SFHarmony: Source Free Domain Adaptation for Distributed Neuroimaging Analysis

Nicola K Dinsdale\textsuperscript{1} \quad Mark Jenkinson\textsuperscript{2,3,4} \quad Ana IL Namburete\textsuperscript{1,2}

1. Oxford Machine Learning in NeuroImaging (OMNI) Lab, Department of Computer Science, University of Oxford, UK
2. Wellcome Centre for Integrative Neuroimaging, FMRIB, University of Oxford, Oxford, UK
3. Australian Institute for Machine Learning (AIML), Department of Computer Science, University of Adelaide, Adelaide, Australia
4. South Australian Health and Medical Research Institute (SAHMRI), North Terrace, Adelaide, Australia

nicola.dinsdale@cs.ox.ac.uk

Abstract

To represent the biological variability of clinical neuroimaging populations, it is vital to be able to combine data across scanners and studies. However, different MRI scanners produce images with different characteristics, resulting in a domain shift known as the ‘harmonisation problem’. Additionally, neuroimaging data is inherently personal in nature, leading to data privacy concerns when sharing the data. To overcome these barriers, we propose an Unsupervised Source-Free Domain Adaptation (SFDA) method, SFHarmony. Through modelling the imaging features as a Gaussian Mixture Model and minimising an adapted Bhattacharyya distance between the source and target features, we can create a model that performs well for the target data whilst having a shared feature representation across the data domains, without needing access to the source data for adaptation or target labels. We demonstrate the performance of our method on simulated and real domain shifts, showing that the approach is applicable to classification, segmentation and regression tasks, requiring no changes to the algorithm. Our method outperforms existing SFDA approaches across a range of realistic data scenarios, demonstrating the potential utility of our approach for MRI harmonisation and general SFDA problems. Our code is available at https://github.com/nkdinsdale/SFHarmony.

1. Introduction

Deep learning (DL) models have proved to be powerful tools for neuroimage analysis. However, the majority of neuroimaging datasets remain small, posing a challenge for the training of sophisticated architectures with many parameters. Thus, it is common practice to combine data from multiple sites and MRI scanners, both to increase the amount of data available for training, and to represent the breadth of biological variability that can be expected in diverse populations. However, the combination of data across MRI scanners with different acquisition protocols and hardware leads to an increase in non-biological variance \cite{25, 26, 50}, which can be large enough to mask the biological signals of interest \cite{49}, even after careful pre-processing with state-of-the-art neuroimaging pipelines \cite{23}. The development of harmonisation methods is therefore vital to enable the joint unbiased analysis of neuroimaging data from different scanners and studies.

The key goal for harmonisation methods is to be discriminative for the main task of interest whilst creating shared feature representations of the data across acquisition scanners, clearly mirroring the goal of domain adaptation (DA) \cite{15}. The majority of deep learning based harmonisation methods are based on DA methods, either using adversarial approaches to create shared feature embeddings \cite{15, 24}, or using generative approaches to create harmonised images \cite{11, 63}.

However, the vast majority of existing methods fail to be applicable in many realistic data scenarios. For example, MR images are inherently personal information so their sharing is protected by legislation, such as GDPR \cite{9} and HIPAA \cite{39}. Thus, the assumption of centralised data stores for model training is infeasible, particularly when working with clinical imaging data, which will be essential in order to produce representative models \cite{14, 52}. Distributed learning offers a promising solution, but the few proposed distributed harmonisation methods \cite{8, 16} assume the simultaneous presence of the source and target data. The source data may not be available for the adaptation phase, for instance, due to confidentiality agreements, loss of the source...
Figure 1. Schematic of the proposed SFHarmony method. The method fits a GMM to the source features, shares these via a global model store, and then completes SFDA by aligning the source and target feature distributions utilising a modified Bhattacharyya distance. $Q_s$ is the source feature representation and $Q_t$ is the target feature representation, and the figure shows the GMM setup, for a single feature $i$, when we are working with $K$, the number of components, being 2. This trivially generalises to more or less components.

data, or computational constraints [3]. Further, federated DA methods such as [16] would require retraining of the model to incorporate any new sites, which is infeasible and computationally expensive.

Therefore, we explore an unsupervised DA setting where only the source model, instead of the source data, is provided to the unlabelled target domain for harmonisation, known as Source Free Domain Adaptation (SFDA). This setting inherently protects individual privacy, whilst allowing the efficient incorporation of new sites without requiring target labels. We propose a simple yet effective solution, termed SFHarmony, which aims to match feature embeddings from the source and target, through characterising the embeddings as a Gaussian Mixture model (GMM) and the use of a modified Bhattacharyya distance [4]. This requires no modifications to the training of the source model, and the only additional communication is of summary statistics of the source feature embedding, allowing it to be simply applied to existing architectures. The summary statistics contain no information about individuals.

Our contributions are as follows: 1) We propose a new method for SFDA, SFHarmony, based on aligning feature embeddings, utilising a modified Bhattacharyya distance, requiring no changes to source training; 2) We demonstrate the method’s applicability to classification, segmentation and regression tasks, and show that the approach outperforms existing SFDA methods for domain shifts experienced when working with neuroimaging data; differential privacy and label imbalance.

2. Related Work

Unsupervised Domain Adaptation (UDA): UDA aims to exploit the knowledge learned from a source dataset to help to create a discriminative model for a related but unlabelled target dataset [33]. DL-based UDA approaches can broadly be split into three categories [33]: discrepancy-based, reconstruction-based, and adversarial. Discrepancy based approaches aim to minimise a divergence criterion, which measures the distance between the source and target data distributions encoded in a learned feature space [10, 27, 35, 48]. Reconstruction-based approaches, instead, use reconstruction as a proxy task to enable the learning of a shared representation for both image domains [5, 22, 38]. Finally, adversarial approaches deploy a discriminator that aims to identify the source of the data; the model is trained both to do the task and to trick the discriminator, creating domain invariant features [21, 51]. These methods all assume simultaneous access to the source and target data, which poses data privacy challenges.

Federated Learning and Domain Adaptation: Federated learning (FL) has been proposed as a method to train models on distributed data [36]. The data are kept on their local servers, and users train local models with private data and communicate the weights or gradients between sites for aggregation. Many FL approaches focus on minimising the impact of distribution shifts between clients [28, 45, 55]; however, most approaches assume that the data at all sites are fully labelled. However, federated DA enables the in-
corporation of an unlabelled site into the federation without sharing data. FADA [40] is a federated DA method, where features are shared between sites in a global knowledge store. The sharing of features, however, still poses privacy concerns as images may be recoverable from the features [19]. Thus, instead FedHarmony [16] encodes the features as Gaussian distributions and thus only the mean and standard deviations of the features need to be shared. Both of these methods still assume access to the source data during training and rely on adversarial approaches that are often unstable and hard to train. Other federated DA methods produce domain-specific models or ensembles [19, 41, 59, 61], meaning that the final predictions depend on the domain of the data.

Source Free Domain Adaptation: SFDA takes the federated approach a step further and assumes that there is no access to the source data available at all: only the source model is available for model adaptation. The majority of SFDA methods have been developed for classification [1, 13, 17, 32, 33, 43, 54, 60], with a few being proposed for segmentation [30, 31, 34, 44, 57]. There are two main approaches taken for SFDA. The first set of approaches are generative, aiming to create source samples using the source model weights [32, 34]. These approaches, however, pose concerns about individual privacy, especially when working with medical images and low numbers of samples [19] and cannot be simply applied to complex target tasks, limiting their utility when working with MRI data [53]. The second set aim to minimise model entropy to improve predictions, guided by various pseudo labelling or uncertainty techniques to prevent mode collapse [1, 13, 17, 29, 33, 43, 60]. These methods are often effective, but largely limited to classification tasks, and may require changes to the source model training to be effective [33, 60]. AdaMI [3] was proposed directly for medical image segmentation, but requires an estimate of the proportion of each label to prevent mode collapse. This ratio is hard to estimate for labels with high variability across populations, such as tumours or lesions. We could not identify any methods proposed for regression, where the lack of softmax outputs limit the direct application of methods based on entropy minimisation.

Harmonisation: Many existing harmonisation approaches are based on COMBAT [7, 20, 42], which uses a linear model to represent the scanner effects on image-derived features. DL-based approaches for harmonisation generally utilise a DA approach, with many being generative, aiming to produce ‘harmonised’ images [6, 11, 37, 62, 63], while the other branch uses adversarial approaches to harmonise the learned model features for a given task [15, 24]. All of these methods assume simultaneous access to the source and target data, with some even requiring paired data [11]. The only existing methods for harmonisation which consider data privacy are Distributed COMBAT [8] and FedHarmony [16]; however, both assume constant communication with the source site.

3. Method

The aim of this work is to create a SFDA method applicable to neuroimaging tasks, and to demonstrate its suitability for MRI harmonisation. Thus, the goal is to create a model where two images with the same label would share a feature embedding, regardless of the acquisition scanner – the domain of the data. We thus follow the framework of [51] and consider the network to be formed of a feature extractor, with parameters \( \Theta_{repr} \), and a label predictor, \( \Theta_p \). This network architecture is the same across source and target sites. The general schematic for training is shown in Fig. 1.

3.1. Creation of the Source Model

The first stage is the training of the source model. This assumes the availability of a labelled training dataset \( D_s = \{X^s_i, y^s_i\} \), where the image and label pairs depend on the task of interest. Unlike some existing methods [33, 60], our proposed approach requires no changes to the training of the source model or to the architecture. The model can thus be flexibly trained following the standard training procedure for the source data, with the goal being to create a well-trained source model. In our experiments, we consider the simplest source training, minimising a loss function \( L_{task} \) dependent on the task of interest with full supervision:

\[
L(X^s, y^s; \Theta_{repr}, \Theta_p) = \frac{1}{N_s} \sum_{i} L_{task}(X^s_i, y^s_i)
\]

where \( N_s \) is the total amount of labelled source data.

3.2. Global Information Store

For successful SFDA, we need to align the learned feature embedding, \( Q^s = f(X^s, \Theta_{repr}) \) for the source and target data. To achieve this without requiring the source data, we propose to follow the precedent of existing privacy-preserving medical imaging approaches [8, 16, 17] and, thus, create a global knowledge store to share summary statistics of the features. In [16], it is proposed that the features can be encoded as Gaussian distributions, and thus the statistics to be shared would be a mean and standard deviation per feature. We hypothesise that, for many tasks, especially classification tasks with discrete categories, simple Gaussian distributions are unlikely to sufficiently characterise \( Q^s \). We thus propose to describe the features using a Gaussian mixture model (GMM), with each feature being encoded as an independent 1D GMM, such that, for feature \( i \in N_{Q^s} \), where \( N_{Q^s} \) is the number of features in \( Q^s \):

\[
Q^s_i \sim \sum_{k=1}^{K} \pi_{k,i} \mathcal{N}(X^s_i; \mu_{k,i}, \sigma_{k,i}^2)
\]
where \( K \) is the number of components in the GMM, \( \mu_{k,i}^2 \) and \( \sigma_{k,i}^2 \) are the mean and variance defining the \( k^{th} \) Gaussian component of the \( i^{th} \) feature for the source site, and \( \pi_{k,i}^s \) is the weighting factor for this \( k^{th} \) Gaussian (which sum to one across components). Note that the features are considered before the activation function. The same number of components, \( K \), are fit for all features. Thus, the GMM for feature \( i \) is defined by the parameters:

\[
\Theta_i^s = \{ \pi_{k,i}^s, \mu_{k,i}^s, \sigma_{k,i}^2 \}, k = 1..K
\]  

(3)

and these parameters can be determined using Expectation Maximisation (EM), by finding the maximum likelihood estimate (MLE) of the unknown parameters:

\[
L(\Theta_i) = \sum_{n=1}^{N_{s,i}} \log(\sum_{k=1}^{K} \pi_{k,i}^s N(X_n^s; \mu_{k,i}^s, \sigma_{k,i}^2))
\]  

(4)

for each feature \( i \) in \( Q^s \). This, therefore, produces three parameter arrays that fully define the GMMs of the source features, which are communicated alongside the source weights to target sites:

\[
\Theta_{Q^s} = \{ \mu^s \in \mathbb{R}^{K \times N_Q^s}; \sigma^{s2} \in \mathbb{R}^{K \times N_Q^s}; \pi^s \in \mathbb{R}^{K \times N_Q^s} \}.
\]  

(5)

These parameters contain no individually identifying information, as they represent aggregate statistics across the whole population.

3.3. Target Model Adaptation

Given that we now have a well trained source model, with parameters \( \Theta_{\text{repr}}^s \) and \( \Theta_s^s \), and the source GMM parameters, \( \Theta_{Q^s} \), we can now adapt the model at any target site. We assume access to an unsupervised target, with only data samples \( X^t \) and no labels available.

We initialise the target model using the source trained weights. Model adaptation only involves finetuning the feature extractor to match the learned feature distribution across the two sites. In adversarial approaches, a discriminator is added to the overall architecture that aims to distinguish between source and target samples. We could utilise this approach, following [16], by drawing feature samples, using the source GMM parameters \( \Theta_{Q^s} \), but adversarial approaches are notoriously unstable and difficult to train. We therefore, instead, propose to minimise the difference between the source feature distribution and target feature distribution using the GMM parameters directly.

Therefore, the first step of model adaptation is to calculate the current target features, \( Q^t = f(X^t, \Theta_{\text{repr}}^s) \), and then, using the same EM approach as above, we can create the parameters of the target GMM fit:

\[
\Theta_{Q^t} = \{ \mu^t \in \mathbb{R}^{K \times N_Q^t}; \sigma^{t2} \in \mathbb{R}^{K \times N_Q^t}; \pi^t \in \mathbb{R}^{K \times N_Q^t} \}.
\]  

(6)

We propose to use a modified Bhattacharyya distance [4] as the loss function. The Bhattacharyya distance measures the similarity of two probability distributions, which for continuous probability distributions is defined as:

\[
D_B(p, q) = -\ln(BC(p, q))
\]  

(7)

where

\[
BC(p, q) = \int_{\mathbb{R}} \sqrt{p(x)q(x)}dx.
\]  

(8)

The Bhattacharyya distance has a simple closed form solution when the two probability distributions are both Gaussian. If \( p \sim \mathcal{N}(\mu_p, \sigma_p^2) \) and \( q \sim \mathcal{N}(\mu_q, \sigma_q^2) \) then:

\[
D_B(p, q) = \frac{1}{4} \left( \frac{\mu_p - \mu_q}{\sigma_p + \sigma_q} \right)^2 + \frac{1}{2} \ln \left( \frac{\sigma_p^2 + \sigma_q^2}{2\sigma_p \sigma_q} \right).
\]  

(9)

There is, however, no equivalent closed form solution for a GMM. In [46] they propose an approximation for the GMM as a sum of the Bhattacharyya distances for each pair of Gaussians in the mixture model, weighted by the associated \( \pi \) values. We suggest that this is not the most appropriate reformulation: we are more interested in the corresponding pairs of Gaussians than in the cross-relationships, as we do not wish to minimise the difference between cross pairs. Rather, we wish specifically to make the target distribution match the source. Thus, if we consider our target and source GMM distributions, parameterised by \( \Theta_{Q^t} \) and \( \Theta_{Q^s} \), we propose to use the following approximation:

\[
D_{GMM}(\Theta_{Q^t}, \Theta_{Q^s}) = \sum_{k=1}^{M} \pi_k^t \pi_k^s \left( \frac{1}{4} \left( \frac{\mu_k^t - \mu_k^s}{\sigma_k^t + \sigma_k^s} \right)^2 + \frac{1}{2} \ln \left( \frac{\sigma_k^t + \sigma_k^s}{2\sigma_k^t \sigma_k^s} \right) \right)
\]  

(10)

such that we find the weighted sum of the Bhattacharyya distances between each corresponding pair of Gaussians, where \( k \) is the component in the GMM. It can further be seen that this approximation retains the desirable property that when \( \Theta_{Q^t} = \Theta_{Q^s} \), then \( D_{GMM}(\Theta_{Q^t}, \Theta_{Q^s}) = 0 \). The correspondence between Gaussians can be ensured by simply ordering the parameters by the mean estimates.

Thus, the feature extractor is finetuned for the target site by minimising \( D_{GMM} \) averaged across all of the features in \( Q^s \). However, for each training iteration, only a fixed size batch is available to estimate the parameters, and for neuroimaging applications the maximum batchsize achievable is often small due to the relatively large image size [14], which affects the estimate of the GMM parameters. As EM is sensitive to initialisation, to mitigate the small batch effect, we initialise the EM algorithm only once per training epoch, using the previous batch estimate as the initialisation for the next, providing memory between batches. The EM algorithm is reinitialised for validation (needed to calculate validation loss), preventing data leakage.
3.4. Inference Time

Finally, inference for the test data simply involves combining the finetuned feature encoder, $\Theta^{\text{repr}}$, and the frozen source label predictor, $\Theta^s_p$, such that $\hat{y}_t = f(X_t, \Theta^{\text{repr}}, \Theta^s_p)$. This therefore ensures that, given data from the source or target domain with the same feature embedding, the same label prediction is achieved across sites.

4. Experimental Results

To validate the effectiveness of our SFDA framework, we conduct a range of experiments with both simulated data with known domain shifts, and real multisite MRI datasets, and we demonstrate the applicability of the method to classification, segmentation and regression tasks.

4.1. Datasets:

Further details for each dataset and model architectures are available in the Supplementary Materials. Example images from each dataset can be seen in Fig. 2.

[Image of example images from each dataset]

OrganAMNIST [56] (Classification): curated as part of MedMNIST [58], we use OrganAMNIST as a test dataset. All images were pre-processed to $28 \times 28$ (2D) with the corresponding classification labels for 11 classes. We created simulated known domain shifts, to enable exploration of the method, with the strength of each shift designed to be such that a degradation in performance was seen across the sites. The dataset was split into 5 sets, each with 5000 samples for training and 2000 for testing and the following domain shifts applied: 1) no shift (source site), 2) decreased intensity range, 3) increased intensity range, 4) Gaussian blurring, 5) salt and pepper noise, to model shifts likely across imaging sites. The backbone architecture took the form of a small VGG-like classifier, with categorical crossentropy as the task loss. Code to reproduce the data is provided.

CC359 [47] (Segmentation): The dataset consists of brain images of healthy adults (29-80 years) acquired on MRI scanners from three vendors: Siemens, Philips and GE, at both 1.5 and 3T, with approximately 60 subjects per vendor and magnetic field strength. A 2D UNet was trained on slices from each site, then the performance when applied to the remaining sites was compared. As a result, the Phillips 1.5T was chosen as the source site as it had the largest performance drop. No additional preprocessing was applied to the images apart from image resizing so that each subject volume was $128 \times 240 \times 160$. The data were split at the subject level per site, such that 40 subjects were available for training and 20 for testing. The segmentation task was skull stripping, using masks from the original study, and Dice loss was used as the task loss function. Further details and example segmentation masks can be found in the Supplementary Material.

ABIDE [12] (Segmentation and Regression): Four sites (Trinity, NYU, UCLA, Yale) were used, so as to span age distributions and subject numbers. The data were split into training/test sets as 80%/20%, yielding a maximum of 127 subjects for training (NYU) and a minimum of 35 (Trinity). NYU was the largest site, spanning the age distribution of all of the other sites, and so was chosen as the source site. For segmentation, we considered tissue segmentation (grey matter (GM), white matter (WM), CSF), using labels automatically generated using FSL ANAT. We used a 2D UNet trained on slices with Dice as the main task loss function. Dice score was averaged across the three tissues. For age prediction, a separate network was trained, following the setup and architecture in [16], with MSE as the main task loss. Further details and example labels can be found in the Supplementary Material.

Implementation Details: All comparison methods used the same task-specific backbone architecture as the proposed method. Features were extracted in the second-to-last layer, before the activation function, following the result in [15]. Model architectures were chosen to give good source performance while allowing the use of large batch sizes, but most standard architectures could be used. Train-
ing was completed on an A10 GPU, using PyTorch 1.12.0. All models were trained with five-fold cross validation and results are presented on the holdout test set. A learning rate of $1 \times 10^{-6}$ was used for all datasets for adaptation with an AdamW optimiser.

### 4.2. Classification: OrganAMNIST

**Baselines:** For the classification task, we first compare our approach to supervised oracles: source model only, centralised data, and target finetuning with frozen label predictor. We then compare to DeepCORAL [48], and two federated DA approaches: FADA [40] and FedHarmony [16], both of which require the presence of the source data. Finally, we compare to SFDA methods: entropy minimisation; SHOT [33], USFAN [43], and gSFDA [60]. We do not compare to any generative SFDA methods, as the ability to create source data would not meet privacy requirements for many applications [53], especially given that GANs often replicate training images when trained with small datasets [19]. Details are provided in the Supplementary Material.

**Methods Comparison:** We first demonstrate the method for a range of batchsizes (5, 50 and 500) because methods that minimise entropy are expected to be more stable when using large batchsizes, which are rarely achievable when working with MR images due to the memory constraints posed by large image sizes [14]. Thus, robustness to the batchsize is vital if a SFDA method is to be used for harmonisation. We use a single source model to allow fair comparison, trained with a batchsize of 50. We wish to maximise performance across all sites: as harmonisation is normally framed as a joint domain adaptation problem [15], the average performance across all sites is reported.

The results can be seen in Table 1, alongside the baseline methods. It can be seen that SFHarmony outperforms the existing SFDA methods, especially when a small batchsize was used for training (86.22% for batchsize 5). SHOT [33] showed comparable performance to SFHarmony when trained with a batchsize of 500 (85.27%), but was highly dependent on the modified source training. Interestingly, several of the SFDA approaches outperformed the adversarial approaches despite them having access to the source data, possibly due to the instability of such approaches.

The proposed $D_{GMM}$ loss is clearly able to align the features across sites using only the GMM summary statistics. This is demonstrated by Fig. 3, which shows the source and target features for each site before and after DA. Clearly the features overlap much more after DA, which both leads to the clear improvement in performance, and shows that the approach is achieving the harmonisation goals of the model having a shared feature embedding across sites. The change shift in the features is more visible for the intensity based shifts (1-2 and 1-3) suggesting that the two largest PCA components largely encode intensity. Thus, as the noise augmentations do not create values outside of the existing intensity range, the noise shifts do not lead to large changes to the features in the PCA space.

We tried modelling the features with $K \in \{1, 2, 3\}$ GMM components: visual inspection of the features suggested that at least 2 components would be beneficial. This was confirmed by the results, with the best performance being achieved when modelling the features with 2 components, as shown in Table 1. However, the approach still performed well for 1 and 3 components, showing limited sensitivity to the number of components chosen. The number of components chosen is the only additional hyperparameter to be tuned with our approach, with only a single loss function to minimise. The results clearly show the robustness to the choice of batchsize, and the results were also robust to the
<table>
<thead>
<tr>
<th>Method</th>
<th>S</th>
<th>T</th>
<th>C</th>
<th>Information Communicated</th>
<th>Batchsize 5</th>
<th>Batchsize 50</th>
<th>Batchsize 500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Model</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>All Data</td>
<td>88.34</td>
<td>91.65</td>
<td>91.27</td>
</tr>
<tr>
<td>Centralised Data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Model Weights</td>
<td>88.15</td>
<td>88.96</td>
<td>83.26</td>
</tr>
<tr>
<td>Target Finetune</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>Model Weights + Features</td>
<td>81.69</td>
<td>76.77</td>
<td>76.53</td>
</tr>
<tr>
<td>DeepCORAL [48]</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>Model Weights + Statistics</td>
<td>81.48</td>
<td>76.12</td>
<td>76.20</td>
</tr>
<tr>
<td>FADA [40]</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Features</td>
<td>82.43</td>
<td>83.85</td>
<td>83.65</td>
</tr>
<tr>
<td>FedHarmony [16]</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>81.69</td>
<td>76.77</td>
<td>76.53</td>
</tr>
<tr>
<td>Minimise Entropy</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights</td>
<td>42.59</td>
<td>83.54</td>
<td>83.96</td>
</tr>
<tr>
<td>SHOT [33] (no smoothing)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights</td>
<td>66.86</td>
<td>83.60</td>
<td>85.40</td>
</tr>
<tr>
<td>SHOT [33] (Source batchsize 5)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights</td>
<td>72.06</td>
<td>74.44</td>
<td>74.61</td>
</tr>
<tr>
<td>SHOT [33] (Source batchsize 500)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights</td>
<td>83.10</td>
<td>84.68</td>
<td>85.27</td>
</tr>
<tr>
<td>gSFDA [60]</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights</td>
<td>60.57</td>
<td>85.87</td>
<td>84.67</td>
</tr>
<tr>
<td>USFAN [43]</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights</td>
<td>26.94</td>
<td>79.83</td>
<td>83.79</td>
</tr>
<tr>
<td>SFHarmony 1 GMM Component</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>85.47</td>
<td>85.71</td>
<td>86.16</td>
</tr>
<tr>
<td>w/o EM (Direct Fit)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>77.26</td>
<td>76.99</td>
<td>86.03</td>
</tr>
<tr>
<td>w/o Batch Memory</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>80.25</td>
<td>82.13</td>
<td>84.60</td>
</tr>
<tr>
<td>SFHarmony 2 GMM Components</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>86.22</td>
<td>86.25</td>
<td>86.21</td>
</tr>
<tr>
<td>SFHarmony 3 GMM Components</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>86.21</td>
<td>85.70</td>
<td>85.96</td>
</tr>
</tbody>
</table>

Table 1. Results on the OrganAMNIST classification task. S = Source data required, T = Target labels required, C = Centralised data. The average accuracy is across all 5 sites, weighted equally, and is reported for training batchsizes of 5, 50 and 500. Best SFDA method for each batchsize is in bold, other methods are included for reference. The w/o (without) components form an ablation study.

The choice of learning rate, with the accuracy staying within 1% of the best result across learning rates from $10^{-7}$ to $10^{-4}$. Therefore, deployment of the proposed approach requires no changes for a new site, only the choice of the number of components for a new source model. This is in contrast to many existing SFDA approaches that require the balancing of several loss functions (e.g. [3, 33]).

**Ablation Study:** We considered the GMM with $K = 1$, allowing us to explore the w/o EM case, where $\mu$ and $\sigma^2$ are calculated directly. We also considered removing the batch memory across the training loop, reinitialising the EM algorithm before each batch. From Table 1 it is clear that both aspects are contributing to the performance, especially for small batchsizes.

**Class Imbalance:** In the above experiments, the distribution of class labels was approximately equal across sites. We now consider the extreme scenario where the source site contains samples from across all classes but target sites are missing classes. This is a conceivable scenario when considering MR images, where a given clinical site specialises in a certain condition and we are trying to harmonise the data to a carefully curated research dataset. Figure 4 shows the average accuracy across sites, when the target sites had samples from an increasing number of classes removed. Each comparison method was trained using the best setting from Table 1. The proposed SFHarmony approach was more robust to the increased class imbalance than existing SFDA methods.

**Differential Privacy (DP):** Finally, we considered simulating the approach when DP is being used to further protect privacy. We simply simulated a Laplace mechanism of DP [18], by injecting noise onto the weights before communication, modelled as: $w = w + \text{Lap}(|w| f)$ where $f$ was varied to create increasing levels of noise. As the GMM is fit at the local site, $\Theta_Q$ can be calculated before the noise is applied. The comparison methods were again all trained using the best setting from Table 1. Although this is a very simple model of DP, with many more sophisticated approaches existing, Fig. 5 demonstrates that many existing methods for SFDA are very sensitive to the applied noise. SHOT [33] is the most dramatically affected, with the pseudo-labelling approach suffering a significant degradation in performance. Our proposed approach maintained...
4.3. Segmentation: CC359 and ABIDE datasets

We now demonstrate our approach on two multisite MRI datasets for segmentation tasks: brain extraction (CC359) with two labels (brain/background) and tissue segmentation (ABIDE) with four labels (WM, GM, CSF, background).

**Baselines:** There are far fewer existing methods for SFDA, and we again did not compare to generative approaches. Thus, we compared to supervised oracles: source model only, centralised data and target finetuning with the frozen label predictor; semisupervised approaches: DeepCORAL [48], FADA [40] and FedHarmony [16]. Then, for SFDA approaches, we compared to minimising entropy, AdaEnt [2] and AdaMI [3], and Direct Fit (w/o EM in ablation study). We were unable to train DeepCORAL with a batchsize of more than 5 due to memory constraints.

**Methods Comparison:** Table 2 shows the results for both tasks. In the classification task there were only 32 features in the fully connected layer; however, now there are many more, for instance for the CC359 data there are 65536 features across all of the convolutional filters. Despite this increase in features, SFHarmony was able to complete the DA for both segmentation tasks, leading to an improved Dice score over the existing methods, across the batchsizes considered. Again, the existing SFDA methods were very sensitive to batchsize, and AdaMI was also sensitive to the choice of tissue ratio prior: as we were completing the segmentation tasks on 2D slices, different slices had varying amounts of the target label present and we had to create a prior that was dependent on slice depth to achieve reasonable performance. The ABIDE tissue segmentation task was more challenging, as can be seen by the comparatively lower Dice Scores, especially due to the large imbalance in tissues, which affected the performance of AdaMI.

No changes needed to be made to the approach compared to the classification task, including the learning rate, showing the generalisability of the method across tasks.

**Subsampling Features:** The increase in the number of features for segmentation is a potential limiting factor for the approach, especially if the approach is to be expanded...
to 3D networks. As the features learned by convolutional layers are highly correlated, large amounts of redundancy exist between the features; thus we considered selecting only a random subset of the features. The procedure would be identical on this subset and the only additional information to be shared would be the random subsampling indices which would be the same across sites. We explored this approach for the CC359 data (3 components, batchsize 5), and the result can be seen in Table 3. It can be seen that using a smaller subset of the features leads to only a small drop in performance for the segmentation task, such that SFHarmony still outperforms the existing methods when less than 1% of the features are shared. Therefore, when expanding the approach to 3D datasets, subsampling the features is likely to be a sensible compromise between performance and the amount of information to be shared between sites.

4.4. Regression: ABIDE dataset

**Baselines:** We could not identify any appropriate SFDA baselines. Therefore, the only comparison methods were source model only, centralised data and target finetuning with frozen label predictor, DeepCORAL [48], FADA [40], FedHarmony [16] and Direct Fit. The maximum batchsize possible was 16, and so we tried batchsizes of 4, 8 and 16.

**Methods Comparison:** It can be seen from Table 4 that for the age prediction task FADA [40] outperformed our proposed approach for two of the three reported batchsizes, unlike in the other tasks. This may well be because the task was completed in 3D, and thus, a small number of samples were available, meaning that the presence of the source data supported the model training. SFHarmony did, however, show comparable performance, especially when modelling the features with more components. We could not identify any SFDA methods in the literature that could be directly applied to regression tasks. Our method is flexible and can be directly applied to the regression task without any change to the model architecture or DA procedure.

### Table 4. Results on the ABIDE dataset for the age prediction task. S = Source data required, T = Target labels required, C = Centralised data, Bs = Batchsize. The average MAE is the performance across all 4 sites, weighted equally, and is reported for training batchsizes of 4, 8 and 16. 16 was the largest batch achievable. The best SFDA method for each batchsize is in bold.

<table>
<thead>
<tr>
<th>Method</th>
<th>S</th>
<th>T</th>
<th>C</th>
<th>Information Communicated</th>
<th>Average MAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Model</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>4.38</td>
</tr>
<tr>
<td>Centralised Training</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>All Data</td>
<td>3.52 3.38 3.36</td>
</tr>
<tr>
<td>Target Finetune</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>Model Weights</td>
<td>3.57 3.60 3.58</td>
</tr>
<tr>
<td>DeepCORAL [48]</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>All Data</td>
<td>4.58 4.41 4.12</td>
</tr>
<tr>
<td>FADA [40]</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Features</td>
<td>3.55 3.42 3.78</td>
</tr>
<tr>
<td>FedHarmony [16]</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>3.61 3.50 3.79</td>
</tr>
<tr>
<td>Direct Fit</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>4.70 4.31 4.05</td>
</tr>
<tr>
<td>SFHarmony 1 GMM Component</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>4.21 4.13 3.71</td>
</tr>
<tr>
<td>SFHarmony 2 GMM Components</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>3.87 3.72 3.69</td>
</tr>
<tr>
<td>SFHarmony 3 GMM Components</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Model Weights + Statistics</td>
<td>3.64 3.72 3.73</td>
</tr>
</tbody>
</table>

5. Conclusion

We have presented SFHarmony, a method for SFDA, motivated by the need to harmonise MRI data across imaging sites while relaxing assumptions about the availability of source data. We have demonstrated the applicability of the method to classification, regression, and segmentation tasks, and have shown that it outperforms existing SFDA approaches when applied to MR imaging data. The approach is general, allowing it to be applied across architectures and tasks. Possible limitations may arise due to the increase in features when applying the approach to 3D volumes, but the initial results on subsampling the features for the segmentation task suggest that the approach will still be applicable.

6. Acknowledgements

ND is supported by a Academy of Medical Sciences Springboard Award. MJ is supported by the National Institute for Health Research, Oxford Biomedical Research Centre, and this research was funded by the Wellcome Trust [215573/Z/19/Z]. WIN is supported by core funding from the Wellcome Trust [203139/Z/16/Z]. AN is grateful for support from the Academy of Medical Sciences under the Springboard Awards scheme (SBF005/1136), and the Bill and Melinda Gates Foundation.

### References


