAR100 (tinyImagenet). See supplementary for more details.

¹Or, equivalently 0.99 for Tensorflow implementation

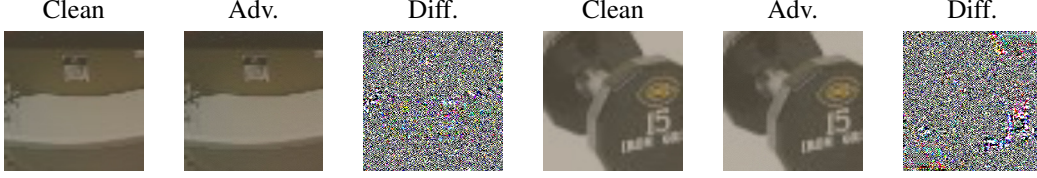


Figure 2: Adversarial examples computed with Algorithm 1 on tinyImagenet. The difference is amplified for visualization purpose.

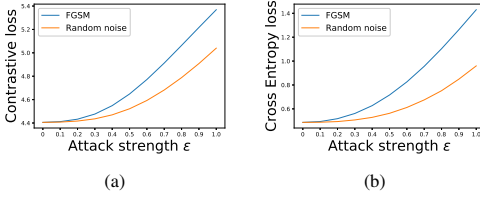


Figure 3: Effect of adversarial and random perturbations on (a) contrastive and (b) cross entropy losses.

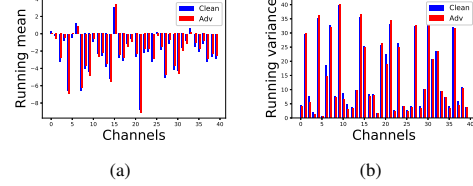


Figure 4: Running mean (a) and variance (b) of batch normalization for clean and adversarial examples, from randomly selected channels.

4.2 Influence of adversarial example

In this section, we study the effect of adversarial examples on both the SSL surrogate and downstream tasks. We compare the adversarial attacks of Algorithm 1 to random additive perturbations of the same magnitude. Fig. 3(a) shows the magnitude of the contrastive loss of the pretext task, on CIFAR10. For a given perturbation strength ϵ , adversarial perturbations (blue) elicit a larger loss than random ones (red). Fig. 3(b) shows that, when the adversarial augmentations are fed into the downstream classification model, they elicit a larger cross entropy loss than random noise. This shows that adversarial augmentation produces more challenging pairs than random perturbations. Examples of adversarial augmentation are visualized in Fig. 2.

Nevertheless, there are some significant differences to the typical behaviour of adversarial examples in the supervised setting. First, the effect of adversarial attacks is weaker for SSL. In the SSL setting, adversarial examples only degrade the downstream classification accuracy by 20%. This is much weaker than previously reported for the supervised setting, using the adversarial examples of (4). Second, as illustrated in Fig. 4, the statistics of the batch normalization layers differ less between clean and adversarial examples than reported for supervised learning in [77]. Both of these observations are explained by the fact that, while the classifier parameters of (2) remain stable across training, those of (10) vary between batches. This creates uncertainty in the perturbation direction of (15), decreasing the differences between clean and adversarial attacks under the SSL setting.

4.3 Comparison to contrastive learning baselines

In this section, we investigate the gains of using CLAE framework for SSL, and the consistency of these gains across CL approaches. Table 1 shows the downstream classification accuracy for the two classifiers and three CL methods considered in these experiments. Note that adversarial training reduces to these methods when $\epsilon = 0$, in which case no adversarial examples are used. It can be seen that adversarial training improves the performance of all CL algorithms on all datasets, with a gain that is consistent across downstream classifiers. While best performance is achieved by using $\epsilon = 0.03$ in (15), $\epsilon = 0.07$ still beats the baseline in most cases.

4.4 Ablation study

An ablation study was conducted using the combination of SimCLR [12] and LR classifier. The study was performed on both CIFAR100 and tinyImagenet, with qualitatively identical results. We present CIFAR100 results here and tinyImagenet on the supplementary.

Batch size Fig. 5(a) shows that larger batch sizes improve the performance of both baseline and adversarial training. While this is consistent with the conclusions of previous studies on the importance of batch size [12, 26], adversarial training makes large batch sizes less critical. Besides outperforming the baseline for all batch sizes, it frequently achieves better performance with smaller sizes. For

Table 1: Downstream classification accuracy for three SSL methods, with and without ($\epsilon = 0$) adversarial augmentation, on different datasets.

Method	ϵ	kNN		LR		
		Cifar10	Cifar100	Cifar10	Cifar100	tinyImageNet
Plain	0	82.78 \pm 0.20	54.73 \pm 0.20	79.65 \pm 0.43	51.82 \pm 0.46	31.71 \pm 0.23
	0.03	83.09\pm0.19	55.28\pm0.12	79.94\pm0.28	52.04 \pm 0.32	32.82\pm0.10
	0.07	83.04 \pm 0.18	54.96 \pm 0.12	79.85 \pm 0.16	52.14\pm0.21	32.71 \pm 0.22
UEL	0	83.63 \pm 0.14	55.23 \pm 0.28	80.63 \pm 0.18	52.99 \pm 0.25	32.32 \pm 0.30
	0.03	84\pm0.15	55.96\pm0.06	80.94\pm0.13	54.27\pm0.40	33.72\pm0.30
	0.07	83.72 \pm 0.19	55.36 \pm 0.22	80.82 \pm 0.12	53.90 \pm 0.11	33.16 \pm 0.36
SimCLR	0	75.92 \pm 0.26	34.94 \pm 0.25	83.27 \pm 0.17	53.79 \pm 0.21	40.11 \pm 0.34
	0.03	76.45 \pm 0.32	38.89\pm0.25	83.32\pm0.26	55.52\pm0.30	41.62\pm0.20
	0.07	76.70\pm0.36	38.41 \pm 0.21	83.13 \pm 0.22	54.96 \pm 0.20	41.46 \pm 0.22

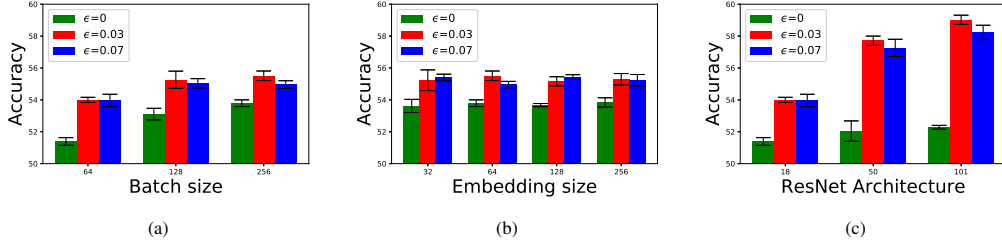


Figure 5: Ablation study of (a) batch sizes, (b) embedding dimensions and (c) ResNet architectures.

example, adversarial training with $\epsilon = 0.03$ and batch size 64 (54%) outperforms the baseline with batch size 256 (53.79%). This suggests that adversarial training is both more robust and efficient.

Embedding dimension impact is evaluated in Fig. 5(b). This dimension does not seem to affect the performance of both baseline and adversarially trained model.

Architecture The impact of different architectures is evaluated in Fig. 5(c), showing that larger networks have better performance. However, the improvement is much more dramatic with adversarial training (red bar), where it can be as high as 5% (ResNet101 over ResNet18), than for the baseline (green bar), where it is at most 1%. This is likely because larger networks have higher learning capacity and can benefit from the more challenging examples produced by adversarial augmentation. Nevertheless, the fact that the ResNet18 with adversarial training beats the ResNet101 baseline shows that there is always a benefit to more challenging training pairs, even for smaller models.

Hyperparameter α weights the contributions of the two losses (L_{aug} and L_{adv}) of (16). Fig. 6(a) shows downstream classification accuracy when α varies from 0 to 2, for $\epsilon = 0.03$. Accuracy starts to increase with $\alpha = 0.2$ and reaches its peak around $\alpha = 0.8$, but performance is fairly stable for $\alpha > 0.2$. There is no significant accuracy drop when the importance of adversarial examples is weighted by as much as twice that of clean examples ($\alpha = 2$). This shows that the features derived from the adversarial examples benefit learning.

Attack strength ϵ is studied in Fig. 6(b), which shows that adversarial training consistently beats the baseline ($\epsilon = 0$). Again, the performance is quite stable with ϵ . This is possibly due to the affect of batch normalization, which aligns the statistics of embeddings from clean and adversarial examples.

Epoch While the default setting of SimCLR is to use 100 training epochs, there are usually gains in using longer pretext training, as shown in Fig. 6(c). While all methods benefit from this, adversarial training consistently beats the baseline. It is also observed that the larger perturbation of $\epsilon = 0.07$ benefits more from longer pretext training than smaller perturbations. Finally, training with adversarial

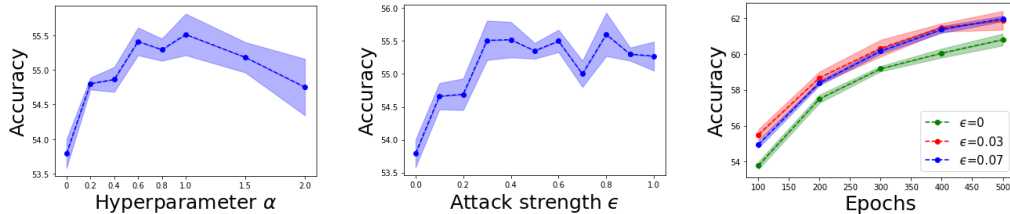


Figure 6: Ablation study for (a) hyperparameter α , (b) attack strength ϵ and (c) longer pretext training.

Table 2: Comparison of transfer learning performance with linear evaluation to other image datasets.

	CIFAR10	CIFAR100	Cars	Aircraft
SimCLR	72.8 \pm 0.3	45.3 \pm 0.1	12.25 \pm 0.0	14.8 \pm 0.9
CLAE	73.6\pm0.3	47.0\pm0.2	12.60 \pm0.1	16.2\pm0.6
	DTD	Pets	Caltech-101	Flowers
SimCLR	50.6 \pm 1.2	44.4 \pm0.4	68.2 \pm 0.3	46.0 \pm 0.3
CLAE	51.5\pm0.5	44.4\pm0.0	69.1\pm0.3	47.1\pm0.8

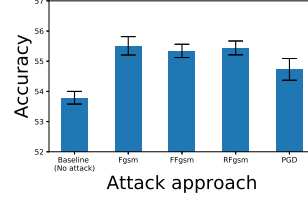


Figure 7: Comparison of different attack methods.

augmentation is more efficient. At 300 epochs, it achieves results close to those of the baseline with 400 epochs; with 400 epochs, it outperforms the baseline at 500 epochs. This is similar to previous observations in metric learning, where challenging training pairs are known to improve the both convergence speed and final embedding performance.

Transfer to other downstream datasets Transfer performance compares how encoders learned by different SSL approaches generalize to various downstream datasets. Following the linear evaluation protocol of [12], we consider the 8 datasets [29, 28, 38, 14, 49, 17, 46] shown in Table 2. Both the encoder of SimCLR [12] and CLAE are trained on ImageNet100 (an ImageNet subset sampled by [63]), using a ResNet18. On ImageNet100, CLAE achieved 62.4 \pm 0.02 classification accuracy, outperforming SimCLR (61.7 \pm 0.02). This indicates that it can scale to large datasets. On the remaining datasets of Table 2, it outperformed SimCLR on 7 out of the 8 datasets. This suggests that it generalizes better across downstream datasets. Since ImageNet100 does not contain any classes related to cars and airplanes, the performance on these 2 datasets is worse than on the others. In any case, CLAE beat [12] on several fine-grained datasets, such as Cars [28], Aircraft [38] and Flowers [46].

Attack methods While FGSM [19] is used in the above experiments, CLAE can be integrated with multiple attack approaches. To demonstrate this property, various attack methods (R-FGSM [65], F-FGSM [72], PGD [37]) were evaluated, with $\epsilon = 0.03$, on CIFAR100. As shown in Figure 7, R-FGSM and F-FGSM have performance comparable to FGSM, while PGD is slightly weaker. However, all these attack methods beat the baseline, indicating that the proposed framework learns a better representation.

5 Conclusion

In self-supervised learning (SSL), approaches based on contrastive learning (CL) do not necessarily optimize on hard negative pairs. In this work, we have proposed a new algorithm (CLAE) that generates more challenging positive and hard negative pairs, on-the-fly, by leveraging adversarial examples. Adversarial training with the proposed adversarial augmentations was demonstrated to improve performance of several CL baselines. We hope this work will inspire further research on the use of adversarial examples in SSL.

6 Broader Impact

This work advances the general use of deep learning technology, especially in the case that dataset annotations are difficult to obtain, and could have many applications. It advances several state of the art solutions on self-supervised learning (SSL), where no labels are provided. Moreover, while prior works in SSL suggest training with larger network, larger batch size and longer training epochs, the experiments in this work demonstrates that these factors are less critical by optimizing on effective training pairs. This can be beneficial in the scenario where time and gpu resource are limited. While this work mainly focuses on the study of image recognition, we hope this work can be extended to other application domains of SSL in the future.

Acknowledgement

This work was partially funded by NSF awards IIS-1637941, IIS-1924937, and NVIDIA GPU donations. We also acknowledge and thank the use of the Nautilus platform for some of the experiments discussed above.

References

- [1] Tiny imagenet visual recognition challenge. <https://tiny-imagenet.herokuapp.com/>.
- [2] P. Agrawal, J. Carreira, and J. Malik. Learning to see by moving. In *2015 IEEE International Conference on Computer Vision (ICCV)*, pages 37–45, Dec 2015.
- [3] Unaiza Ahsan, Rishi Madhok, and Irfan A. Essa. Video jigsaw: Unsupervised learning of spatiotemporal context for video action recognition. *CoRR*, abs/1808.07507, 2018.
- [4] Anurag Arnab, Ondrej Miksik, and Philip H. S. Torr. On the robustness of semantic segmentation models to adversarial attacks. In *CVPR*, 2018.
- [5] Sanjeev Arora, Hrishikesh Khandeparkar, Mikhail Khodak, Orestis Plevrakis, and Nikunj Saunshi. A theoretical analysis of contrastive unsupervised representation learning. *CoRR*, abs/1902.09229, 2019.
- [6] H. Bilen and A. Vedaldi. Universal representations: The missing link between faces, text, planktons, and cat breeds. Technical report, 2017.
- [7] Avishek Joey Bose, Huan Ling, and Yanshuai Cao. Adversarial contrastive estimation. *CoRR*, abs/1805.03642, 2018.
- [8] Avishek Joey Bose, Huan Ling, and Yanshuai Cao. Compositional hard negatives for visual semantic embeddings via an adversary. 2018.
- [9] Nicholas Carlini and David A. Wagner. Towards evaluating the robustness of neural networks. *CoRR*, abs/1608.04644, 2016.
- [10] Anirban Chakraborty, Manaar Alam, Vishal Dey, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. Adversarial attacks and defences: A survey. *CoRR*, abs/1810.00069, 2018.
- [11] Shang-Tse Chen, Cory Cornelius, Jason Martin, and Duen Horng Chau. Robust physical adversarial attack on faster R-CNN object detector. *CoRR*, abs/1804.05810, 2018.
- [12] Ting Chen, Simon Kornblith, Mohammad Norouzi, and Geoffrey Hinton. A simple framework for contrastive learning of visual representations. *arXiv preprint arXiv:2002.05709*, 2020.
- [13] S. Chopra, R. Hadsell, and Y. LeCun. Learning a similarity metric discriminatively, with application to face verification. In *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’05)*, volume 1, pages 539–546 vol. 1, 2005.
- [14] M. Cimpoi, S. Maji, I. Kokkinos, S. Mohamed, , and A. Vedaldi. Describing textures in the wild. In *Proceedings of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2014.
- [15] Carl Doersch, Abhinav Gupta, and Alexei A. Efros. Unsupervised visual representation learning by context prediction. *2015 IEEE International Conference on Computer Vision (ICCV)*, pages 1422–1430, 2015.
- [16] Kevin Eykholt, Ivan Evtimov, Earlene Fernandes, Bo Li, Amir Rahmati, Florian Tramèr, Atul Prakash, Tadayoshi Kohno, and Dawn Song. Physical adversarial examples for object detectors. *CoRR*, abs/1807.07769, 2018.
- [17] Li Fei-Fei, Rob Fergus, and Pietro Perona. Learning generative visual models from few training examples: An incremental bayesian approach tested on 101 object categories. *Computer Vision and Pattern Recognition Workshop*, 2004.
- [18] Spyros Gidaris, Praveer Singh, and Nikos Komodakis. Unsupervised representation learning by predicting image rotations. *CoRR*, abs/1803.07728, 2018.
- [19] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *CoRR*, abs/1412.6572, 2014.
- [20] Michael Gutmann and Aapo Hyvärinen. Noise-contrastive estimation: A new estimation principle for unnormalized statistical models. In Yee Whye Teh and Mike Titterton, editors, *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, volume 9 of *Proceedings of Machine Learning Research*, pages 297–304, Chia Laguna Resort, Sardinia, Italy, 13–15 May 2010. PMLR.
- [21] Tengda Han, Weidi Xie, and Andrew Zisserman. Video representation learning by dense predictive coding. In *Workshop on Large Scale Holistic Video Understanding, ICCV*, 2019.

- [22] Kaiming He, Haoqi Fan, Yuxin Wu, Saining Xie, and Ross Girshick. Momentum contrast for unsupervised visual representation learning. *arXiv preprint arXiv:1911.05722*, 2019.
- [23] Aapo Hyvärinen and Hiroshi Morioka. Unsupervised feature extraction by time-contrastive learning and nonlinear ica. In R. Garnett, D.D. Lee, U. von Luxburg, I. Guyon, and M. Sugiyama, editors, *Advances in Neural Information Processing Systems*, number NIPS 2016 in Advances in neural information processing systems, pages 3772–3780, United States, 2016. Neural Information Processing Systems Foundation.
- [24] Andrew Ilyas, Shibani Santurkar, Dimitris Tsipras, Logan Engstrom, Brandon Tran, and Aleksander Madry. Adversarial examples are not bugs, they are features. In *NeurIPS*, 2019.
- [25] Longlong Jing and Yingli Tian. Self-supervised visual feature learning with deep neural networks: A survey. *CoRR*, abs/1902.06162, 2019.
- [26] Prannay Khosla, Piotr Teterwak, Chen Wang, Aaron Sarna, Yonglong Tian, Phillip Isola, Aaron Maschinot, Ce Liu, and Dilip Krishnan. Supervised contrastive learning. *arXiv preprint arXiv:2004.11362*, 2020.
- [27] Dahun Kim, Donghyeon Cho, Donggeun Yoo, and In So Kweon. Learning image representations by completing damaged jigsaw puzzles. *CoRR*, abs/1802.01880, 2018.
- [28] Jonathan Krause, Michael Stark, Jia Deng, and Li Fei-Fei. 3d object representations for fine-grained categorization. In *4th International IEEE Workshop on 3D Representation and Recognition (3dRR-13)*, Sydney, Australia, 2013.
- [29] Alex Krizhevsky. Learning multiple layers of features from tiny images. 2009.
- [30] B. G. Vijay Kumar, Ben Harwood, Gustavo Carneiro, Ian D. Reid, and Tom Drummond. Smart mining for deep metric learning. *CoRR*, abs/1704.01285, 2017.
- [31] Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio. Adversarial examples in the physical world. *CoRR*, abs/1607.02533, 2016.
- [32] Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio. Adversarial machine learning at scale. *CoRR*, abs/1611.01236, 2016.
- [33] Gustav Larsson, Michael Maire, and Gregory Shakhnarovich. Learning representations for automatic colorization. *CoRR*, abs/1603.06668, 2016.
- [34] Hsin-Ying Lee, Jia-Bin Huang, Maneesh Singh, and Ming-Hsuan Yang. Unsupervised representation learning by sorting sequences. *CoRR*, abs/1708.01246, 2017.
- [35] Saehyung Lee, Hyun-Gyu Lee, and Sungroh Yoon. Adversarial vertex mixup: Toward better adversarially robust generalization. *ArXiv*, abs/2003.02484, 2020.
- [36] Hong Liu, Mingsheng Long, Jianmin Wang, and Michael Jordan. Transferable adversarial training: A general approach to adapting deep classifiers. In Kamalika Chaudhuri and Ruslan Salakhutdinov, editors, *Proceedings of the 36th International Conference on Machine Learning*, volume 97 of *Proceedings of Machine Learning Research*, pages 4013–4022, Long Beach, California, USA, 09–15 Jun 2019. PMLR.
- [37] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. In *International Conference on Learning Representations*, 2018.
- [38] S. Maji, J. Kannala, E. Rahtu, M. Blaschko, and A. Vedaldi. Fine-grained visual classification of aircraft. Technical report, 2013.
- [39] Ishan Misra and Laurens van der Maaten. Self-supervised learning of pretext-invariant representations. In *CVPR*, 2020.
- [40] Ishan Misra, C. Lawrence Zitnick, and Martial Hebert. Unsupervised learning using sequential verification for action recognition. *CoRR*, abs/1603.08561, 2016.
- [41] T. Miyato, S. Maeda, M. Koyama, and S. Ishii. Virtual adversarial training: A regularization method for supervised and semi-supervised learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41(8):1979–1993, 2019.
- [42] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. Universal adversarial perturbations. *CoRR*, abs/1610.08401, 2016.

- [43] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, and Pascal Frossard. Deepfool: a simple and accurate method to fool deep neural networks. *CoRR*, abs/1511.04599, 2015.
- [44] T. Nathan Mundhenk, Daniel Ho, and Barry Y. Chen. Improvements to context based self-supervised learning. *CoRR*, abs/1711.06379, 2017.
- [45] Muzammal Naseer, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, and Fatih Porikli. A self-supervised approach for adversarial robustness. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020.
- [46] M-E. Nilsback and A. Zisserman. Automated flower classification over a large number of classes. In *Proceedings of the Indian Conference on Computer Vision, Graphics and Image Processing*, Dec 2008.
- [47] Mehdi Noroozi and Paolo Favaro. Unsupervised learning of visual representations by solving jigsaw puzzles. *CoRR*, abs/1603.09246, 2016.
- [48] Nicolas Papernot, Patrick D. McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik, and Ananthram Swami. The limitations of deep learning in adversarial settings. *CoRR*, abs/1511.07528, 2015.
- [49] O. M. Parkhi, A. Vedaldi, A. Zisserman, and C. V. Jawahar. Cats and dogs. In *IEEE Conference on Computer Vision and Pattern Recognition*, 2012.
- [50] Omkar M. Parkhi, Andrea Vedaldi, and Andrew Zisserman. Deep face recognition. In Xianghua Xie, Mark W. Jones, and Gary K. L. Tam, editors, *Proceedings of the British Machine Vision Conference (BMVC)*, pages 41.1–41.12. BMVA Press, September 2015.
- [51] Deepak Pathak, Philipp Krähenbühl, Jeff Donahue, Trevor Darrell, and Alexei A. Efros. Context encoders: Feature learning by inpainting. *CoRR*, abs/1604.07379, 2016.
- [52] Ishan Misra Pedro Morgado, Nuno Vasconcelos. Audio-visual instance discrimination with cross-modal agreement. <https://arxiv.org/abs/2004.12943>, 2020.
- [53] S-A. Rebuffi, H. Bilen, and A. Vedaldi. Learning multiple visual domains with residual adapters. In *Neural Information Processing Systems (NeurIPS)*, 2017.
- [54] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. *CoRR*, abs/1503.03832, 2015.
- [55] Pierre Sermanet, Corey Lynch, Jasmine Hsu, and Sergey Levine. Time-contrastive networks: Self-supervised learning from multi-view observation. *CoRR*, abs/1704.06888, 2017.
- [56] Pierre Sermanet, Corey Lynch, Jasmine Hsu, and Sergey Levine. Time-contrastive networks: Self-supervised learning from multi-view observation. *CoRR*, abs/1704.06888, 2017.
- [57] Ali Shafahi, Mahyar Najibi, Amin Ghiasi, Zheng Xu, John P. Dickerson, Christoph Studer, Larry S. Davis, Gavin Taylor, and Tom Goldstein. Adversarial training for free! *CoRR*, abs/1904.12843, 2019.
- [58] E. Simo-Serra, E. Trulls, L. Ferraz, I. Kokkinos, P. Fua, and F. Moreno-Noguer. Discriminative learning of deep convolutional feature point descriptors. In *2015 IEEE International Conference on Computer Vision (ICCV)*, pages 118–126, 2015.
- [59] Kihyuk Sohn. Improved deep metric learning with multi-class n-pair loss objective. In D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, editors, *Advances in Neural Information Processing Systems* 29, pages 1857–1865. Curran Associates, Inc., 2016.
- [60] Hyun Oh Song, Yu Xiang, Stefanie Jegelka, and Silvio Savarese. Deep metric learning via lifted structured feature embedding. *CoRR*, abs/1511.06452, 2015.
- [61] Jiawei Su, Danilo Vasconcellos Vargas, and Kouichi Sakurai. One pixel attack for fooling deep neural networks. *CoRR*, abs/1710.08864, 2017.
- [62] Yumin Suh, Bohyung Han, Wonsik Kim, and Kyoung Mu Lee. Stochastic class-based hard example mining for deep metric learning. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2019.
- [63] Yonglong Tian, Dilip Krishnan, and Phillip Isola. Contrastive multiview coding. *arXiv preprint arXiv:1906.05849*, 2019.
- [64] Florian Tramèr and Dan Boneh. Adversarial training and robustness for multiple perturbations. *CoRR*, abs/1904.13000, 2019.

- [65] Florian Tramèr, Alexey Kurakin, Nicolas Papernot, Ian Goodfellow, Dan Boneh, and Patrick McDaniel. Ensemble adversarial training: Attacks and defenses. In *International Conference on Learning Representations*, 2018.
- [66] Michael Tschannen, Josip Djolonga, Paul K. Rubenstein, Sylvain Gelly, and Mario Lucic. On mutual information maximization for representation learning. *ArXiv*, abs/1907.13625, 2020.
- [67] Dimitris Tsipras, Shibani Santurkar, Logan Engstrom, Alexander Turner, and Aleksander Madry. Robustness may be at odds with accuracy. *arXiv: Machine Learning*, 2018.
- [68] Aäron van den Oord, Yazhe Li, and Oriol Vinyals. Representation learning with contrastive predictive coding. *CoRR*, abs/1807.03748, 2018.
- [69] Riccardo Volpi, Hongseok Namkoong, Ozan Sener, C. John Duchi, Vittorio Murino, and Silvio Savarese. Generalizing to unseen domains via adversarial data augmentation. *NeurIPS*, pages 5334–5344, 2018.
- [70] X. Wang and A. Gupta. Unsupervised learning of visual representations using videos. In *2015 IEEE International Conference on Computer Vision (ICCV)*, pages 2794–2802, 2015.
- [71] Kilian Q. Weinberger and Lawrence K. Saul. Distance metric learning for large margin nearest neighbor classification. *Journal of Machine Learning Research*, 10(9):207–244, 2009.
- [72] Eric Wong, Leslie Rice, and J. Zico Kolter. Fast is better than free: Revisiting adversarial training. In *International Conference on Learning Representations*, 2020.
- [73] Chao-Yuan Wu, R. Manmatha, Alexander J. Smola, and Philipp Krähenbühl. Sampling matters in deep embedding learning. *CoRR*, abs/1706.07567, 2017.
- [74] Zhirong Wu, Yuanjun Xiong, Stella Yu, and Dahua Lin. Unsupervised feature learning via non-parametric instance-level discrimination. *CoRR*, abs/1805.01978, 2018.
- [75] Cihang Xie, Mingxing Tan, Boqing Gong, Jiang Wang, Alan L. Yuille, and Quoc V. Le. Adversarial examples improve image recognition. *ArXiv*, abs/1911.09665, 2019.
- [76] Cihang Xie, Jianyu Wang, Zhishuai Zhang, Yuyin Zhou, Lingxi Xie, and Alan L. Yuille. Adversarial examples for semantic segmentation and object detection. *CoRR*, abs/1703.08603, 2017.
- [77] Cihang Xie and Alan L. Yuille. Intriguing properties of adversarial training. *CoRR*, abs/1906.03787, 2019.
- [78] Mang Ye, Xu Zhang, Pong C. Yuen, and Shih-Fu Chang. Unsupervised embedding learning via invariant and spreading instance feature. *CoRR*, abs/1904.03436, 2019.
- [79] Xiaoyong Yuan, Pan He, Qile Zhu, Rajendra Rana Bhat, and Xiaolin Li. Adversarial examples: Attacks and defenses for deep learning. *CoRR*, abs/1712.07107, 2017.
- [80] Hongyang Zhang, Yaodong Yu, Jiantao Jiao, Eric P. Xing, Laurent El Ghaoui, and Michael I. Jordan. Theoretically principled trade-off between robustness and accuracy. *CoRR*, abs/1901.08573, 2019.
- [81] Richard Zhang, Phillip Isola, and Alexei A. Efros. Colorful image colorization. *CoRR*, abs/1603.08511, 2016.
- [82] Yue Zhao, Hong Zhu, Qintao Shen, Ruigang Liang, Kai Chen, and Shengzhi Zhang. Practical adversarial attack against object detector. *CoRR*, abs/1812.10217, 2018.