ROBUST DOMAIN-FREE DOMAIN GENERALIZATION
WITH CLASS-AWARE ALIGNMENT

Wenyu Zhang†  Mohamed Ragab †*  Ramon Sagarna†
† Institute for Infocomm Research, Singapore
* Nanyang Technological University, Singapore

ABSTRACT
While deep neural networks demonstrate state-of-the-art performance on a variety of learning tasks, their performance relies on the assumption that train and test distributions are the same, which may not hold in real-world applications. Domain generalization addresses this issue by employing multiple source domains to build robust models that can generalize to unseen target domains subject to shifts in data distribution. In this paper, we propose Domain-Free Domain Generalization (DFDG), a model-agnostic method to achieve better generalization performance on the unseen test domain without the need for source domain labels. DFDG uses novel strategies to learn domain-invariant class-discriminative features. It aligns class relationships of samples through class-conditional soft labels, and uses saliency maps, traditionally developed for post-hoc analysis of image classification networks, to remove superficial observations from training inputs. DFDG obtains competitive performance on both time series sensor and image classification public datasets.

Index Terms— Domain generalization; data distribution shift, model robustness

1. INTRODUCTION
While deep neural networks have widely acclaimed classification performance in diverse fields, their performance is often reliant on the assumption that all the train and test examples are sampled from the same distribution. In practical applications, though, changes in the data generation regimes are common during operation, effectively causing a shift in the data distribution that can significantly deteriorate model performance [1][2][3]. This not only compromises the accuracy of the existing deep model, but also the applicability if there are no available samples from the new distribution. In response to such issues, domain adaptation algorithms [4] aim at learning a model aligning the source distribution(s) and the new target distribution through a common feature representation space. For training, these methods require a sufficient amount of source samples and target inputs, and in some cases additional target labels. In the more extreme field of domain generalization [5][6][7][8], no target samples are available at train time. The goal is to learn a robust model that can directly generalize when unseen new data distributions arise. This allows to address many realistic scenarios in which the model needs to be deployed in the wild and new data cannot be collected for constant retraining. For example, in object recognition, new images of the same object with different background types may be encountered [6][9]; in fault diagnosis from sensing devices, new operating conditions may display unseen signals [10]; or, in speech recognition, an arbitrary number of unknown speakers may emerge [3].

A core aim of domain generalization is to find a common representation space of the multiple source domains such that the class-discriminative information is captured and the domain-specific statistics are ignored [8][7][11][12]. A popular approach is to minimize the discrepancy among the marginal distributions of input features [13] or the class-conditional distributions [14]. One important limitation is the need for domain labels to identify the groupings of samples for alignment [9]. Typically in domain adaptation and generalization literature, dataset labels are used as domain labels. This restrains the applicability of the methods since domain labels may be unavailable in practice, and dataset labels cannot replace domain labels in cases where samples of a dataset are drawn from a mixture of domains, take for example photos taken with different devices on social media websites if device type is the domain.

Aiming at a widely applicable domain generalization problem, in this work we propose a Domain-Free Domain Generalization (DFDG) method that learns domain-invariant class-discriminative features without the need for domain labels. As illustrated in Figure 1, we propose novel strategies for:

- Model regularization to learn domain-invariant features without domain labels by aligning soft labels conditioned on the classes to the class centroid;
- Automatic augmentation of inputs to remove superficial, less class-discriminative observations through saliency maps.

DFDG is model-agnostic and does not require expert knowledge for feature engineering, which renders it suitable for learning tasks in general. In our experiments, we consider both time series sensor and image classification benchmarks, and demonstrate that DFDG of-

![Fig. 1: Overview: DFDG learns domain-invariant class-discriminative features without the use of domain labels by (a) aligning class relationships of samples in the same class to the class centroid, and (b) masking superficial observations (e.g. domain-specific backgrounds) from training inputs guided by saliency maps.](image-url)
fers competitive performance compared to state-of-the-art methods. Although saliency maps are developed and conventionally used for image-based applications [15], our results show empirically that the technique can also be applied on time series sensor data.

2. RELATED WORKS

2.1. Combining source models

With multiple source domains, some works predict for new domains by training a model for each source and combining the respective predictions [11, 16, 17]. Similarly, some meta-learning frameworks select models for unseen target datasets by exhaustively training all candidate models on each source dataset, and select the final model by matching features and statistics between source and target datasets [18, 19]. These methods require storing a model for each source domain. In DFDG, only a single model is trained and stored.

2.2. Learning domain-invariant features

Many previous works for domain generalization focus on the goal of learning domain-invariant features which are class discriminative. This can be achieved through auxiliary losses with known domain labels. Besides the classification loss, the objective function also includes a domain alignment loss to reduce the distance between samples from different domains [8]. This has been implemented through meta-learning [7, 14, 20], or directly minimizing the distance between feature representations of different domains [5, 13]. Some works have an additional separation loss to maximize the distance between samples from different classes to encourage local clustering [5, 14]. In the case where domain labels are unknown, [9] shows that samples can be clustered into latent domains and then aligned. Knowledge of accurate domain labels cannot always be assumed in real-world applications, hence we work in the most general setting where domain labels are unavailable.

2.3. Learning robust features

Learning features that aim to improve model performance in general by being robust to sample variations at training are found to improve generalization performance in new domains. Popular approaches to learn robust features is to perturb the network [12] or representations during training. Domain-specific representations are removed either from the latent feature space [21] or from the observed input space [22], but these techniques are specific to image inputs. [6] zeros out penultimate-layer feature representations associated with the highest gradient in the final classification layer so that the network learns other features for classification. [23] regularizes the network through an auxiliary self-supervised task to learn spatial correlations within an image.

Other works propose to extrapolate to unseen target distributions by generating adversarial samples [24] or by enforcing equality in training risks across domains [25]. The latter implies that the worst-performing domain may be improved at the cost of other domains.

3. PROBLEM SETUP

We describe the problem setup and notations used in this paper. We denote the set of $K$ source domains as $D_S = \{D_1, \ldots, D_K\}$ and the unseen target domain as $D_t$. For each domain $D_i$ samples are drawn from a fixed distribution $\left( X^{(D)}, Y^{(D)} \right) \sim P^{(D)}$ where $X$ and $Y$ are the predictor and response variables. We denote the observed samples as $\left( x_i^{(D)}, y_i^{(D)} \right)_{i=1}^{N_D}$ for a sample size of $N_D$. We focus on classification tasks in this paper, so $y_i$ is a one-hot vector of the true class label in $C$ classes. No sample from the target domain $D_t$ is available at the training and validation stages of model learning. In the domain-free setting, we further assume that domain labels are unavailable, which is a realistic assumption for data collection. The aim is to train a model $f$ parameterized by $\theta$ to achieve good classification performance on the target domain $D_t$.

A common strategy for classification is to estimate the class probabilities for an input $x_i$. Let $p_i$ be the soft labels or vector of class probabilities for input $x_i$ as learned by the model $f$, that is, $p_i = \text{softmax}(f(x_i; \theta))$ where $\text{softmax}(\alpha)[c] = \frac{\exp(\alpha_c)}{\sum_{j=1}^{C} \exp(\alpha_j)}$ with $\alpha_c$ denoting the element of vector $\alpha$ corresponding to class $c$. The predicted class is the class with the highest probability in $p_i$.

4. PROPOSED METHOD: DFDG

A key concept in domain generalization is to learn representations which are domain-invariant but class-discriminative. To train the model for classification, we use the cross-entropy loss as the base objective for each batch of samples with indices $B$:

$$\ell_{ce} = -\frac{1}{|B|} \sum_{i \in B} y_i^T \log(p_i).$$

where $y_i$ is the one-hot vector of the true label and $p_i$ is the soft label estimated for sample $i$. Additionally, DFDG learns soft labels $p_i$’s such that they are aligned across source domains. We combine this with input augmentation so that model training focuses on class-discriminative inputs.

4.1. Regularizing for class relationship alignment

Constraining the model by aligning features from different domains tends to learn features that are more robust and applicable across domains, and less domain-specific. Being overly reliant on domain-specific features risks overfitting to the source domains and hence poor performance on out-of-distribution samples where these features are absent. Instead of aligning intermediate features, DFDG aligns the estimated soft labels which are lower dimensional and reflects relationships between class concepts. Alignments in the label space have been applied in domain adaption and domain generalization problems where domain labels are known [14, 26, 27]. Without domain labels, we propose an alignment loss:

$$\ell_{align} = \sum_{c=1}^{C} \frac{1}{|B(c)|} \sum_{i \in B(c)} \| p_i - \mu(c) \|^2_2$$

$$\mu(c) = \frac{1}{|B(c)|} \sum_{i \in B(c)} p_i$$

where for each class $c$, $B(c) = \{ i \in B, y_i = c \}$ are indices of samples, $\mu(c)$ is the cluster center for the corresponding class, and $p_i$ is the vector of soft labels for sample $i$. The regularization encourages samples from the same class to have similar class relationships regardless of their domains. The complete objective function with this alignment regularization is

$$L = \ell_{ce} + \alpha \ell_{align}$$

with hyperparameter $\alpha$ balancing the effects from the two parts.
4.2. Masking superficial observations

The presence of superficial or domain-specific observations in the input space can lead to overfitting to training data if the model learns to rely on these observations for the classification task. We use the term ‘observation’ here to denote a pixel in an image and a reading at one time step for a time series as examples. In images, these superficial observations can be pixels for backgrounds or styles. We propose augmenting m% of the samples in each batch at training to mask superficial observations by perturbing the observations least relevant to the desired classification task. We perturb by randomly shuffling the least relevant observations, hence preserving the overall statistics of the input. The intuition is that the trained model will be more robust to variations in these superficial observations in the target domain.

While a binary map that exactly pinpoints the location of class-discriminative features in the input is the most desirable and has been found to improve classification performance [28], such accurate maps require human-in-the-loop processing and cannot be readily available for most datasets. Our strategy also differs from feature muting [29] that sets a fixed number of features to zero, which can drastically change sample statistics and risk muting useful features through the fixed threshold. In DFDG, we use SmoothGrad saliency maps [15] to rank the relevance of each observation. Saliency maps are developed to explain decisions made by neural network models for image classification by assigning a saliency score to each pixel [15,30]. A ‘vanilla’ gradient-based saliency map \( g(x,c) \) of an input image \( x \) for class \( c \) is obtained by differentiating the class logit of model \( f \) with respect to \( x \) and taking the square element-wise:

\[
g(x,c) = \left( \frac{\partial f(x, \theta)[c]}{\partial x} \right)^2
\]  

(5)

where each saliency score reflects the amount of influence that a small change in a pixel has on the class logit. SmoothGrad denotes the saliency map by averaging \( n \) replicates of \( g(x,c) \) where Gaussian noise \( N(0, \sigma^2) \) is added to \( x \) in each replicate, and we denote the resulting SmoothGrad saliency map as \( sg(x,c) \). We fix \( n = 25 \) and \( \sigma = 0.15 \), the default in [31], throughout our experiments. We apply the technique on time series as well as image data.

We rank how class-discriminative an observation is by its saliency score. Observations below a threshold is masked and shuffled. The threshold is the \( q \)th percentile of the saliency scores of a image, uniformly sampled from \([0,q_{Max}]\) where \( q_{Max} \) is the maximum threshold percentile. In this sampling scheme, less relevant observations will be masked more often and the model will be less reliant on them. Figure 1 shows examples of saliency maps and masked input images for \( q = 70 \).

5. EXPERIMENTS

We evaluate DFDG on 3 public datasets: Bearings fault classification from vibration sensor signals, HHAR heterogeneous human activity recognition from motion sensor signals and PACS image classification. We report classification accuracy by treating each domain in turn as the unseen target domain and the rest as source domains. Details of the datasets and implementation configurations can be found in Section 5.1. For all datasets, we compare with TrainAll which is a vanilla training of source samples, RSC [6] which is a robustness method using feature muting that has achieved state-of-the-art performance for image classification including PACS, and MMLD [9] which clusters samples into latent domains using convolutional feature statistics and aligns the domains with a discriminator network.

5.1. Datasets and implementation

**Bearings Dataset**: The Case Western Reserve University (CWRU) Bearings dataset is widely used for rolling element bearings diagnostics in rotating machines [32]. Vibration signals are collected with 12kHz sampling rate under 8 different working conditions or domains [33]. The operating conditions comprise 4 loading torques and two different locations (drive end, fan end). The system has three major types of faults, namely inner-race fault (IF), outer-race fault (OF), and ball fault (BF), and each fault type occurs with three different dimensions 0.007, 0.014, 0.021 inches. Overall, we have 10 classes with 9 faulty classes and 1 healthy class. We extracted samples of length 4096 by applying a sliding window with shift size 290 [33]. We use a 6-layer convolutional neural network (CNN) as feature extractor and a 3-layer fully-connected network as classifier.

**HHAR**: The HHAR dataset consists of sensor readings to classify six activities, namely Biking, Standing, Sitting, Walking, Stair down, and Stair up. Gyroscope and accelerometer motion sensors in 8 smartphones and 4 smartwatches are used for monitoring. Nine different users execute these activities without predefined order while carrying the devices. We treat each user as a domain and, following a recent work on domain adaption [34], we focus on data from 8 smartphones with accelerometer sensors, pre-processed as in that work. We use a 3-layer CNN as feature extractor and a 1-layer fully-connected network for classification [33].

**PACS**: PACS is an image classification dataset containing images from 4 styles or domains, namely Photo, Art painting, Cartoon and Sketch. Each domain has a total of 7 classes: dog, elephant, giraffe, guitar, horse, house and person. Following [6,9,23], we use a ResNet18 network architecture and apply the same image augmentations to the samples, namely random cropping to 80-100% size, horizontal flipping, color jittering and conversion to grayscale.

We fix DFDG hyperparameters \( \alpha = 0.1 \), \( m = 50 \) and \( q_{Max} = 70 \), with further ablation studies in Section 5.3. During training, the alignment regularization and input masking strategies are randomly alternated across batches of size 128. The time series sensor datasets are trained for 2000 iterations, and PACS is trained for 3000 iterations. The learning rate is 0.001, and decayed by factor 0.1 after 80% iterations. To prevent classes from being unrepresented in batches, minority classes are upsampled uniformly at random, keeping a minority-to-majority class ratio of at least 0.5 in each batch. All the results are averaged over runs from 3 different seeds. RSC [6] and MMLD [9] were running their open-source implementations on the same seeds.

5.2. Generalization performance

Table 1 shows the classification performance on unseen target domains for the Bearings dataset. Since time series may be less distinguishable across domains than images, clustering with convolutional feature statistics as originated from image stylization [9] may have resulted in incorrect latent domains and hence negative transfer in MMLD. Our proposed DFDG improves average classification
accuracy by 2.83% over the baseline TrainAll. Combining DFDG with RSC, by randomly alternating between the two strategies across batches at training, attains the best accuracy of 84.65%. This shows that DFDG can complement other domain generalization methods. Figure 2 plots the 2-dimensional t-SNE representations of DFDG features. From Figure 2a, samples from the same class tend to cluster together. For exceptions such as the class “BF: 0.021” where there are two clusters, observe from the corresponding Figure 2b that one cluster correspond to domains (A, B, C, D) with drive-end bearings location, and the other correspond to domains (E, F, G, H) with fan-end bearings location. Samples from the same location are clustered closer together due to greater inter-domain similarity.

Table 1: Bearings: Classification accuracy for 10 fault types

| Target | TrainAll | RSC | MMLD | DFDG | DFDG+RSC |
|--------|----------|-----|------|------|----------|
| A      | 52.33    | 68.43 | 65.70 | 66.60 | 68.23    |
| B      | 90.50    | 91.10 | 95.37 | 89.30 | 90.90    |
| C      | 92.90    | 97.60 | 89.33 | 89.67 | 92.47    |
| D      | 74.97    | 77.73 | 65.87 | 77.73 | 77.97    |
| E      | 70.73    | 70.33 | 64.20 | 73.40 | 74.77    |
| F      | 88.53    | 86.40 | 79.03 | 91.50 | 90.23    |
| G      | 87.20    | 90.20 | 86.83 | 91.40 | 94.30    |
| H      | 85.20    | 90.50 | 75.53 | 85.30 | 88.37    |
| Avg    | 80.30    | 84.04 | 77.73 | 83.13 | **84.65** |

Table 2: HHAR: Classification accuracy for 6 activities

| Target | TrainAll | RSC | MMLD | DFDG |
|--------|----------|-----|------|------|
| Art    | 78.73    | 80.37 | 78.99 | 79.23 |
| Cartoon| 74.30    | 76.84 | 77.06 | 75.84 |
| Photo  | 94.55    | 94.99 | 95.41 | 95.45 |
| Sketch | 76.19    | 74.40 | 62.56 | 77.87 |
| Avg    | 80.94    | 81.65 | 78.51 | **82.10** |

Table 3: PACS: Classification accuracy for 7 classes.

Table 4: Ablation study of DFDG on Bearings dataset. Hyperparameter values 0 are represented by ‘-’ (dash).

| Regularization | Masking | Avg Accuracy (%) |
|----------------|---------|-------------------|
| α m qMax       |         |                   |
| 0              | - -     | 79.75             |
| 0.01           | - -     | 80.21             |
| 0.1            | - -     | 79.97             |
| - 33 30        | - -     | 83.21             |
| - 50 70        |         | 83.42             |

Table 3 shows the classification performance for the PACS dataset. MMLD performed irregularly across our runs on the Sketch domain where images have white backgrounds unlike those in the source domains, and lags clearly behind the other methods. DFDG improves performance over the baseline TrainAll uniformly across all 4 domains, and offers the best average accuracy of 82.10% in this comparison.

5.3. Ablation studies

We perform ablation studies on the effects of alignment regularization and input masking using the Bearings dataset. From Table 4 we see that regularization and masking both improve classification performance, with the latter having a larger effect. The exact amount of regularization and masking that works best varies by dataset.

We also study the effect of using different saliency maps for input masking on the Bearings dataset. The vanilla saliency map, which takes the derivative of the class logit with respect to the input, results in an average classification accuracy of 80.77%. This approach can produce noisy maps giving poor estimates of how class-discriminative an observation is. In contrast, SmoothGrad is less noisy, and obtains a noticeably higher accuracy of 83.42%.

6. CONCLUSION

In this paper, we proposed DFDG, a model-agnostic method for domain generalization that does not require domain labels for training. DFDG aligns class-conditional soft labels and masks superficial observations from training inputs to learn domain-invariant class-discriminative features. Overall, DFDG exhibits better performance against competing methods for both time series sensor and image classification problems. Namely, DFDG outperforms TrainAll and the state-of-the-art MMLD and RSC on the PACS image dataset and the HHAR sensor dataset. On the Bearings sensor dataset, RSC obtains a higher accuracy, however we demonstrate that DFDG can complement this method to achieve the best accuracy results.
