Augmenting Image Classifiers using Data Augmentation Generative Adversarial Networks

Antreas Antoniou\textsuperscript{1}, Amos Storkey\textsuperscript{1}, and Harrison Edwards\textsuperscript{1,2}

\textsuperscript{1} University of Edinburgh, Edinburgh, UK
{a.antoniou,a.storkey,h.l.edwards}@sms.ed.ac.uk
https://www.ed.ac.uk/
\textsuperscript{2} Open AI
https://openai.com/

Abstract. Effective training of neural networks requires much data. In the low-data regime, parameters are underdetermined, and learnt networks generalise poorly. Data Augmentation alleviates this by using existing data more effectively, but standard data augmentation produces only limited plausible alternative data. Given the potential to generate a much broader set of augmentations, we design and train a generative model to do data augmentation. The model, based on image conditional Generative Adversarial Networks, uses data from a source domain and learns to take a data item and augment it by generating other within-class data items. As this generative process does not depend on the classes themselves, it can be applied to novel unseen classes. We demonstrate that a Data Augmentation Generative Adversarial Network (DA-GAN) augments classifiers well on Omniglot, EMNIST and VGG-Face.

1 Introduction

Over the last decade Deep Neural Networks have enabled unprecedented performance on a number of tasks. They have been demonstrated in many domains \cite{12} including image classification \cite{25, 17, 16, 18, 21}, machine translation \cite{44}, natural language processing \cite{12}, speech recognition \cite{19}, and synthesis \cite{42}, learning from human play \cite{6} and reinforcement learning \cite{27, 35, 10, 40, 13} among others. In all cases, very large datasets have been utilized, or in the case of reinforcement learning, extensive play. In many realistic settings we need to achieve goals with limited datasets; in those cases deep neural networks seem to fall short, overfitting on the training set and producing poor generalisation on the test set.

Techniques have been developed over the years to help combat overfitting such as L1/L2 regularization \cite{28}, dropout \cite{20}, batch normalization \cite{23}, batch renormalisation \cite{22} or layer normalization \cite{2}. However in low data regimes, even these techniques fall short, since the the flexibility of the network is so high. These methods are not able to capitalise on known input invariances that might form good prior knowledge for informing the parameter learning.

It is also possible to generate more data from existing data by applying various transformations \cite{25} to the original dataset. These transformations include
random translations, rotations and flips as well as addition of Gaussian noise. Such methods capitalize on transformations that we know should not affect the class. This technique seems to be vital, not only for the low-data cases but for any size of dataset, in fact even models trained on some of the largest datasets such as Imagenet [7] can benefit from this practice.

Typical data augmentation techniques use a limited set of known invariances that are easy to invoke. Here, we recognize that we can learn a model of a much larger invariance space through training a form of conditional generative adversarial network (GAN) in some \textit{source domain}. This can then be applied in the low-data domain of interest, the \textit{target domain}. We show that such a Data Augmentation Generative Adversarial Network (DAGAN) enables effective neural network training even in low-data target domains. As the DAGAN does not depend on the classes themselves it captures the cross-class transformations, moving data-points to other points of equivalent class.

In this paper we train a DAGAN and then evaluate its performance on low-data tasks using standard stochastic gradient descent neural network training. We use 3 datasets, the Omniglot dataset, the EMNIST dataset and the more complex VGG-Face dataset. The DAGAN trained on Omniglot was used for augmenting both the Omniglot and EMNIST classifiers to demonstrate benefit even when transferring between substantially different domains. The VGG-Face dataset provides a considerably more challenging test for the DAGAN, VGG-Face was used to evaluate whether the DAGAN training scheme could work on human faces, which are notoriously hard to model using a generator. Furthermore the usefulness of the generated faces was measured when used as augmentation data in the classification training.

2 Background

**Transfer Learning and Dataset Shift:** The term \textit{dataset shift} [36] generalises the concept of covariate shift [33, 37, 38] to multiple cases of changes between domains. For data augmentation, we may learn a generative distribution that maintains class consistency on one set of classes and apply that consistency transformation to new unseen classes, on the understanding the the transformations that maintain consistency generalise across classes.

**Generative Adversarial Networks:** GANs [11], and specifically Deep Convolutional GANs (DCGAN) [29] use the ability to discriminate between true and generated examples as a learning objective for generative models. GAN approaches can learn complex joint densities. Recent improvements in the optimization process [1, 14, 3] have reduced some of the failure modes of the GAN learning process as well as produced objectives that correlate well with sample quality [1, 14]. Furthermore image conditional GANs have been used to achieve image to image translation [24], as well as augment datasets [5, 45, 34]. However the work relating to the enhancement of datasets only uses the GAN to either fine tune simulated data or generate data by attempting to reconstruct
existing data points. Whereas our model is explicitly trained to produce data augmentations as a manifold of samples around real data samples.

As demonstrated in [14], the Wasserstein formulation for training GANs has shown superior sample diversity and quality in multiple instances. Additionally the Wasserstein GANs (WGAN) with Gradient Penalty (GP) have the additional benefit of being trainable using advanced architectures such as ResNets [16]. This is especially important since most GAN formulations can only be successfully trained using very specific and often less expressive model architectures. Furthermore WGAN with GP discriminator losses have been empirically observed to correlate with sample quality. Taking into consideration available state of the art methods including standard GAN, LS-GAN, WGAN with clipping and WGAN with Spectral normalization, we focus on the use WGAN with GP training in this paper due to its versatility in terms of architectures and its superior qualitative performance. Our own experiments with other approaches confirm the stated benefits; we found WGAN with GP to produce the most stable models with the best sample quality both qualitatively and quantitatively.

Data Augmentation: Data augmentation similar to [25] is routinely used in classification problems. Often it is non-trivial to encode known invariances in a model. It can be easier to encode those invariances in the data instead by generating additional data items through transformations from existing data items. For example the labels of handwritten characters should be invariant to small shifts in location, small rotations or shears, changes in intensity, changes in stroke thickness, changes in size etc. Almost all cases of data augmentation are from a priori known invariance. Various attempts at augmenting features instead of data are investigated in [39, 8]. Moreover, the effectiveness of data augmentation has also been shown in other domains except images. Two such domains is sound [32] and text [31]. There has been little previous work that attempts to learn data augmentation strategies. One paper that is worthy of note is the work of [15], where the authors learn augmentation strategies on a class by class basis. Additional papers that attempt to learn models for data augmentation include [9, 4, 30]. These approaches do not transfer to the setting where completely new classes are considered.

3 Model

If we know that a class label should be invariant to a particular transformation then we can apply that transformation to generate additional data. If we do not know what transformations might be valid, but we have other data from related problems, we can attempt to learn valid transformations from those related problems that we can apply to our setting. This is an example of meta-learning; we learn on other problems how to improve learning for our target problem.

3.1 Model Overview

Consider a collection of datasets \( \{(x_i^c | i = 1, 2, \ldots, N_c) | c \in C \} \), with each dataset labelled by \( c \), the class, taken from the set of classes \( C \), and with each element
in a dataset \( c \) indexed by \( i \) and denoted by \( x_i^c \). Let \( x_i^c \in X \), the space of inputs. In this paper \( X \) will be a space of input images.

The goal is to learn a mapping between a conditional sample \( x_i^c \) of a certain class \( c \) to other samples \( x_j^c \) from that same class, using training data \( \{(x_i^c|i = 1,2,\ldots,N^c)|c \in C\} \). To do so we learn a differentiable function \( G \) which we call a generator. Given some random standard Gaussian vector \( z \), we require a mapping \( G : (x_i^c, z) \) such that, \( \forall j \), \( x_j^c \) has high probability under the density of \( z \) mapped through \( G \). Since \( G \) is differentiable, \( z \) maps out a whole manifold in \( X \) space associated with input \( x_i^c \) in a class consistent way. Yet \( G \) does not have access to the class \( c \) itself, thus enabling the DAGAN to generalize to unseen classes. We parameterize our generator function \( \hat{x} = G(x_i^c, z) \) as a neural network and we train it as a GAN using the WGAN with GP formulation. Training a GAN also requires a discriminator network, denoted as \( D \), to be trained along with the generator network. The discriminator network attempts to discriminate between real and fake samples whilst the generator attempts to minimize the discriminator’s performance in guessing real from fake.

3.2 Model Objective Definition

We modify the WGAN with GP formulation to account for the fact that we are using an image-conditional GAN with a discriminator that takes as input 2 images, instead of 1. Figure 1 shows the high level overview of our training setup. Our generator and discriminator objectives can be expressed as:

\[
L_{\text{discr}} = \mathbb{E}_{\tilde{x} \sim P_g}[D(x_i^c, \tilde{x})] - \mathbb{E}_{x \sim P_r}[D(x_i^c, x_j^c)] + \lambda \mathbb{E}_{\tilde{x} \sim P_e}(||\nabla_{\tilde{x}}D(x_i^c, \tilde{x})||_2 - 1) \tag{1}
\]

\[
L_{\text{gen}} = -\mathbb{E}_{\tilde{x} \sim P_g}[D(x_i^c, \tilde{x})] \tag{2}
\]

where \( x \) represents real samples, \( x_i^c \) and \( x_j^c \) represent two separate instances of samples from class \( c \), \( \tilde{x} \) represents generated samples from the generator \( G \). \( \hat{x} \) is, as defined in [14], randomly sampled points on linear interpolations between the samples of the real distribution \( P_r \) and generated distribution \( P_g \). The only difference from the original WGAN with GP formulation is the use of 2 entries in the discriminator arguments, one for the conditional sample \( x_i^c \) and one for the target sample \( x_j^c \) (for real case) or \( \hat{x} \) (for fake case).

3.3 Architectures

We chose to use a state of the art DenseNet discriminator and, for the generator, a powerful combination of two standard networks, UNet and ResNet, which we henceforth call a UResNet. The code for this paper is available\(^3\), and that provides the full implementation of the networks. However we describe the implementational details here.

\(^3\) https://github.com/AntreasAntoniou/DAGAN
Augmenting Image Classifiers using DAGAN

**Fig. 1.** DAGAN Architecture. Left: the generator network is composed of an encoder taking an input image and projecting it to a lower dimensional manifold. A random vector \( z \) is transformed and concatenated with the bottleneck vector; these are both passed to the decoder network which generates a within-class image. Right: the adversarial discriminator network is trained to discriminate between the samples from the real distribution (two real images from the same class) and the fake distribution (a real sample and a generated sample). Adversarial training enables the network to generate within-class images that look different enough to be considered a different sample.

The UResNet generator has a total of 8 blocks, each block having 4 convolutional layers (with leaky rectified linear (ReLU) activations and batch renormalisation (batchrenorm) [22]) followed by one downsampling or upsampling layer. Downsampling layers (in blocks 1-4) were convolutions with stride 2 followed by leaky ReLU, batch normalisation and dropout. Upscaling layers were implemented by employing a nearest neighbour upscale, followed by a convolution, leaky ReLU, batch renormalisation and dropout. For Omniglot and EMNIST experiments, all layers had 64 filters. For the VGG-Face experiments the first 2 blocks of the encoder and the last 2 blocks of the decoder had 64 filters and the last 2 blocks of the encoder and the first 2 blocks of the decoder 128 filters.

In addition each block of the UResNet generator had skip connections. As with a standard ResNet, we used either a summation skip connection between layers with equivalent spacial dimensions or a strided 1x1 convolution for between layers with different spacial dimensions, thus bypassing the between block non-linearity to help gradient flow. Finally skip connections were introduced between equivalent sized filters at each end of the network (as with UNet).

We used a DenseNet [21] discriminator, using layer normalization instead of batch normalization; the latter would break the assumptions of the WGAN objective function (as mentioned in [[14] chapter 4). The DenseNet was composed of 4 Dense Blocks and 4 Transition Layers, as defined in [21]. We used a growth rate of \( k = 64 \) and each Dense Block had 5 convolutional layers. We removed
the 1x1 convolutions usually before the 3x3 convolutions as we observed this improved sample quality. For the discriminator we used dropout at the last convolutional layer of each Dense Block; this too improved sample quality.

For each classification experiment we used a DenseNet classifier composed of 4 Dense Blocks and 4 Transition Layers with a \( k = 64 \), each Dense Block had 3 convolutional layers within it. The classifiers were a total of 17 layers (i.e. 16 layers and 1 softmax layer). Furthermore we applied a dropout of 0.5 on the last convolutional layer in each Dense Block.

4 Datasets and Experiments

We tested the DAGAN augmentation on 3 datasets: Omniglot, EMNIST, and VGG-Face. All datasets were split randomly into source domain sets, validation domain sets and test domain sets.

For classifier networks, data for each character (handwritten or person) was further split into 2 test cases (for all datasets), 3 validation cases and a varying number of training cases depending on the experiment. Classifier training was done on the training cases for all examples in all domains; hyperparameter choice used validation cases. Test performance was reported only on the test cases for the target domain set. Case splits were randomized across each test run.

The Omniglot data [26] was split into source domain and target domain similarly to the split in [41]. The class ids were sorted in an increasing manner. The first 1200 were used as a source domain set, 1201-1412 as a validation domain set and 1412-1623 as a target domain test set.

The EMNIST data was split into a source domain that included classes 0-34 (after random shuffling of the classes), the validation domain set included classes 35-42 and the test domain set included classes 42-47. Since the EMNIST dataset has thousands of samples per class we chose only a subset of 100 for each class, so that we could make our task a low-data one.

In the VGG-Face dataset case, we randomly chose 100 samples from each class that had 100 or more, uncorrupted images, resulting in 2396 of the full 2622 classes available in the dataset. After shuffling, we split the resulting dataset into a source domain that included the first 1802 classes. The test domain set included classes 1803-2300 and the validation domain set included classes 2300-2396.

4.1 Training of DAGAN in source domain

A DAGAN was trained on Source Omniglot domains using a variety of architectures: standard VGG, U-Net, and ResNet inspired architectures. Increasingly powerful networks proved better generators, with the UResNet described in Section 3.3 generator being our model of choice. Examples of generated data are given in Figure 2. We trained each DAGAN for 200K iterations, using a learning rate of 0.0001, and an Adam optimizer with Adam parameters of \( \beta_1 = 0 \) and \( \beta_2 = 0.9 \). We used a pretrained DenseNet classifier to quantify the performance of the generated data in terms of how well they classify in real classes. We chose the model that had the best validation accuracy performance on this classifier.
4.2 Classifiers

The primary question of this paper is how well the DAGAN can augment vanilla classifiers trained on each target domain. A DenseNet classifier (as described in Section 3.3) was trained first on just real data (with standard data augmentation) with 5 to 100 examples per class (depending on dataset). In the second case, the classifier was also trained on DAGAN generated data. The real or fake label was also passed to the network, via adding 1 filter before each convolution of either zeros (fake) or ones (real) to enable the network to learn how best to emphasise true over generated data. This last step proved crucial to maximising the potential of the DAGAN augmentations. In each training cycle, varying numbers of augmented samples were provided for each real example (ranging from 1-10). The best hyperparameters were selected via performance on the validation domain. The classifier was trained with standard augmentation: random Gaussian noise was added to images (with 50% probability), random shifts along x and y axis (with 50% probability), and random 90 degree rotations (all with equal probability of being chosen). Classifiers were trained for 200 epochs, with a learning rate of 0.001, and an Adam optimizer with $\beta_1 = 0.9$ and $\beta_2 = 0.99$. The results on the held out test cases from the target domain is given in Table 1. In every case the augmentation improves the classification.

5 Conclusions

Data augmentation is a widely applicable approach to improving performance in low-data settings. The DAGAN is a flexible model to automatically learn to augment data. We demonstrate that a DAGAN can improve performance of classifiers even after standard data-augmentation. Furthermore, it is worth
Augmenting Image Classifiers using DAGAN

<table>
<thead>
<tr>
<th>Samples Per Class</th>
<th>Augment with DAGAN</th>
<th>Omniglot</th>
<th>EMNIST</th>
<th>VGG-Face</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>False</td>
<td>68.99%</td>
<td>-</td>
<td>04.47%</td>
</tr>
<tr>
<td>5</td>
<td>True</td>
<td>82.13%</td>
<td>-</td>
<td>12.59%</td>
</tr>
<tr>
<td>10</td>
<td>False</td>
<td>79.41%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>True</td>
<td>86.22%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td>False</td>
<td>81.97%</td>
<td>73.93%</td>
<td>39.33%</td>
</tr>
<tr>
<td>15</td>
<td>True</td>
<td>87.42%</td>
<td>76.07%</td>
<td>42.93%</td>
</tr>
<tr>
<td>25</td>
<td>False</td>
<td>-</td>
<td>78.35%</td>
<td>57.99%</td>
</tr>
<tr>
<td>25</td>
<td>True</td>
<td>-</td>
<td>80.26%</td>
<td>58.46%</td>
</tr>
<tr>
<td>50</td>
<td>False</td>
<td>-</td>
<td>81.51%</td>
<td>-</td>
</tr>
<tr>
<td>50</td>
<td>True</td>
<td>-</td>
<td>82.78%</td>
<td>-</td>
</tr>
<tr>
<td>100</td>
<td>False</td>
<td>-</td>
<td>83.78%</td>
<td>-</td>
</tr>
<tr>
<td>100</td>
<td>True</td>
<td>-</td>
<td>84.80%</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1. Classification Results: All results are averages over 5 independent runs. The DAGAN augmentation improves the classifier performance in all cases. Test accuracy is the result on the test cases in the test domain. Here for the purposes of compactness we omit the number of generated samples per real sample hyperparameter since that would produce more than 100 rows of data. We should note however that the optimal number of generated samples per real image was found to be 3.

noting that a DAGAN can be easily combined with other model types, including few shot learning models. Further work is needed to evaluate the usefulness in the few shot learning. However the flexibility of the DAGAN makes it a powerful means of enhancing models working with a small amount of data.

Acknowledgements This work was supported in by the EPSRC Centre for Doctoral Training in Data Science, funded by the UK Engineering and Physical Sciences Research Council and the University of Edinburgh as well as by the European Unions Horizon 2020 research and innovation programme under grant agreement No 732204 (Bouseyes) and by the Swiss State Secretariat for Education Research and Innovation (SERI) under contract number 16.0159. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

References

43. White, T.: Sampling Generative Networks (September 2016)