Label Noise Types and Their Effects on Deep Learning

Görkem Algan∗†, Ilkay Ulusoy∗
∗Middle East Technical University, Electrical-Electronics Engineering
†ASELSAN
galgan@aselsan.com.tr

Abstract—The recent success of deep learning is mostly due to the availability of big datasets with clean annotations. However, gathering a cleanly annotated dataset is not always feasible due to practical challenges. As a result, label noise is a common problem in datasets, and numerous methods to train deep neural networks in the presence of noisy labels are proposed in the literature. These methods commonly use benchmark datasets with synthetic label noise on the training set. However, there are multiple types of label noise, and each of them has its own characteristic impact on learning. Since each work generates a different kind of label noise, it is problematic to test and compare those algorithms in the literature fairly. In this work, we provide a detailed analysis of the effects of different kinds of label noise on learning. Moreover, we propose a generic framework to generate feature-dependent label noise, which we show to be the most challenging case for learning. Our proposed method aims to emphasize similarities among data instances by sparsely distributing them in the feature domain. By this approach, samples that are more likely to be mislabeled are detected from their softmax probabilities, and their labels are flipped to the corresponding class. The proposed method can be applied to any clean dataset to synthesize feature-dependent noisy labels. For the case of other researchers to test their algorithms with noisy labels, we share corrupted labels for the most commonly used benchmark datasets. Our code and generated noisy synthetic labels are available online1.

Index Terms—deep learning, label noise, synthetic noise, noise robust, noise tolerant

I. INTRODUCTION

Recent advancement in deep learning has led to great improvements in computer vision systems [1]–[4]. Even though it is shown that deep networks have an impressive ability to generalize [4]–[9], these powerful models have a great tendency to memorize even complete random noise [7]–[9]. Therefore, avoiding memorization is an important challenge to be overcome in order to obtain representative neural networks and it gets even more crucial in the presence of noise [6], [10].

There are two types of noise, namely: feature noise and label noise [11]. Generally speaking, label noise is considered to be more harmful than feature noise [12].

It is known that label noise has a negative impact on the training process for broad range of applications [5], [12]–[14]. As a result, various methods are proposed in the literature to prevent performance degradation caused by noisy labels [11], [15]. However, it is problematic to test those algorithms when the dataset is noisy and there is no ground truth available. Therefore, commonly adopted methodology is to add synthetic label noise to training set of an available benchmark dataset while keeping test set clean. Since there is no generic framework to corrupt labels of the given dataset in a systematic way to mimic real-world noise, each work adds their own characteristic label noise. This results in subjective evaluation of algorithms and prevents fair comparison of the methods. Even though literature generally considers noisy labels phenomenon as one compact problem, there are multiple types of label noise [11] (uniform noise, class-dependent noise, feature-dependent noise) and each has its own characteristic affect on performance.

Negative effect of label noise depending on its type is an understudied problem. Works of [5] focuses on uniform label noise and its impact on learning solely. However, as shown on section IV uniform label noise can easily be handled by neural networks without an extra modification. Therefore, it can be misleading to draw conclusion about label noise by experimenting only with uniform label noise.

In their unpublished work [10], authors consider the case of class-dependent and class-independent noise. But, this is still and uncompleted picture, since feature dependent noise is not considered. Also, it is shown in section IV that feature-dependent noise is more harmful than class-dependent noise. To the best of our knowledge, there is no work devoted to fully investigate the negative effects of all types of label noise on deep networks. In this work, each of these label noise types are analyzed and their effects on learning process is investigated. We show that, each one has its own characteristic effect on learning and therefore should be evaluated under their own category.

Even though some benchmark datasets with noisy training set and clean test set exists [4], literature still commonly adopts the approach off corrupting labels synthetically. The main reason for this approach is the ability to generate corrupted datasets from toy datasets in purpose of quick application and testing of proposed algorithm. Yet, question of how to add synthetic noise in order to test noise robust algorithms stays to be an open question. For this purpose, most human-like noise type is feature-dependent noise, in which features of each instance effects probability of being mislabeled. For example, in cars dataset, some sport cars

1Github repository: https://github.com/spidy390/corrupting_labels_with_distillation
are more similar to classic cars than others. These specific instances have greater chance to be mislabeled by a human annotator. However, this relation among specific instances is not considered in uniform or class-dependent noise. This work proposes a feature-dependent label corruption algorithm, that is inspired by knowledge-distillation technique [16]. Our methodology aims to learn representations which would result in sparse distribution of data instances in feature domain. At the end, similarities among data samples are extracted and labels are flipped for uncertain samples. Additionally, we provide pre-generated noisy labels for commonly used datasets (MNIST [17], Fashion-MNIST [18], CIFAR10 [19], CIFAR100 [20]) in purpose of other researchers to test their label noise robust algorithms.

Our contribution to literature can be summarized as follows

- Detailed analysis of negative impacts of different types of label noise on learning.
- Label corruption algorithm that utilizes data similarities in feature domain by creating sparse representation of data.

This paper is organized as follows. In section II, different label noise types are explained. Proposed solution to generate synthetic noise is given in section III. Section IV discusses the effects of different types of label noise on learning. Finally, section V concludes the paper.

II. PRELIMINARY

This chapter presents label noise types and their implementations in literature. Label noise types can be subdivided into three main groups as follows.

- **Uniform noise:** Flipping probability of label from its true class to any other class is equally distributed. Many works in literature use synthetic uniform label noise by just flipping labels randomly for a given percentage of data instances [21]–[24].
- **Class-dependent noise:** Flipping probability of label depends on the true class of the data instance. This is mostly represented by a confusion matrix and can be designed in different ways. The easiest way is to attain inter-class transition probabilities just random [25], so that there is still class dependence since transition probabilities are given according to classes but without any correlation to class similarities. In a more structured way, noise transition matrix can be designed in a way that similar classes have a bigger probability to be flipped to each other [26]–[30]. Some works use pairwise noise, in which transition from one class can only be defined to one another class [31]–[35]. Work of [36] checks the popularity of classes and constructs transition matrix so that mislabeling happens from popular class to unpopular class or vice versa.
- **Feature-dependent noise:** The probability of mislabeling depends on features of instances. In order to generate feature-dependent noise, features of each instance should be extracted, and their similarities to other instances from different classes should be evaluated. Unlike uniform and class-dependent noise, there are much fewer implementations of synthetic feature-dependent label noise. One particular work in this field is [37], where data is clustered with the kNN algorithm, and labels are flipped randomly for clusters of data. This method provides concentrated noise in the feature space. But, this type of synthetic noise doesn’t evaluate the instance similarities and therefore different from our proposed approach. Alternatively, in case there is a surrounding text for each image in the dataset, some works create noisy labels from the interpretations of these texts [38]–[41], assuming surrounding texts are related to features of data. But this approach is restricted to datasets with surrounding user-defined texts, which is not the case for most of the time.

In this work, we focus on the closed set problem, in which all data instances are from the given class set. However, some works also investigated open set problem [42], where the dataset is polluted with instances that don’t belong to any class from the class set.

III. GENERATING SYNTHETIC NOISE

This section presents the methodologies to produce different types of synthetic label noise. Uniform noise and class-dependent noise can be represented with noise transition matrix \( N \) where \( N_{ij} \) represents the probability of flipping label from class \( i \) to \( j \). Since noise transition matrix consists of probabilities, \( \sum_j N_{ij} = 1 \). On the other hand, in feature-dependent noise, each instance has its own transition probability depending on its features. Therefore, it cannot be generated using a noise transition matrix. The following sections will describe the process of generating these types of noises. Generated noisy labels are visualized with T-SNE plots in Figure III.

A. Uniform Noise

For this type of noise, each entry in the noise transition matrix, besides diagonal ones, are equally distributed. Noise transition matrix can be defined as follows:

\[
N_{ij} = \begin{cases} 
   p & \text{if } i = j \\
   1 - p & \text{if } i \neq j \\
   \frac{M - 1}{M} & \text{if } i = j 
\end{cases}
\]

(1)

where \( M \) is the number of classes.

B. Class-dependent Noise

As mentioned earlier, there are various types of class-dependent noise. In this work, we consider structured class-dependent noise, where similar classes have a higher probability of being mislabeled with each other. In order to generate a structured confusion matrix, a deep network is trained on the training set, and its confusion matrix is calculated depending on its predictions on the test set. This confusion matrix is then used for the noise transition matrix.
C. Feature-dependent noise

Compared to the previous two label noise models, feature dependent noise is harder to implement since all samples should be vectorized in the feature domain, and similarities among samples should be calculated. The teacher network extracts features of data that it is trained on, it is prone to overfitting. Since we are especially interested in similarities among instances in feature space, it is desired that samples are sparsely distributed. On the contrary, in the case of overfitting, samples are gathered in a small region in feature space.

Therefore, in this work we used the idea of knowledge distillation [16]. In the original work, the authors used distillation to transfer knowledge from the big teacher network to a much smaller student network without decreasing the performance. The idea is mainly motivated by learning from soft labels where the similarity of each instance to each class is emphasized by temperature hyperparameter.

Class probabilities on softmax output, beyond the true class probability, are usually very low. But, compared with each other, some classes may have a much higher probability than others, and this carries important information about that data instance, which is also called as dark knowledge. By making probability distribution smoother, this relation is emphasized, as shown in Equation 2.

\[
q_i = \frac{\exp(z_i/T)}{\sum_j \exp(z_j/T)}
\]  

Instead of being trained on hard labels, the student network is trained on the weighted sum of hard labels and soft labels produced by the teacher network. So, the loss function is defined as follows.

\[
L(y_i, f(x_i)) = \alpha l(y_i, f(x_i)) + (1 - \alpha)l(q_i, f(x_i))
\]  

where \(q_i\) represents the soft labels produced by the teacher network using temperature \(T\) and \(y_i\) represents the given label.

Within the context of this work, we are not interested in compressing the network to a smaller network. However, the idea of learning by emphasizing instance similarities can be used to find instances that have similar features with other classes. For that purpose, our student network is at the same size as the teacher network. Firstly, the teacher network is trained on the dataset. Secondly, soft labels are produced from the softmax output of the teacher for a given temperature \(T\). Thirdly, the student network is trained on soft labels and hard labels with a weighting factor \(\alpha\) in the loss function. Finally, by checking softmax probabilities of instances, samples that have similar features to other classes are detected, and their labels are flipped to corresponding classes.

To see if the proposed method results in a more sparse distribution of data in feature space, we can check variance of instances belonging to classes and average over each class as follows

\[
\sigma = \frac{\sum_i var(Q_i)}{M}
\]  

where \(M\) is the number of classes and \(Q_i\) is the feature matrix of instances belonging to class \(i\). Features are extracted from the layer output before the softmax layer.

For straightforward training on the MNIST dataset, the network manages to get 99% test accuracy while having \(\sigma = 78.3\). On the other hand, the network trained with distillation achieves 95% accuracy while having \(\sigma = 563.5\). Its accuracy is comparable to the original network, but learned representations are much more sparse, which is useful to extract similarities.

IV. Experiments

We performed our experiments on different datasets under various conditions to inspect the effect of label noise under different setups. When simulating label noise, training-set and validation-set are corrupted with the same type of noise, while keeping the test set clean. With this setup, the validation set is used to measure the transferability of learned representations from noisy training set to the noisy validation set, since it means high accuracy on the validation set. On the other hand, the test set is used to evaluate the true performance of the network. The following subsections present the results of various experiments. All experiments are run on Intel i7, GTX
A. Datasets and Models

**MNIST-Fashion:** We have used CNN with two convolutional layers followed by a max-pooling layer and two fully-connected layers. There are dropout layers after the max-pooling layer and the first fully connected layer. Categorical cross-entropy is used as the loss function and stochastic gradient descent with learning rate 0.1 and momentum 0.9 as the optimizer. The learning rate is halved at every 20 epochs.

**CIFAR100:** We have used a model based on VGG16 architecture. Categorical cross-entropy is used as the loss function and stochastic gradient descent with learning rate 0.1 and momentum 0.9 as the optimizer. The learning rate is halved at every 20 epochs.

B. Noise Types

Figure IV-B shows accuracies for various noise types. In this setup training set and validation set are corrupted with the same noise while keeping the test set clean. As can be seen from the figures, both proposed feature-dependent noise and locally-concentrated noise causes most performance degradation on the test set. We observed that the network fits locally-concentrated noise slowest. This is expected behavior since it is harder to find decision boundaries due to corrupted clusters of data. Interestingly, proposed feature-dependent noise gives almost the same behavior as no noise case, in terms of convergence speed and validation accuracy. However, it results in much worse performance on the test set. Therefore, it can be concluded that, in the case of feature-dependent noise and absence of a clean test set, it is harder to evaluate whether the network is overfitting the noisy samples or not.

D. Dataset Size

We experimented with different dataset sizes in order to investigate if the number of samples affects the performance in the presence of various label noise types. 1%, 10%, 40%, 70%, and 100% of data from the dataset is taken, and the network is trained on this subset. As can be seen in Table IV-B, increasing the size of the dataset results in an increase of accuracy in all noise types besides feature-dependent noise. This is due to the correlation of noise to the real feature distribution of data. With the increasing number of data points, the negative effect of uncorrelated or less correlated noise types is diminishing, since updates caused by noisy samples are overwhelmed by gradient updates from clean samples.

E. Hyper-Parameters

We investigated the effect of dropout layer and model complexity for different noise types, as presented below.

- **Dropout:** We tried out performances of the same architectures with and without dropout layers. Increase in performances are given in Table IV-E. As can be seen, dropout boosts the performance of feature independent...
TABLE II: Train, validation and test accuracies for different noise ratios for MNIST-Fashion. High accuracies for train and validation sets are marked with green and low accuracies for test set are marked with red.

| Noise Ratio (%) | Uniform | Class Dep. | Locally Con. | Feature Dep. | Uniform | Class Dep. | Locally Con. | Feature Dep. | Uniform | Class Dep. | Locally Con. | Feature Dep. |
|-----------------|---------|------------|--------------|--------------|---------|------------|--------------|--------------|---------|------------|--------------|--------------|
| 5               | 85%     | 84%        | 84%          | 91%          | 88%     | 87%        | 87%          | 93%          | 91%     | 91%        | 90%          | 89%          |
| 15              | 75%     | 75%        | 73%          | 93%          | 77%     | 76%        | 77%          | 95%          | 88%     | 86%        | 90%          | 80%          |
| 25              | 66%     | 66%        | 65%          | 99%          | 68%     | 68%        | 69%          | 91%          | 90%     | 89%        | 85%          | 80%          |
| 35              | 57%     | 57%        | 56%          | 83%          | 58%     | 50%        | 60%          | 83%          | 78%     | 89%        | 83%          | 76%          |
| 45              | 48%     | 49%        | 48%          | 81%          | 48%     | 49%        | 54%          | 80%          | 68%     | 86%        | 70%          | 67%          |
| 55              | 29%     | 40%        | 40%          | 73%          | 39%     | 40%        | 44%          | 76%          | 77%     | 80%        | 68%          | 57%          |
| 65              | 30%     | 35%        | 37%          | 71%          | 36%     | 37%        | 40%          | 74%          | 85%     | 77%        | 50%          | 48%          |
| 75              | 21%     | 36%        | 31%          | 61%          | 22%     | 36%        | 35%          | 65%          | 81%     | 21%        | 35%          | 43%          |

TABLE III: Increase ratio in test accuracies due to usage of dropout layer for CIFAR100 dataset for different types of noises at different noise rates.

| Noise Rates (%) | Uniform | Class Dep. | Locally Con. | Feature Dep. |
|-----------------|---------|------------|--------------|--------------|
| 25              | 18%     | 21%        | 1%           | 6%           |
| 35              | 80%     | 18%        | 6%           | 2%           |
| 45              | 21%     | 30%        | 1%           | 6%           |
| 55              | 39%     | 36%        | 17%          | 5%           |

TABLE IV: Test accuracies of noise-robust algorithms on CIFAR100 dataset for different types of noisy labels for noise ratio of 35%. Normal column represents training results without additional noise-robust algorithm applied.

| Noise Type | Uniform | Normal | Forward | Bootstrap | D2L | Co-Teach. |
|------------|---------|--------|---------|-----------|-----|-----------|
| Class Dep. | 52%     | 59%    | 57%     | 59%       | 59% | 57%       |
| Locally Con.| 31%     | 35%    | 31%     | 30%       | 28% | 31%       |
| Feature Dep.| 38%     | 41%    | 39%     | 35%       | 28% | 35%       |

F. Noise-Robust Algorithms

We tested noise robust algorithms from literature on given label noise types to see their effectiveness. Used methods can be listed as below:

- **Forward Loss Correction** [26]: Proposes to use confusion matrix for loss correction. In their work, authors propose methods to estimate the true confusion matrix. However, in our case, since we already know the true confusion matrix of synthetic noise, it is directly used without approximation.
- **Bootstrap** [43]: Checks the consistency among network predictions and given labels to test its noisiness.
- **D2L** [21]: Monitors complexity of network to see if it starts to overfit noise and uses this information to regularize learning.
- **Co-Teaching** [31]: Uses two networks in pair. Each network back-propagate on instances where its pair has a small loss.

Experimental results at Table IV-F shows that each algorithm behaves differently for different label noise type. For example, forward loss and D2L gives the best performance on uniform noise while co-teaching is the best for option other types of noise. Interestingly, the D2L method gives one of the best performances at uniform noise but achieves worse than normal training for locally-concentrated and feature-dependent noises. Overall, we found that co-teaching is the most efficient method among the listed methods.

V. Conclusion

In this work, we analyzed the negative impacts of label noise on deep learning algorithms, depending on the noise type. Even though lots of works in literature are devoted to overcoming the label noise phenomenon, it is problematic that each method is tested under their own generated synthetic label noise. Therefore, we propose a generic label corruption algorithm with synthetic feature-dependent label noise. The proposed methodology uses distillation technique to create a sparse distribution of data in the learned feature domain and therefore emphasizes similarities among data samples. We investigated the negative effects of each type of label noise form a different perspective. Interestingly, it is observed that feature dependent noise shows similar behavior in the training and validation phase while resulting in much lower test accuracy. Therefore, it is much harder to evaluate the progress of the network in case of feature-dependent noise by just checking outputs on noisy training and validation sets. Moreover, it is seen that noise-robust algorithms behave differently for different types of noises. Therefore, it is important to consider the noise type while evaluating the proposed methodology. For future researches, we provided generated label noise at different ratios for common benchmark datasets: MNIST, MNIST-Fashion, CIFAR10, CIFAR100. However, the
proposed algorithm can be used to generate feature-dependent noise on any given dataset.

REFERENCES

[1] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in Advances in neural information processing systems, 2012, pp. 1097–1105.

[2] 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.

[3] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014.

[4] O. Litany and D. Freedman, “Soseleto: A unified approach to transfer learning and training with noisy labels,” arXiv preprint arXiv:1805.09622, 2018.

[5] D. Hendrycks, M. Mazeika, D. Wilson, and K. Gimpel, “Using trusted data to train deep networks on labels corrupted by severe noise,” in Advances in neural information processing systems, 2018, pp. 10456–10465.

[6] A. Krizhevsky, G. Hinton, and R. H. Zemel, “Learning multiple layers of features with large datasets,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2012, pp. 1097–1105.

[7] G. Patrini, A. Rozza, A. Krishna Menon, R. Nock, and L. Qu, “Making deep neural networks robust to label noise: A loss correction approach,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 1944–1952.

[8] Y. Li, Y. Wang, Q. Zhao, and M. Kankanhalli, “Learning to learn from noisy labeled data,” 2018.

[9] K. J. Y. and J. Wu, “Probabilistic End-to-End Noise Correction for Learning with Noisy Labels,” mar 2019.

[10] S. Sukhbaatar, J. Bruna, M. Paluri, L. Bourdev, and R. Fergus, “Training convolutional networks with noisy labels,” arXiv preprint arXiv:1406.2080, 2014.

[11] D. Hendrycks, M. Mazeika, D. Wilson, and K. Gimpel, “Using trusted data to train deep networks on labels corrupted by severe noise,” in Advances in neural information processing systems, 2018, pp. 10456–10465.

[12] B. Han, Q. Yao, X. Yu, G. Niu, M. Xu, W. Hu, I. Tsang, and M. Sugiyama, “Co-teaching: Robust training of deep neural networks with extremely noisy labels,” in Advances in Neural Information Processing Systems, 2018, pp. 8527–8537.

[13] M. Ren, W. Zeng, B. Yang, and R. Urtasun, “Learning to reweight examples for robust deep learning,” arXiv preprint arXiv:1803.09050, 2018.

[14] J. Goldberger and E. Ben-Reuven, “Training deep neural-networks using a noise adaptation layer,” 2016.

[15] B. Han, G. Niu, J. Yao, X. Yu, M. Xu, I. Tsang, and M. Sugiyama, “Pumpout: A meta approach for robustly training deep neural networks with noisy labels,” arXiv preprint arXiv:1809.11008, 2018.

[16] A. Krizhevsky, G. Hinton, and R. H. Zemel, “Learning multiple layers of features with large datasets,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2012, pp. 1097–1105.

[17] G. Algan and I. Ulusoy, “Image classification with deep learning in the presence of noisy labels: A survey,” IEEE transactions on neural networks and learning systems, vol. 25, no. 5, pp. 845–869, 2014.

[18] D. Hendrycks, M. Mazeika, D. Wilson, and K. Gimpel, “Using trusted data to train deep networks on labels corrupted by severe noise,” in Advances in neural information processing systems, 2018, pp. 10456–10465.

[19] X. Yu, P. Cao, Y. Kong, and Y. Wang, “L-dmi: A novel information-theoretic loss function for training deep nets robust to noisy labels,” in Advances in Neural Information Processing Systems, 2019, pp. 6222–6233.

[20] D. Hendrycks, M. Mazeika, D. Wilson, and K. Gimpel, “Using trusted data to train deep networks on labels corrupted by severe noise,” in Advances in neural information processing systems, 2018, pp. 10456–10465.

[21] A. Krizhevsky, G. Hinton, and R. H. Zemel, “Learning multiple layers of features with large datasets,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2012, pp. 1097–1105.

[22] X. Zhu and X. Wu, “Class noise vs. attribute noise: A quantitative study,” in Advances in neural information processing systems, 2018, pp. 10456–10465.

[23] A. Krizhevsky, G. Hinton, and R. H. Zemel, “Learning multiple layers of features with large datasets,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2012, pp. 1097–1105.

[24] A. Krizhevsky, G. Hinton, and R. H. Zemel, “Learning multiple layers of features with large datasets,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2012, pp. 1097–1105.

[25] A. Krizhevsky, G. Hinton et al., “Learning multiple layers of features from tiny images,” Citeseer, Tech. Rep., 2009.

[26] O. Litany, Y. Wang, Q. Zhao, and M. Kankanhalli, “Learning to learn from noisy labeled data,” in Proceedings of the European Conference on Computer Vision (ECCV), 2018, pp. 618–633.

[27] J. Jindal, M. Nokleby, and X. Chen, “Learning deep networks from noisy labels with dropout regularization,” in 2016 IEEE 16th International Conference on Data Mining (ICDM). IEEE, 2016, pp. 967–972.

[28] B. Yuan, J. Chen, W. Zhang, H. S. Tai, and S. McMains, “Iterative cross learning on noisy labels,” in Proceedings - 2018 IEEE Winter Conference on Applications of Computer Vision, WACV 2018, vol. 2018-Janua, 2018, pp. 757–765.