Background Invariant Classification on Infrared Imagery by Data Efficient Training and Reducing Bias in CNNs

Maliha Arif,1,2
Calvin Yong,2†
Abhijit Mahalanobis1,2
1Center for Research in Computer Vision (CRCV)
2University of Central Florida
4000 University Boulevard
Orlando, Florida, USA 32816
{maliha.arif,calvinyong}@knights.ucf.edu, amahalan@crcv.ucf.edu

Abstract

Even though convolutional neural networks can classify objects in images very accurately, it is well known that the attention of the network may not always be on the semantically important regions of the scene. It has been observed that networks often learn background textures which are not relevant to the object of interest. In turn this makes the networks susceptible to variations and changes in the background which negatively affect their performance.

We propose a new two-step training procedure called split training to reduce this bias in CNNs on both Infrared imagery and RGB data. Our split training procedure has two steps: using MSE loss first train the layers of the network on images with background to match the activations of the same network when it is trained using images without background; then with these layers frozen, train the rest of the network with cross-entropy loss to classify the objects. Our training method outperforms the traditional training procedure in both a simple CNN architecture, and deep CNNs like VGG and Densenet which use lots of hardware resources, and learns to mimic human vision which focuses more on shape and structure than background with higher accuracy.

Introduction

Deep CNNs with millions of parameters are able to learn complex patterns by developing low-level feature understanding leading to high-level scene understanding. However, training such deep networks requires huge amounts of training data that in turn requires too many computing resources. The very popular VGG (Simonyan and Zisserman 2014) was trained using 4 NVIDIA Titan Black GPUs, and it took 2–3 weeks to train the architecture on 1.3 million images of the ImageNet dataset. When the dataset is limited in size, the network is often unable to learn the semantically important regions of the scene for object classification. An example of this occurs for infrared object recognition where the data sets are relatively small, and applying transfer learning to networks trained with RGB data does not work well. Motivated by such issues, we propose a split training method to efficiently learn from limited available data on infrared imagery and RGB data without relying on deep models, at the same time reducing background bias in CNNs.

It is very important to understand what the learned representations in a deep CNN correspond to. In many cases, it is ignored as long as the accuracy and generalization capabilities of the network is observed to be high. We question this narrative in our research and try to see what the learned representations are using Grad-CAM (Selvaraju et al. 2017). CNNs when trained with cross-entropy loss do not always use the actual target when making a prediction for an image; yet we would like such a model to be aware of the target. Figure 1 shows the gradient class activation map (Grad-CAM) (Selvaraju et al. 2017) on test images from a deep CNN model trained with images of a tank placed in a textured background. On the right is a test image of a tank with background. While the model has classified the target correctly, the attention map shows the strong contribution of the background to the result. The test image on the left contains a tank but no background. Yet the same network (trained on images involving background), produces a Grad-CAM attention map which is largely outside the object of interest. Our goal is to avoid this problem by forcing the CNN to...
learn the semantic features (shape and structure) rather than background before it makes a prediction.

Different works have tried to address the background bias problem. A very recent work by (Sehwag et al. 2020) explicitly studies the effects of background on the classification performance of deep CNNs. Their focus is on background invariance and background influence, which they observe by switching backgrounds and by masking the foreground, and then performing classification respectively. They show using a series of experiments on deep CNNs (like ResNet-18) and diverse datasets (like ImageNet), that even though the foreground is masked/removed, the network can still correctly identify the class. Similarly, when the background is switched and foreground remains intact, test accuracy decreases. On the VOC12 dataset (Everingham et al. 2013), test accuracy decreases from 75% to 46% when different backgrounds are introduced and object of interest or foreground is kept the same. The question is, are the current training paradigms being used in deep learning the only way to train a deep CNN? What is the CNN actually using when it makes a prediction? And how can available data be used efficiently for better test accuracy? To answer these questions, we propose a novel training strategy called ‘Split training’ which aims to teach the model to focus on the object (and ignore the background) by matching its activations at some specified layer to that of another model which was trained on masked (background removed) images and consequently produces ideal activations as shown in Figure 2.

Our method outperforms the standard training method and transfer learning methods, and produces activation maps that show the object is used to make predictions rather than texture and background. In the following sections, we describe some related studies, our proposed training method, and then various experimental results and ablation studies.

### Related Work

Different works have tried to address the background bias problem. (Chen et al. 2017) propose a dual path network (DPN) which outperforms both ResNet and DenseNet deep CNNs. In particular, a shallow DPN with 26% smaller model size surpasses ResNet-Xt-101 performance on ImageNet dataset which shows that just because a network is deep, it still might not be learning the best representations of the data. Further, it also uses 25% less computational power and 8% lower memory hence reducing the overall carbon footprint. (Xiao et al. 2020) study confirms that standard image classification models rely too much on signals from background and ignore foreground. Background correlations are largely predictive and influence model decisions to a great extent. Models often misclassify images even when correct foregrounds are present, up to 87.5% of the time when random adversarial backgrounds are chosen. The backgrounds become a strong point of correlation between images and their labels which the authors show comprehensively via experiments involving ImageNet dataset with modified backgrounds. The backgrounds are created in a very interesting fashion. Some subsets include unmodified background but black foreground and some include unmodified background but tiled foreground. Some subsets also involve black background and unmodified foreground which we will use in our proposed training method. (Zhu, Xie, and Yuille 2016) exploit the visual hints in an image by learning them explicitly and adding them in a conventionally trained CNN model to increase test classification. They also show through a series of experiments how deep CNNs achieve high performance by relying on visual contents of the whole image, mostly the background. By contrast humans tend to learn and classify objects based on foreground which is shown by conducting human recognition experiments on either pure background or pure foreground (created using bounding boxes). The results indicate that human beings are outperformed by networks trained on background but are able to beat deep CNNs when trained on foreground implying that deep CNNs fail to classify images based on object shape and structure. A recent work that indicates how CNNs are biased by texture is (Geirhos et al. 2018). The authors demonstrate texture bias using all major deep CNN models and experiment with stylized versions of ImageNet dataset, similar to the way done in (Xiao et al. 2020). They create grayscale versions of objects which contain both shape and texture, silhouette images where object outline is filled with black color, images with only edges and lastly images with contrasting shapes and textures, for example a cat with texture of an elephant. All popular deep CNN for image classification fail to recognize shape and do better with texture, VGG-16 gives 17.2% accuracy using shape vs. 82.8% when using texture; GoogleNet gives 31.2% using shape vs. 68.8% when using only texture and ResNet-50 gives 22.1% accuracy using shapes as compared to 77.9% when using texture. Human observers do much better as expected with 95.9% accuracy when shapes are clearly defined. These results confirm our theory and are a motivation behind our proposed training method which aims to guide a network...
to focus more on object shape than background and texture. Lastly, as mentioned before deep networks like VGG-16 fail to work well with Infrared images due to different domain types. VGG-16, ResNet and Densenet have been trained on ImageNet (an RGB dataset) hence transfer learning does not work well when such networks are finetuned on infrared imagery.

Datasets

**Synthetic IR data - (Infrared Imagery):** The first dataset we use for our experiments is a synthetic infrared dataset of military vehicles. The dataset contains three classes/targets: APC, tank, and truck. Each of the targets are in 18 different backgrounds and thermal signatures, and viewed in various angles, with azimuth angles between 0° and 359°, and elevation angles of 15°, 30°, 45°, 60°, 75°, and 90°. This gives a total of 38880 images per class, and thus a total of 116640 images for the entire dataset. Examples from the dataset are shown in Figure 3. Our dataset also contains masks that we can use to remove the background of each target. Figure 4 shows the same images as Figure 3 but with the background removed by using the mask. The masked dataset will be used to train our primary model, while the dataset including the background will be used to train the secondary model.

**Preprocessing:** The infrared images have a different pixel range compared to color (RGB) images. Infrared images use 16 bits per pixel, and in the dataset, the pixel values range from about 400 to 4000. For preprocessing, we centered the image by subtracting the mean value of the target from each pixel, then scaled the image to unit variance. To generate the images with no background, we take the pre-processed dataset with background, and set the background pixels to 0. This ensures that the target values are the same between the dataset with background and the dataset without background.

**MS-COCO (RGB data):** We also illustrate our work using RGB data to show our method’s validity. MS-COCO is a main-stream computer vision dataset for object detection, segmentation and classification. Figure 5 and 6 show examples of unmasked and masked images which we use in our experiments. MS-COCO has 91 categories in all, with 81 suitable for segmentation. These object categories are grouped into 11 super categories. We make use of 10 of the 81 classes for instance segmentation and perform 2 experiments - one involving 3 classes and one involving 10. These classes include airplane, dogs, elephant, motorcycle, bus, giraffe, umbrella, tie, tennis racket and clock. In order to avoid confusion between classes, we selected training images which have only one object. However, we do end up with few images having multiple instances of the same class (and multiple classes) as can be seen in Figure 5. We use a total of 20k training images (2k per class) and 1k test images. To create the set of masked images i.e. with background removed (Figure 6), we use Pycoco (VP 2020) library and the ground truth annotations provided with the dataset. We mask the background by replacing the corresponding pixel values by zero. MS-COCO is a complex dataset with much of the images containing a lot of background, as a result of which the object of interest appears to be very small and not in the center. This becomes a good challenging point for our proposed method.

**Preprocessing:** The RGB pixel values range from 0 to 255 unlike infrared images. We perform our experiments with and without mean target subtraction and find out that without mean target subtraction, our model performs better. Hence we stick to only normalizing our dataset by scaling the images to unit variance.

**Method**

Our split training method comprises of 3 main steps which are as follows:

1. First train a primary model - m1 (a simple CNN) using cross-entropy loss on masked images (no background).
2. Next, train a secondary model - m2 (architecturally identical to the primary model), using unmasked images such that the MSE between the activations of one of the higher convolutional layers of the secondary and primary networks is minimized.
3. Lastly, freeze the trained layers of the secondary model.

   Using unmasked images, train the remaining layers to the end of the network using cross entropy (CE) loss.

The premise is that by design the primary network learns and responds to target information (since there is no background). Forcing the activations of the primary and secondary network to be similar encourages the latter to re-
Figure 5: MS-COCO sample images with background (Unmasked) - First row: Airplane (Left and second last to Right), Dog (Second to left and Right); 2nd row (L to R): Elephant, Motorcycle, Bus, Giraffe; 3rd row (L to R): Umbrellas, Tie, Tennis racket, Clock.

Figure 6: MS-COCO sample images without background (Masked) - First row: Airplane (Left and second last to Right), Dog (Second to left and Right); 2nd row (L to R): Elephant, Motorcycle, Bus, Giraffe; 3rd row (L to R): Umbrellas, Tie, Tennis racket, Clock.

respond to the target and thereby learn to ignore the background. The proposed approach is also shown in Algorithm 1. Our method differs from transfer learning methods in the following way. When finetuning a model pretrained on some dataset $D_1$ with another target dataset $D_2$, the convolutional layers are frozen with features learned from $D_1$ using large amounts of data, while the fully connected layers are finetuned to classify samples from $D_2$. In our split training method, all of the layers are trained using samples from the target dataset $D_2$. The model first starts with randomly initialized weights. Then the convolutional layers of the secondary model are trained to learn features from $D_2$ to match the activations of the primary model trained on $D_1$. Then, with those convolutional layers frozen, the fully connected layers are trained to learn weights to classify samples from $D_2$ given the features from the frozen convolutional layers.

Algorithm 1: Split training method

Require: $i \leftarrow$ Training Images
1: for $i \in \{1...n\}$ do
2: $\text{mean}_{i \in \{\text{mask} \neq 0\}}$.mean() \{For IR images\}
3: $i = \text{mean}$ \{For IR images\}
4: normalize $i$
5: if masked then
6: $i[\text{mask} == 0] = 0$
7: end if
8: end for
9: $m1 \leftarrow$ Train primary model on masked images $i1$
10: $m2 \leftarrow$ Train secondary model on Unmasked images $i2$
11: $k \leftarrow$ Last feature layer of network
12: for layer $\in \{1...k\}$ do
13: Optimize layer
14: loss = MSE $[m1(i1) - m2(i2)]$ \{For matching activations\}
15: use lr=1e-3
16: end for
17: for layer $\in \{1...k + 1...n\}$ do
18: Load weights ($m2$) and finetune layer $\in \{1...k\}$
19: Optimize layer
20: loss = CE
21: use lr=1e-4
22: end for

Experiments

Synthetic IR data

We perform 2 sets of experiments using the synthetic IR data - one set of experiments use a train/test split involving 120k original images using the data set as provided, and the second using images in random background. We use a simple CNN architecture which is a feedforward network with 4 Conv-BatchNorm-ReLU-MaxPool blocks. We train our network in 3 ways, one using masked images which gives us our ground truth activations, second using unmasked images and standard training procedure and then lastly, using unmasked images together with our split training method. For our split training method, we use the last feature layer as well as an intermediate layer for comparison. We use Adam optimizer and learning rate of 1e-3 to train our initial layers using Mean Square Error(MSE) loss function. Once this part of the network is trained, we freeze the weights and train the top classifier part using Cross Entropy(CE) loss. We also compare our results with other architectures, details of which are ahead under section Ablations and Comparisons. This is followed by another set of experiments where we modify our test set and make it more challenging.

Table I show the mean and standard deviations for the accuracy of each model architecture trained with various methods. Our method outperforms the standard (conventional) training and finetuning methods, with performance gains depending on the choice of feature layer to match the secondary model’s activations with. With Mobilenet, if we perform the MSE loss on the last feature layer, we get that our method does as well as the standard training method, yielding about 74% accuracy. We believe this is because the
Table 1: Test accuracies for each architecture and training method on synthetic IR (infrared) data. Numbers in parentheses are the standard deviation of the accuracies over 10 runs.

| Architecture | Standard Training | Finetuning / Transfer learning | Ours (last feature layer) | Ours (intermediate layer) |
|--------------|-------------------|-------------------------------|--------------------------|---------------------------|
| Simple       | 75.162% (5.576%)  | 69.160% (3.050%)             | **91.664% (2.435%)**     | 87.222% (6.648%)          |
| Mobilenet    | 73.580% (8.243%)  | 34.191% (6.161%)             | 74.319% (5.536%)         | **93.226% (2.118%)**     |
| VGG11        | 72.798% (13.000%) | 48.224% (7.565%)             | **89.355% (3.498%)**     | 83.537% (7.338%)          |
| Densenet     | 66.597% (7.741%)  | 50.098% (4.361%)             | **85.388% (2.604%)**     | **88.557% (3.712%)**     |

Table 2: Test accuracies on synthetic IR (infrared) data for each architecture and training method on the random background test dataset.

| Architecture | Standard | Finetuning / Transfer learning | Ours (last feature layer) | Ours (intermediate layer) |
|--------------|----------|-------------------------------|--------------------------|---------------------------|
| Simple       | 70.417% (5.830%) | 83.875% (2.372%)             | **88.070% (5.757%)**     | 83.118% (5.802%)          |
| Mobilenet    | 67.558% (6.048%) | 45.961% (8.007%)             | 80.158% (3.555%)         | **95.969% (2.189%)**     |
| VGG11        | 62.337% (8.995%) | 69.323% (5.503%)             | **86.238% (4.417%)**     | 80.548% (5.469%)          |
| Densenet     | 66.378% (1.363%) | 55.573% (1.698%)             | **85.305% (2.184%)**     | **85.753% (2.208%)**     |

output shape at that layer has 1280 channels each with size 4 x 4. The spatial dimension at the output is very small, and the model may not benefit from the information that the activations of the secondary model give. When we use a layer closer to the input, and where the shape is large enough, we get a significant increase in performance, yielding a validation accuracy of 93%. A poor choice in an intermediate feature layer can be worse than the last feature layer, as the results for VGG show.

Random background Test Data For each class, we take 3 subsets of thermal signatures to use for our test set. When choosing our subsets, since some backgrounds may look similar, we visually check them in order to avoid validating on images that may look similar to the training set. This gives us about a 83- 17 training-test split. Figure 7 shows the 9 subsets of the data we choose, which are viewed with 0° azimuth and 90° elevation. From top to bottom, the rows correspond to APC, tank, and truck class. Since our goal is to have the model focus on the target and ignore the background, we also validate on the synthetic IR dataset, by replacing the background with a random solid color. That way, we hope that if our method does actually learn to ignore the background, the model should also do well on the dataset with random background. We initialize each model per training method with the same weights for uniformity. We find average of test accuracies on this random background data for each model across 10 runs, and report the mean and standard deviation in Table 2. Here we show the validation accuracy for the architectures and training methods on the random background test set. We see similar results to Table 1. The finetuning validation accuracy for the random background test set is higher than the finetuning accuracy on the regular validation set. This could be due to the pretrained model being trained on images with no background and random test set (mix set) also containing images with no background(random solid color).

Ablations and Comparisons On synthetic IR dataset, we compare our method with the conventional training method using only cross entropy loss, and also transfer learning. For our method, we experimented with the last feature layer for the MSE loss, along with an arbitrary chosen layer between the input layer and the last feature layer. We benchmarked our method on 4 different models: a simple CNN, Mobilenet (Sandler et al. 2018), VGG (Simonyan and Zisserman 2014), and DenseNet (Huang et al. 2017). To clarify, we only used the architecture of these deep models which are known to work really well on RGB data. When we say we did transfer learning, we trained the deep model first using masked images of our IR dataset only and then finetuned using unmasked images and reported those results. We did not use pre-trained weights, trained on RGB - ImageNet data since they do not work well on Infrared imagery (Arif and Mahalanobis 2021). Further, we do not want to employ a method that adds to the carbon footprint during training and uses lots of hardware resources/GPUs and memory.

Choice of Intermediate Layer Table 3 shows the validation accuracies for Mobilenet on the infrared dataset with background for varying output activation sizes. The activation sizes are denoted by (c;h;w), where c is the number of channels, h is the height, and w is the width. The table shows that the intermediate feature layer that had an output size of

| Activation Size | Validation Accuracy | Standard Deviation |
|-----------------|---------------------|--------------------|
| (24, 30, 30)    | 88.907%             | 3.282%             |
| (32, 15, 15)    | 94.417%             | 2.110%             |
| (64, 8, 8)      | 96.318%             | 1.165%             |
| (96, 8, 8)      | 92.503%             | 2.638%             |
| (1280, 4, 4)    | 93.226%             | 2.118%             |
Table 4: Total Computation (training) time using different pretrained networks and our method

| Network     | Split Training/ Transfer learning | Training time(s) |
|-------------|----------------------------------|------------------|
| Simple      | Split Training                   | < 36000 s        |
| Mobilenet   | Transfer learning                | > 44800 s        |
| VGG11       | Transfer learning                | > 1,209,600 s    |
| Densenet    | Transfer learning                | > 1,209,600 s    |

(64, 8, 8) yielded the highest accuracy. So in few cases, it could be beneficial to target an intermediate feature layer with a large enough spacial size.

**Computation Time:** We also want to note the computation time for the different methods and training strategies. Table 4 shows these statistics. A simple network using our method takes less than 36000 s ~10 hrs to train on 3 classes of the infrared data. MobileNet is known to be nearly as accurate as VGG and is 32 times smaller and 27 times less computationally expensive (Sandler et al. 2018). VGG network alone took around 2-3 weeks when being trained on ImageNet, so whatever dataset it is finetuned on will cumulatively take longer than 1,209,600 s ~336 hours. In our exclusive case, since we did not use pretrained weights and trained on VGG11 architecture from scratch, the depth and additional parameters meant longer training time than 10 hrs. Densenet networks are the most memory hungry networks among all popular deep models. Further, they are much deeper than VGG or MobileNet architectures. Computation time to train ImageNet dataset on Densenet is similar to VGG networks or more. Hence cumulative time to finetune on another dataset would be greater than 14 days ~1,209,600 s ~336 hours also. Training from scratch took longer than a simple CNN network that we proposed for our split training method.

**MS-COCO**

On MS-COCO (RGB data), we perform 2 experiments. First, we use only 3 classes as a starting point. We use 6k training images and 300 test images. We use a simple CNN as our shallow base network. It consists of 4 Conv-BatchNorm-ReLU-MaxPool blocks as also illustrated in Figure 2. We first train this simple CNN using our masked images for 3 classes to obtain ground truth activations and also obtain the best model which focuses only on object since there is no background to get confused with. We use Adam optimizer with a learning rate of 1e-3 for the first 40 epochs and then 1e-4 for 30 more epochs. We perform a similar experiment involving 10 classes and use 20k training and 1k test images. As shown in Table 5 for both 3 and 10 class problems, our method’s performance is better than Standard(conventional) training technique on unmasked images.

**Grad-CAM Results**

In the introduction section, we mentioned that the Grad-CAM output from the model trained on images without background yielded a more appealing output compared to the Grad-CAM output from the model trained using background. Figure 9 shows the Grad-CAM outputs for the model trained with our split training method on the infrared dataset. We see that since our method trains the model to match the activations of the primary model, the Grad-CAM/heatmaps closely match. We also observe the method’s performance on MS-COCO (RGB) data as demonstrated in Figure 8. Bottom row shows test images and top
Figure 8: Comparision of Grad-CAM heatmaps obtained using a CNN trained with our split training method and conventional methods on masked and unmasked versions of MS-COCO dataset.

Figure 9: Grad-CAM heatmaps from a CNN trained with our split training method. L: Ground truth activations(heatmap) on masked image. R: Resultant heatmap after training on unmasked image.

rows show the different heatmaps obtained at the last feature layer using different sets of input images (masked and unmasked). It is noteworthy that the attention maps produced by our method on test images with background (third row) are similar to the ideal attention maps obtained with masked images without background (top row). In contrast, the attention maps produced by conventional training techniques (second row) are observed to be less focused on the object of interest and semantically important parts of the scene.

Conclusion
We have shown that our split training method outperforms the standard(conventional) training and finetuning methods on Infrared and RGB data. When we split the training into two steps: minimize the difference between the activations of a primary model and a secondary model using MSE, and minimize the final probabilities using CE loss, our model learns to focus on the object, which is shown by the Grad-CAM outputs. For our datasets, learning to focus on the object yielded better classification performance subsequently.

Acknowledgements The authors would gratefully like to acknowledge the technical feedback of Dr.Nazanin Rahnavard (University of Central Florida) while pursuing this research.

References
Arif, M.; and Mahalanobis, A. 2021. Few Shot Learning For Infra-Red Object Recognition Using Analytically Designed Low Level Filters For Data Representation. In 2021 IEEE International Conference on Image Processing (ICIP), 1079–1083. IEEE.

Chen, Y.; Li, J.; Xiao, H.; Jin, X.; Yan, S.; and Feng, J. 2017. Dual path networks. arXiv preprint arXiv:1707.01629.

Everingham, M.; Eslami, S. A.; Van Gool, L.; Williams, C. K.; Winn, J.; and Zisserman, A. 2015. The pascal visual object classes challenge: A retrospective. International journal of computer vision, 111(1): 98–136.

Geirhos, R.; Rubisch, P.; Michaelis, C.; Bethge, M.; Wichmann, F. A.; and Brendel, W. 2018. ImageNet-trained CNNs are biased towards texture; increasing shape bias improves accuracy and robustness. arXiv preprint arXiv:1811.12231.

Huang, G.; Liu, Z.; Van Der Maaten, L.; and Weinberger, K. Q. 2017. Densely connected convolutional networks. In Proceedings of the IEEE conference on computer vision and pattern recognition, 4700–4708.

Sandler, M.; Howard, A.; Zhu, M.; Zhmoginov, A.; and Chen, L.-C. 2018. Mobilenetv2: Inverted residuals and linear bottlenecks. In Proceedings of the IEEE conference on computer vision and pattern recognition, 4510–4520.

Sehwag, V.; Oak, R.; Chiang, M.; and Mittal, P. 2020. Time for a Background Check! Uncovering the impact of Background Features on Deep Neural Networks. arXiv preprint arXiv:2006.14077.

Selvaraju, R. R.; Cogswell, M.; Das, A.; Vedantam, R.; Parikh, D.; and Batra, D. 2017. Grad-cam: Visual explanations from deep networks via gradient-based localization. In Proceedings of the IEEE international conference on computer vision, 618–626.

Simonyan, K.; and Zisserman, A. 2014. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.
Xiao, K.; Engstrom, L.; Ilyas, A.; and Madry, A. 2020. Noise or signal: The role of image backgrounds in object recognition. *arXiv preprint arXiv:2006.09994*.

Zhu, Z.; Xie, L.; and Yuille, A. L. 2016. Object recognition with and without objects. *arXiv preprint arXiv:1611.06596*. 

VP. 2020. PyCOCO. [https://github.com/virafpatrawala/COCO-Semantic-Segmentation](https://github.com/virafpatrawala/COCO-Semantic-Segmentation). Accessed: 2021.