C. Lehman, D. Temel and G. AlRegib, "On the Structures of Representation for the Robustness of Semantic Segmentation to Input Corruption," IEEE International Conference on Image Processing (ICIP), Abu Dhabi, United Arab Emirates, Oct. 2020.

https://github.com/olivesgatech/segmentation_corruption

@INPROCEEDINGS{Lehman2020,
  author={C. Lehman and D. Temel and G. AlRegib},
  booktitle={IEEE International Conference on Image Processing (ICIP)},
  title={On the Structures of Representation for the Robustness of Semantic Segmentation to Input Corruption},
  year={2020},}

©2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

alregib@gatech.edu  https://ghassanalregib.com/
charlie.k.lehman@gmail.com  https://charlielehman.github.io/
dcantemel@gmail.com  http://cantemel.com/
ON THE STRUCTURES OF REPRESENTATION FOR THE ROBUSTNESS OF SEMANTIC SEGMENTATION TO INPUT CORRUPTION

Charles Lehman, Dogancan Temel, and Ghassan AlRegib

OLIVES at the Center for Signal and Information Processing, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332-0250 USA
{charlie.k.lehman,cantemel,alregib}@gatech.edu

ABSTRACT
Semantic segmentation is a scene understanding task at the heart of safety-critical applications where robustness to corrupted inputs is essential. Implicit Background Estimation (IBE) has demonstrated to be a promising technique to improve the robustness to out-of-distribution inputs for semantic segmentation models for little to no cost. In this paper, we provide analysis comparing the structures learned as a result of optimization objectives that use Softmax, IBE, and Sigmoid in order to improve understanding their relationship to robustness. As a result of this analysis, we propose combining Sigmoid with IBE (SCrIBE) to improve robustness. Finally, we demonstrate that SCrIBE exhibits superior segmentation performance aggregated across all corruptions and severity levels with a mIOU of 42.1 compared to both IBE 40.3 and the Softmax Baseline 37.5.

Index Terms— Robustness in Machine Learning, Semantic Segmentation, Implicit Background, Sigmoid

1. INTRODUCTION

In the past two years alone, there has been explosive growth in automated applications built upon advances made in deep learning [1]. For vision systems alone, deep learning has paved the way to a host of new products and services in safety-critical applications from autonomous vehicles to medical diagnosis to surveillance [2]. Largely attributed to the increase in accessibility of open-source software and computing power [3], the barriers between lab-born innovations and market-ready products are lower than ever before. Though this results in the ability to bring deep vision systems to market quickly, it may be premature for safety-critical applications [5, 6]. For applications where the failure of the vision system can result in severe consequences—such as, damage or harm—it is necessary that they are robust. In essence, robustness ensures that a system can prevent or minimize the impact of failures. Despite being of limited use in safety-critical applications, much of the work toward robustness of deep vision is centered around image classification [17–22].

To be more relevant to real-world need, we study semantic segmentation, which is at the heart of safety-critical decision systems across a broad spectrum of applications due to simultaneously performing localization and classification. Despite the dizzying pace of advancements for semantic segmentation, contributions have largely only been toward improving task performance on increasingly challenging datasets [23–26] or reducing the resource-footprint to capability ratio [27–30]. Though still limited, there have been recent contributions to semantic segmentation for assessing and improving robustness to adversarial [31], out-of-distribution [32], and corrupted inputs [6]. Though we expand upon the techniques from [32], the most similar work to the presented work in this paper is conducted in [6]. Kamann et al. [6] provide a benchmark comparing several popular semantic segmentation models trained on CityScapes Dataset [25] and PASCAL VOC 2012 [23], then tested on corrupted versions of the same. They proposed and verified that training models on noise can improve robustness to noise, but only reported ablation benchmarks across other types of corruption from [13].

In an effort to continue bridging the gap between innovations made in robustness and semantic segmentation, we investigate the effects of corrupted images on a popular semantic segmentation model, DeeplabV3+ [33] with a Resnet50 [34] backbone. Further, we provide evidence that improved robustness is a consequence of constructing pixel-wise representations with Implicit Background Estimation (IBE) from [32] and, even more so, with our proposed method to combine with the Sigmoid Cross Entropy objective (SCrIBE). We validate our proposed method against the Baseline (Softmax Cross Entropy) and IBE (Softmax Cross Entropy with IBE) using the Imagenet-C Corruption Toolkit from [13] to corrupt the PASCAL VOC 2012 validation set [23].

2. BACKGROUND

To better illustrate why IBE and SCrIBE benefit robustness, we must first review the structural properties of representation from the context of semantic segmentation. We will first analyze Softmax and provide insight on some properties that may result in susceptibility to corrupted inputs. Then, we will discuss IBE and outline why it results in the improved robustness observed in [32]. Finally, we will...
depends on every component, exhibits a chaotic structure in the autocorrelation of $v_k$ so as associated with negative detection are neglected in optimization—more of $f$ Semantic Segmentation: Let a semantic segmentation model be, in robustness to corruption.

Semantic Segmentation: Let a semantic segmentation model be, $f(x) : \mathbb{R}^{H \times W \times 3} \rightarrow \mathbb{R}^{H \times W \times k}$ and at each pixel location the output of $f(x)$ is $v_{i,j} \in \mathbb{R}^k$, where $k$ is the number of classes. $f(x)$ learns a representation for $v_{i,j}$, which we define as $K \in \mathbb{R}^{k}$. Also defined at each pixel is a categorical label, $y_{i,j}$, as a one-hot vector. Let softmax be, $\sigma_{SM}(x)$ and sigmoid be, $\sigma(x)$.

2.1. Softmax

Consider a model trained with Softmax Cross Entropy that achieves satisfactory task performance. Beginning with the definition for the gradient of the Softmax Cross Entropy Loss for Semantic Segmentation in (1). Let $x^{(n)}$ be the scalar value of a vector indexed at $n$.

$$
\frac{\delta L}{\delta v_{i,j,n}} = \sigma_{SM}(v_{i,j})^{(n)} - y_{i,j,n}. \quad (1)
$$

During training, the updates follow the pattern of reinforcing True Positives (TP) by making that component larger and positive, reinforcing True Negatives (TN) by making those components larger and negative, and punishing False Positives (FP) and False Negatives (FN) in the opposite way. Though this behavior is desirable, Softmax heavily favors reinforcing TP and punishing FP because the updates for FN and TN depend on the relative magnitude of the components in $v_{i,j}$ where $y_{i,j,n} = 0$. One insight is that those components associated with negative detection are neglected in optimization—more so as $k$ increases. This is evident in Fig. 3, where the Baseline exhibits a chaotic structure in the autocorrelation of $v_{i,j}$ because throughout training the FN and TN components were neglected leaving them close to the responses at initialization. Another insight is that the structure of optimization depends only on the relative response in $v_{i,j}$. This structure is fully connected because detection depends on every component, $v_{i,j,n}$, as shown for the Baseline in Fig. 1.

2.2. Implicit Background Estimation

When background is a class that must be learned—as with VOC2012—a problem arises with neglecting negative detection and requiring a fully connected dependency. Background is the complement of the foreground classes. In the case of VOC2012, the model must learn to represent potentially $k - 1$ representations for background—one for each foreground class. As was demonstrated in [13] and shown in Fig. 3 by restricting detection of the background class to when all of the foreground components, $v_{FG} \in \mathbb{R}^{k-1}$ are all in the negative orthant of $\mathbb{R}^{k-1}$, the surjections of Softmax are eliminated. Also, by inspecting the gradient update for IBE formulated as

$$
\frac{\delta L}{\delta v_{i,j,n}} = \begin{cases} 
-\frac{2e^{v_{i,j,n}}}{\sum_{m=0}^{k-1} e^{v_{i,j,m}}} - 1 & n = \text{Background} \\
\sigma_{SM}(v_{i,j})^{(n)} - y_{i,j,n} & n \in \text{Foreground}
\end{cases} \quad (2)
$$

We can observe that the TN and FN components for foreground classes are reinforced when the background is updated. This is again evident in Fig. 3 where for both IBE and SCrIBE, there is orthogonality evident between component 13 and all other components. The outcome of this reinforcement will decorrelate TP detections allowing for the observed improvements in calibration and out-of-distribution detection in [23]. However, as Softmax is still in use, the structure retains fully connected dependence for the foreground, and a binary dependence between the foreground classes and the shared background class as illustrated in Fig. 1.

2.3. Sigmoid

To give some context on why Sigmoid is a poor choice for categorical classification consider the gradient update at $i,j$, which can be formulated as

$$
\frac{\delta L}{\delta v_{i,j,n}} = -y_{i,j,n}(1 - \sigma(v_{i,j,n})). \quad (3)
$$

Notice that the update penalizes only for FN. Additionally, it allows for undesirable cases where $v_{i,j}$ is a collection of large positive values—driving the $1 - \sigma(v_{i,j,n})$ term to 0—resulting in no gradient updates regardless the value of $y_{i,j,n}$. However, the key difference from Softmax, that we will utilize, is that Sigmoid "pins" component responses about 0, eliminating the relative dependence inherent with Softmax resulting in a structure of $k$ independent binary detectors.
3. SIGMOID CROSS ENTROPY WITH IMPLICIT BACKGROUND ESTIMATION

When combining IBE with a Sigmoid Cross Entropy objective the gradient update becomes

\[
\delta L \delta v_{i,j,n} = \begin{cases} 
-\frac{e^{v_{i,j,n}}}{1 + \sum_{m \in \text{Background}} e^{v_{i,j,m}}} & n = \text{Background} \\
-v_{i,j,n} (1 - \sigma(v_{i,j,n})) & n \in \text{Foreground} 
\end{cases}
\]

resulting in \(k-1\) binary dependencies with only a single manifesting at a time, which is depicted in Fig. 1. This arises from the background update enforcing the shared representation between each class and the Sigmoid operation acting on each component, \(v_{i,j,n}\), independently. Unlike the case of Sigmoid alone, training a collection of binary detectors with SCrIBE enforces an update to all foreground components when a background label is present. The consequence of these updates is that the model must learn a rich representation for background to support foreground detection. The resulting retention of dimensionality—notionally the “wiggle room”—should improves the robustness for corruptions that affect affine transformations in \(K\).

4. EXPERIMENTAL RESULTS

To validate the analysis in Section 2 and test the hypothesis in Section 2, we evaluate all three versions of a single model. We trained DeepLabV3+ with ResNet50 backbone on the unmodified VOC2012 training set augmented with the Semantic Boundaries Dataset (SBD) \[35\] to about 10k examples. Each model was trained with images randomly scaled and cropped down to \(224 \times 224\) pixels, a batch size of 30, “poly” scheduled learning rates starting at 0.01 for the backbone and 0.1 for the classifier, and weight decay of 5e-5. Note that the hardware used were \(2 \times \text{TITAN RTX with 24GB GPU memory}\) each, but similar results are possible with a smaller batch size and lower learning rate.

Inspection of Representation Structure: To verify the observations made in analysis from 2, we compare the auto-correlation matrices and the accumulated explained variance for the data. Let \(V\) be the matrix formed by every pixel response for a \(l\) number of inputs or \(V^{(l)} = v_{i,j}\). The responses shown in Fig. 3 are normalized auto-correlation computed with \(V\). Though only shown for a single class, these are consistent across all 21 classes. It is clear that IBE is structuring the response away from the chaotic response shown for Baseline. By decomposing the covariance matrix and inspecting the effective dimensionality of the learned representation, shown in Fig. 4, we can see the effect of using Sigmoid in the place of Softmax. SCrIBE has an inherently higher-dimensional representation compared to Baseline and IBE, as is evident from the slower accumulation of Explained Variance. In order to help support the notion that more “wiggle-room” results in resistance to the affine-in-\(K\) corruptions, we evaluate with a variety of corruptions.

Robustness to Corrupted Input: To test the robustness of each model, mean Intersection-over-Union (mIOU) metric was measured for the VOC 2012 validation set (1449 examples) that was corrupted using the first 15 corruptions in the ImageNet-C Corruption Toolkit at all 5 severity levels to create about 109k examples. All models were tested on the same corrupted input simultaneously to remove effects caused by the variability in generating corruptions at runtime. Additionally, the models were tested using the Multi-Scale Classification (MSC) method from \[33\] for comparison. As summarized by Fig. 5 and Table 2 and detailed in Table 1 SCrIBE is clearly supe-

Fig. 5: This plot aggregates mIOU across each corruption to show the effects of corruption severity. Severity 0 indicates uncorrupted inputs. With Multi-Scale Classification (MSC) both models have similar performance at Severity 0, but only SCrIBE continues to benefit from MSC. The Baseline actually performs worse when MSC is used for corrupted inputs.

Fig. 6: The (top) row, labeled Original, shows a comparison between Baseline and SCrIBE for the input. The proceeding rows, labeled Corrupted, shows a comparison across the first 3 severity levels for the 3 corruptions. Though severities 4 and 5 are not shown, it is clear by the results in Table 1 the predictions are generally entirely incorrect.
In this paper, we provided analytical and empirical evidence about the underlying structures of representation for semantic segmentation. We determined that the decorrelated components produced by IBE result in improved robustness. From the analysis, we hypothesised about corruptions that act as affine transformations in the representation space $K$. We then showed that the effects of affine-in-$K$ corruptions can be further reduced by retaining dimensionality of the representation through applying SCrIBE. Though these results are promising for improving the robustness of semantic segmentation models, the evidence suggests that the properties of representation structure are largely unknown and likely untapped. Namely, though the addition of IBE and SCrIBE did improve robustness to corruptions and evidence was presented to associate observable properties with the improvement, the question of direct causality is still unanswered.

5. CONCLUSION

In this paper, we provided analytical and empirical evidence about the underlying structures of representation for semantic segmentation. We determined that the decorrelated components produced by IBE result in improved robustness. From the analysis, we hypothesised about corruptions that act as affine transformations in the representation space $K$. We then showed that the effects of affine-in-$K$ corruptions can be further reduced by retaining dimensionality of the representation through applying SCrIBE. Though these results are promising for improving the robustness of semantic segmentation models, the evidence suggests that the properties of representation structure are largely unknown and likely untapped. Namely, though the addition of IBE and SCrIBE did improve robustness to corruptions and evidence was presented to associate observable properties with the improvement, the question of direct causality is still unanswered.

References

[1] “Machine learning market by service (professional services, and managed services): Global industry perspective, comprehensive analysis, and forecast, 2017-2024.” Tech. Rep., Zion Market Research, 2019.

[2] W. G. Hatcher and W. Yu, “A survey of deep learning: Platforms, applications and emerging research trends,” IEEE Access, vol. 6, pp. 24411–24432, 2018.

[3] A. Paszke et al., “Pytorch: An imperative style, high-performance deep learning library,” in Advances in Neural Information Processing Systems 32, pp. 8024–8035. Curran Associates, Inc., 2019.

[4] M. Abadi et al., “TensorFlow: Large-scale machine learning on heterogeneous systems,” 2015, Software available from tensorflow.org.

[5] N. T. S. Board, “Collison between vehicle controlled by developmental automated driving system and pedestrian,” Tech. Rep., NTSB, 2019.

[6] C. Kamann and C. Rother, “Benchmarking the Robustness of
Semantic Segmentation Models,” arXiv:1908.05005 [cs, eess], Aug. 2019.

[7] D. Hendrycks and K. Gimpel, “A baseline for detecting misclassified and out-of-distribution examples in neural networks,” Proceedings of International Conference on Learning Representations, 2017.

[8] S. Liang, Y. Li, and R. Srikant, “Enhancing the reliability of out-of-distribution image detection in neural networks,” in International Conference on Learning Representations, 2018.

[9] K. Lee, K. Lee, H. Lee, and J. Shin, “A simple unified framework for detecting out-of-distribution samples and adversarial attacks,” in Advances in Neural Information Processing Systems, 2018, pp. 7167–7177.

[10] D. Hendrycks et al., “Deep Anomaly Detection with Outlier Exposure,” arXiv preprint, 2018.

[11] C. Guo et al., “On calibration of modern neural networks,” in Proceedings of the 34th International Conference on Machine Learning-Volume 70. JMLR. org, 2017, pp. 1321–1330.

[12] K. Lee et al., “Training confidence-calibrated classifiers for detecting out-of-distribution samples,” in International Conference on Learning Representations, 2018.

[13] D. Hendrycks and T. Dietterich, “Benchmarking neural network robustness to common corruptions and perturbations,” in International Conference on Learning Representations, 2019.

[14] N. Carlini and D. Wagner, “Towards evaluating the robustness of neural networks,” in Security and Privacy (SP), 2017 IEEE Symposium On. 2017, pp. 39–57, IEEE.

[15] N. Paperot et al., “The limitations of deep learning in adversarial settings,” in 2016 IEEE European symposium on security and privacy (EuroS&P). IEEE, 2016, pp. 372–387.

[16] I. J. Goodfellow et al., “Explaining and harnessing adversarial examples,” arXiv preprint arXiv:1412.6572, 2014.

[17] D. Temel, J. Lee, and G. AlRegib, “CURE-OR: Challenging Unreal and Real Environments for Object Recognition,” in IEEE International Conference on Machine Learning and Applications (ICMLA), 2018.

[18] D. Temel, M. Chen, and G. AlRegib, “Traffic sign detection under challenging conditions: A deeper look into performance variations and spectral characteristics,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–11, 2019.

[19] R. Geirhos et al., “Generalisation in humans and deep neural networks,” p. 13.

[20] D. Temel, G. Kwon, M. Prabhushankar, and G. AlRegib, “CURE-TSR: Challenging unreal and real environments for traffic sign recognition,” in Neural Information Processing Systems (NeurIPS) Workshop on Machine Learning for Intelligent Transportation Systems, 2017.

[21] D. Temel and G. AlRegib, “Traffic signs in the wild: Highlights from the ieee video and image processing cup 2017 student competition [sp competitions],” IEEE Sig. Proc. Mag., vol. 35, no. 2, pp. 154–161, 2018.

[22] D. Temel, J. Lee, and G. AlRegib, “Object recognition under multifarious conditions: A reliability analysis and a feature similarity-based performance estimation,” in 2019 IEEE International Conference on Image Processing (ICIP), Sep. 2019, pp. 3033–3037.

[23] M. Everingham et al., “The Pascal Visual Object Classes Challenge: A Retrospective,” International Journal of Computer Vision, vol. 111, no. 1, pp. 98–136, Jan. 2015.

[24] T.-Y. Lin et al., “Microsoft COCO: Common Objects in Context,” arXiv:1405.0312 [cs], Feb. 2015.

[25] M. Cordts et al., “The cityscapes dataset for semantic urban scene understanding,” in Proc. of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.

[26] B. Zhou et al., “Scene parsing through ade20k dataset,” in Proc. CVPR, 2017.

[27] M. Siam et al., “RTSeg: Real-Time Semantic Segmentation Comparative Study,” in 2018 25th IEEE International Conference on Image Processing (ICIP), Athens, Oct. 2018, pp. 1603–1607, IEEE.

[28] S. Mehta et al., “ESPNet: Efficient Spatial Pyramid of Dilated Convolutions for Semantic Segmentation,” in Computer Vision – ECCV 2018, vol. 11214, pp. 561–580. Springer International Publishing, Cham, 2018.

[29] A. G. Howard et al., “MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications,” arXiv:1704.04861 [cs], Apr. 2017.

[30] A. Paszke et al., “ENet: A Deep Neural Network Architecture for Real-Time Semantic Segmentation,” arXiv:1606.02147 [cs], June 2016.

[31] W. Zhou et al., “Automated Evaluation of Semantic Segmentation Robustness for Autonomous Driving,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–13, 2019.

[32] C. Lehman, D. Temel, and G. AlRegib, “Implicit background estimation for semantic segmentation,” in 2019 IEEE International Conference on Image Processing (ICIP), IEEE, 2019, pp. 1935–1939.

[33] L.-C. Chen et al., “DeepLab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 40, no. 4, pp. 834–848, Apr. 2018.

[34] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 770–778.

[35] B. Hariharan, P. Arbelaez, L. Bourdev, S. Maji, and J. Malik, “Semantic contours from inverse detectors,” in International Conference on Computer Vision (ICCV), 2011.