Pseudo-Representation Labeling Semi-Supervised Learning

Song-Bo Yang
Taiwan Evolutionary Intelligence Laboratory
National Taiwan University
r07921077@ntu.edu.tw

Tian-Li Yu
Taiwan Evolutionary Intelligence Laboratory
National Taiwan University
tianliyu@ntu.edu.tw

Abstract

In recent years, semi-supervised learning (SSL) has shown tremendous success in leveraging unlabeled data to improve the performance of deep learning models, which significantly reduces the demand for large amounts of labeled data. Many SSL techniques have been proposed and have shown promising performance on famous datasets such as ImageNet and CIFAR-10. However, some exiting techniques (especially data augmentation based) are not suitable for industrial applications empirically. Therefore, this work proposes the pseudo-representation labeling, a simple and flexible framework that utilizes pseudo-labeling techniques to iteratively label a small amount of unlabeled data and use them as training data. In addition, our framework is integrated with self-supervised representation learning such that the classifier gains benefits from representation learning of both labeled and unlabeled data. This framework can be implemented without being limited at the specific model structure, but a general technique to improve the existing model. Compared with the existing approaches, the pseudo-representation labeling is more intuitive and can effectively solve practical problems in the real world. Empirically, it outperforms the current state-of-the-art semi-supervised learning methods in industrial types of classification problems such as the WM-811K wafer map and the MIT-BIH Arrhythmia dataset.

Index Terms Semi-Supervised Learning, Pseudo Labeling, Self-Supervised Learning

1 Introduction

Deep neural networks have achieved outstanding results in lots of computer vision challenge, such as object detection [8], image classification [5], object segmentation [17], and so on. However, these successes mentioned above are built on large amounts of label data, which is expensive to collect. Therefore, if a certain degree of knowledge can be extracted from a considerable quantity of unlabeled data, it must bring substantial commercial value.

Semi-supervised learning (SSL) explores unlabeled data to alleviate the problem of classifier overfitting caused by limited labeled data. In recent semi-supervised learning research, it is common to use consistent regularization on large amounts of unlabeled data to constrain model predictions to mitigate input noise [1] [20]. Due to the data outlier influence, this kind of method may not generate significant benefits on some real-world classification problems, e.g., wafer defect map classification and electrocardiography classification. This work proposes a modified version of pseudo labeling [12]. In the beginning, the system trains a self-supervised model through unlabeled data to learn the representation of the data. It then combines supervised and unsupervised models and trains the classifier with both the
Figure 2. Images of the WM-811K wafer map and the MIT-BIH Arrhythmia dataset. The WM-811K wafer map has seven classes, and the MIT-BIH Arrhythmia dataset has five classes.

The remainder of this paper is organized as follows. Section 2 reviews the recent semi-supervised learning and self-supervised learning researches. Section 3 introduces the framework and the algorithm of pseudo-representation labeling. More details and experimental results are evaluated in Section 4. Finally, Section 5 summarizes the entire work.

2 Related Work

Pseudo-representation labeling is built on recent semi-supervised learning and self-supervised learning approaches. To make the overall background more clear, this section reviews the current state-of-the-art in both fields.

2.1 Semi-Supervised Learning

Semi-supervised learning is a technique leveraging unlabeled data to improve the performance of deep learning models. A common assumption is that unlabeled data comes from the same distribution as labeled data. Survey according to [1], recent semi-supervised learning approaches can be mainly divided into consistency regularization, entropy minimization, and traditional regularization. Next, this section explains these categories one by one.

2.1.1 Consistency Regularization

The main idea of consistency regularization is that, after the input to be undergone data augmentation, its class semantic should remain the same. Due to the perturbations of unlabeled data should not influence class consistency. This idea is widely utilized in many state-of-the-art semi-supervised algorithms such as UDA [20], Mixmatch [1], and EnAET [19]. However, to overcome the noise caused by augmentation and maintain the stability of the model, it is usually essential to use a relatively stable loss term for the consistency part. For example, VAT [15] adds KL divergence in the unsupervised loss term

$$L = P(y|\text{Augment}(x)) \log \frac{P(y|\text{Augment}(x))}{P(y|\text{Augment}(x))'} \quad (1)$$

and Mixmatch adds L2 norm in the unsupervised loss term.

$$L = \| P(y|\text{Augment}(x)) - P(y|\text{Augment}(x))' \|_2^2 \quad (2)$$

Different from the previous methods of adding loss term to unlabeled data, Mean Teacher [18] using two models to update the weights with exponential moving average (EMA), and force the prediction results of both models to be the same. This design is useful in overcoming the overfitting problem on a single model. In addition to loss term related methods, data augmentation is also an essential technique
for consistency regularization. Proposed in UDA [20], RandAugment [4] is a data augmentation method with two hyperparameters, which control the intensity and amount of augmentation respectively. EnAET [19] proposed an ensemble method to combine spatial and non-spatial transformations to implement augmentation.

2.1.3 Traditional Regularization

Central idea through entropy minimization believes that unlabeled data, which is located in high confidence regions, belong to nearby labels, and the decision boundary locates near low-density areas. The most classic research of them is the pseudo labeling [12]. Pseudo labeling uses the predicted label as the real label through cross-entropy

\[- P(y|x) \log P(y|x) \]  

and gradually increase the proportion of its loss during the training process. However, an essential point in this method is that if the error rate of the model at the beginning is too high, the subsequent training process only gets worse. Because our assumption is usually a tiny amount of labeled data and a lot of unlabeled data, this situation happens often. Pseudo-representation labeling borrows and improves the idea of pseudo labeling. The detailed explanation is be placed in Section 4.

2.1.2 Entropy Minimization

Traditional regularization refers to directly restricting the loss term of the model to make the prediction curve smoother, and this technique generalizes the model to avoid the overfitting caused by a small amount of data. For example, weight decay [11] is a kind of regularization widely used in machine learning models.

\[ L(\theta) = L(\theta) + \frac{1}{2} \lambda \sum_{i=1}^{n} \theta_i^2 \]  

Many new techniques have also been discussed in recent years, such as [16, 13, 14]. Traditional regularization is simple and easy to implement, and thus it becomes the most commonly used technique among the three kinds of semi-supervised methods. However, traditional regularization can not learn the information from unlabeled data, but it only needs to adjust the loss term of the model. In our thought, the quantity of information added is insufficient.

2.2 Self-Supervised Learning

Self-supervised learning is a simple but powerful technique able to extract information from unlabeled data. We can design appropriate problems for unlabeled data in many different ways according to different scenarios as long as one can define the characteristics of data. In recent years, self-supervised learning has become popular due to an excellent pre-trained model without the artificial image label is valuable. This is not only helpful for unsupervised learning but also be advantageous to semi-supervised learning.

However, designing an appropriate self-supervised problem is not an easy job because it must consider the characteristics of the training data. For example, image rotation [9] is a well-known self-supervised learning task, which rotates the image through different angles, and uses the rotation angle as the label. It can achieve good results on most types of data. However, if the semantic meaning of training data is not significantly altered after rotation (for example, the data is round), this technique does not work well. Predicting the relative position of image patches is also a self-supervised method [7], by cutting the picture into grids and randomly sampling two patches to determine the relative position of each other. This method performs much better on image detection than image classification, and once again shows that it is critical to design appropriate self-supervised tasks based on different scenarios.

Compared with image classification, relative position prediction is more reasonable on object detection. In addition, there are also methods for converting grayscale images to color [24] or predicting the transformation of images [23] to achieve image representation learning.

All of the above methods have shown that self-supervised learning can significantly improve model performance. In practice, one can fix the pre-train model weight to do the classification or just use labeled data to fine-tune the pre-train model. This paper explains how to use self-supervised learning to integrate pseudo-representation labeling in Section 3.

3 Pseudo-Representation Labeling

This section introduces the technique of pseudo-representation labeling, a flexible and straightforward framework that combines self-supervised learning and pseudo labeling techniques to an integrated architecture. Our framework applies to semi-supervised learning in image classification, and it can be mainly divided into two parts. The first part is to gradually spread from a small amount of label data to unlabeled data, and the second part is to combine the self-supervised learning technique to improve the overall performance.

3.1 Pseudo-batch labeling

In machine learning tasks, as the number of labeled data increases, the classifier accuracy is also increased due to the benefit from labeled data. On the contrary, when the noise
in the label data enlarges, the classifier accuracy decreases. We use WM-811k and MIT-BIH Arrhythmia dataset to conduct our experiment and show these two kinds of mechanisms in Figure 3. These phenomena are simple and intuitive, which are also the problem to be encountered in the real world. When pseudo labels are assigned to unlabeled data and merged with labeled data, the new labeled data contain a certain degree of incorrect labels that form the labeled data noise. The noise causes a decrease in accuracy and conflict with the benefit of increased label data. It shows that if the accuracy decline cause from data noise is greater than the benefit brought by adding unlabeled data, this problem may not be in line with our scenario. Therefore, what we need to do is to suppress the noise of the data as much as possible during the process of adding labeled data.

It was mentioned in pseudo labeling that data selected by prediction confidence is an excellent metric to minimize the prediction entropy and to reduce the input noise. Our experiments measure how different prediction confidences in the testing data affect accuracy. In Figure 4, wafer defect maps and ECG heartbeat graph are used for image classification training. The result shows that selected testing data through high prediction confidence can indeed find data with smaller noise and higher accuracy. So the question this section discuss next becomes how much unlabeled data should be added each iteration to maximize the performance of our classifier. If too much unlabeled data be added per round, the noise rises too fast, and the model performance decreases. On the other hand, if too little be added each time, it leads to inefficiency and high training cost. We show and discuss the results of adding unlabeled data at different sizes each iteration in Section 4.

Figure 3. Trend charts of data amount and data noise. We use WM-811k wafer map and MIT-BIH Arrhythmia heartbeat graph for image classification, and these experiments are implemented with data augmentation. The left figure shows the amount of data and accuracy increase at the same time. The right figure shows that noise reduces accuracy. In the process of adding data, the two kinds of mechanisms conflict with each other.

Figure 4. A graph shows the impact of confidence on the accuracy. We use WM-811k wafer map and MIT-BIH Arrhythmia dataset for image classification, and these experiments are implemented with data augmentation. The results show that the testing data selected through higher prediction confidence by this classifier indeed have higher accuracy.

Figure 5. A framework to combine self-supervised learning and semi-supervised learning. This framework can be divided into two parts. First, it trains a classifier on unlabeled data with self-supervised learning. Next, it trains labeled data with supervised learning. By fixing the parameters of these two nets and concatenating them, this framework generates a classifier to do image classification.
3.2 Representation Learning Integration

Our system integrates the information learned from unlabeled data during the training process to improve our classifier performance. To achieve this, we designed a framework that strengthens the process of label selection in combination with self-representation learning. This framework is shown in Figure 5, and it can be divided into two parts. First, it trains a classifier on unlabeled data with self-supervised learning. Next, it trains labeled data with supervised learning. By fixing the parameters of these two nets and concatenating them, this framework generates a classifier to do image classification. In our framework, the appropriate self-representation learning method is chosen according to the type of data.

The algorithm is as follows Algorithm 1. First, N times of augmentation of labeled data \( \chi \) and unlabeled data \( U_x \) are performed respectively. Then, we train a self-supervised model on unlabeled data and a supervised model on labeled data according to the image classification task. Feature embedding vectors are extracted based on these two models, and the feature embedding vectors are used to train the image classification classifier. Finally, \( \alpha \times N \) unlabeled data is selected in each class to be added to the labeled data according to the prediction confidence by this classifier.

3.3 Feature Space Data Augmentation

Mixup [22] is a milestone data augmentation technology to increase the training data amount. It is useful and easy to implement and widely used in recent semi-supervised learning algorithms. However, Mixup may not work well under specific scenarios, and the example is shown in Figure 6. Figure 6 shows a synthetic crack dataset. Class 1 and Class 2 represent the crack on the left and right, respectively, and Class 3 means both sides. If Class 1 and Class 2 are combined by Mixup, the one-hot label should not be the weighted value of these two but Class 3. This type of challenge appears on datasets for industrial applications frequently, and it is necessary to find the solution to solve this problem.

In [6], three different data augmentation methods are performed in the feature space, but the improvement is not apparent. Variational auto-encoder (VAE) [10] may be a solution to make feature space data augmentation more reasonable. By adding noise to the embedding layer to train the model, the transition between instances of different two classes is slow, and the mixed image contains the characteristics of both classes. This property makes Mixup in the feature space more applied to the industrial types of datasets. Thus, we adopt Mixup by VAE to perform data augmentation at the embedding layer instead of the input layer in the framework.

4 Experiments

In this section, we explain the relevant experimental results. Section 4.1 introduces the experiment implementation details. Section 4.2 compares the impact of noise according to different amounts of labeled data. Section 4.3 records the influence of adding unlabeled data under different batch sizes. The importance of the self-supervised part is revealed in Section 4.4. Section 4.5 implements feature space Mixup in different model layers. Finally, Section 4.6 compares the experimental results with other state-of-the-art semi-supervised learning algorithms.
4.1 Implementation Details

Datasets: In our experiment, the WM-811K wafer map and the MIT-BIH Arrhythmia dataset from Kaggle are used as our assessed benchmarks. For WM-811K, due to the uneven class quantity and image size, we randomly sample 3150 images from seven classes and resize them into 32x32. For ECG, the MIT-BIH arrhythmia dataset is a five classes classification problem, and the number of sample data is 2000. Both of the unlabeled data are randomly sampled from the initial dataset, and the rest are treated as labeled data. Apart from this, the experiments also independently sample the testing data.

Experiment details: Wide ResNet-28 [21] model is used to implement these experiments. For the hyperparameters, these experiments set the dropout rate as 0.2, the weight decay as 0.0005, and the batch size as 64 at each update. We use an initial learning rate of 0.1 and Adam as an optimizer to update the model weights. For the augmentation strategy, we apply horizontal flipping, vertical flipping, and rotation in WM-811K, and only horizontal flipping, vertical flipping in ECG. For both datasets, autoencoder is adopted to self-learned data representation.

4.2 Noise Evaluation

In the Section it is mentioned that noise is generated during the process of adding unlabeled data to the labeled data, and this phenomenon conflict with the benefit of increased label data. However, in reality, the user does not know how much noise affects their data in advance, because they only hold a small part of the data on hand. In Figure 7, these experiments take only 10% of the WM-811K data and add different levels of noise to observe the tendency of accuracy. Unexpectedly, the 10% data declining accuracy is quite similar to the declining accuracy calculated from 100% data. According to the results, the user can try to estimate how much the noise influences the accuracy by using a small amount of existing data when we do not know the distribution of unknown data.

4.3 Utilized Unlabeled Data Size

Now we investigate the impact of different sizes of labeled data added per iteration. It was mentioned earlier that noise harms the benefits of labeled data. Here we use experiments in Figure 8 to illustrate how it happened. In the experiment shown in Figure 8, 315 labeled wafer defect maps and 2835 unlabeled wafer defect maps are used to implement semi-supervised classification. This experiment has not yet added self-supervised technology, but only selects...
Three charts comparing the improvement with different added unlabeled data sizes. We used 630 labeled wafer defect maps and the rest as unlabeled data. Experiments show that adding the representation of unsupervised data during training iteration helps model performance.

Figure 10. Mixup according to different model layers to compare the training performance. In the results, compared to doing mixup in the input layer, feature space Mixup outperforms in both datasets.

The accuracy of the initial model trained with the labeled data is only 75.3%, and we add unlabeled data according to different sizes. Given symbol $\alpha$ is the ratio that controls the size, and $N$ is the labeled data amount. In each round, $\alpha \times N$ unlabeled data is selected in each class to be labeled data. When the $\alpha$ is large ($\alpha = 1$), the accuracy increases slightly when trained with some pseudo-label data, and then decreases with more pseudo-label data due to noise. When the alpha is small ($\alpha <= 0.5$), the growth of accuracy is more stable. After growing to a certain level, the accuracy still declines due to the increased noise. To summarize that small unlabeled data size can make the model grow more steadily, and we should use the validation set to select a better model before the accuracy drops.

4.4 Self-Supervised Learning Improvement

To improve this framework, in this step, self-supervised technology is joined to our framework, and the improvement is compared with different added unlabeled data sizes. We used 630 labeled wafer defect maps and the rest as unlabeled data. Besides, auto-encoder is chosen to be the self-supervised task in Figure 9. Experiments show that adding the representation of unsupervised data during training iteration helps model performance and accuracy achieve a certain degree of growth in all different added unlabeled sizes.

4.5 Mixup in Different Model Layer

In Section 3.3, we propose to adopt feature space Mixup to perform data augmentation at the embedding layer instead of the input layer. Thus, another question is which

| Method                    | Wafer (630 Label) | ECG (200 Label) |
|---------------------------|-------------------|-----------------|
| Supervised                | 19.5              | 23.2            |
| MixMatch [1]              | 18.8              | 20.4            |
| EnAET [19]                | 16.6              | 22.6            |
| Curriculum Labeling [2]   | 17.9              | 21.7            |
| Pseudo-Representation     | **15.1**          | **18.8**        |

Table 1. We use the WM-811K wafer map and the MIT-BIH Arrhythmia dataset to evaluate the error rate of the current semi-supervised state-of-the-art methods.
layer to execute on has higher performance. We perform the experiment in the input layer, convolution 1, convolution 2, convolution 3, and flatten layer, respectively, and the results are shown in Figure 10. The results show that Mixup in the input layer may not as well as a result without Mixup in these two datasets, and the best results occur in the second and third convolution layer, respectively. [22] recommends that Mixup in the input layer or the earlier convolution layer is a good choice. Based on the results of our experiments and the experiments in [22], we suggest performing Mixup in the second convolution layer as default to implement feature space Mixup.

4.6 Results Comparison

Finally, the WM-811K wafer map and the MIT-BIH Arrhythmia dataset are used to evaluate pseudo-representation labeling. Implementing semi-supervised learning with 630 labels and 200 labels respectively, we measure the error rate of the current semi-supervised state-of-the-art methods in the Table 1. The results show that the pseudo-representation labeling outperforms the exiting semi-supervised learning techniques in these two datasets.

5 Conclusion

This paper proposed pseudo-representation labeling, a flexible SSL framework that combines self-representation learning with pseudo labeling to improve the performances of the image classification models. The system also adopted Mixup to perform data augmentation at the embedding layer instead of the input layer. Empirically, pseudo-representation labeling is more intuitive and effective than existing approaches for industrial applications, such as the WM-811K wafer map and the MIT-BIH Arrhythmia dataset. As for future work, we aim to ensemble different kinds of self-supervised methods to enhance the representations. Also, we would like to investigate different augmentation methods for pseudo-representation labeling.

References

[1] D. Berthelot, N. Carlini, I. Goodfellow, N. Papernot, A. Oliver, and C. A. Raffel. Mixmatch: A holistic approach to semi-supervised learning. In Advances in Neural Information Processing Systems, pages 5050–5060, 2019.

[2] P. Cascante-Bonilla, F. Tan, Y. Qi, and V. Ordonez. Curriculum labeling: Self-paced pseudolabeling for semi-supervised learning. arXiv preprint arXiv:2001.06007, 2020.

[3] O. Chapelle, B. Scholkopf, and A. Zien. Semi-supervised learning (chapelle, o. et al., eds.; 2006)[book reviews]. IEEE Transactions on Neural Networks, 20(3):542–542, 2009.

[4] E. D. Cubuk, B. Zoph, J. Shlens, and Q. V. Le. Randaugment: Practical data augmentation with no separate search. arXiv preprint arXiv:1909.13719, 2019.

[5] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei. Imagenet: A large-scale hierarchical image database. In 2009 IEEE conference on computer vision and pattern recognition, pages 248–255. Ieee, 2009.

[6] T. DeVries and G. W. Taylor. Dataset augmentation in feature space. arXiv preprint arXiv:1702.05538, 2017.

[7] C. Doersch, A. Gupta, and A. A. Efros. Unsupervised visual representation learning by context prediction. In Proceedings of the IEEE International Conference on Computer Vision, pages 1422–1430, 2015.

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

[9] S. Gidaris, P. Singh, and N. Komodakis. Unsupervised representation learning by predicting image rotations. arXiv preprint arXiv:1803.07728, 2018.

[10] D. P. Kingma and M. Welling. Auto-encoding variational bayes. arXiv preprint arXiv:1312.6114, 2013.

[11] A. Krogh and J. A. Hertz. A simple weight decay can improve generalization. In Advances in neural information processing systems, pages 950–957, 1992.

[12] D.-H. Lee. Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks. In Workshop on challenges in representation learning, ICML, volume 3, page 2, 2013.

[13] I. Loshchilov and F. Hutter. Decoupled weight decay regularization. arXiv preprint arXiv:1711.05101, 2017.

[14] I. Loshchilov and F. Hutter. Fixing weight decay regularization in adam. 2018.

[15] T. Miyato, S.-i. Maeda, M. Koyama, and S. Ishii. Virtual adversarial training: a regularization method for supervised and semi-supervised learning. IEEE transactions on pattern analysis and machine intelligence, 41(8):1979–1993, 2018.
[16] K. Nakamura and B.-W. Hong. Adaptive weight decay for deep neural networks. *IEEE Access*, 7:118857–118865, 2019.

[17] J. Pont-Tuset, F. Perazzi, S. Caelles, P. Arbeláez, A. Sorkine-Hornung, and L. Van Gool. The 2017 davis challenge on video object segmentation. *arXiv preprint arXiv:1704.00675*, 2017.

[18] A. Tarvainen and H. Valpola. Mean teachers are better role models: Weight-averaged consistency targets improve semi-supervised deep learning results. In *Advances in neural information processing systems*, pages 1195–1204, 2017.

[19] X. Wang, D. Kihara, J. Luo, and G.-J. Qi. Enaet: Self-trained ensemble autoencoding transformations for semi-supervised learning. *arXiv preprint arXiv:1911.09265*, 2019.

[20] Q. Xie, Z. Dai, E. Hovy, M.-T. Luong, and Q. V. Le. Unsupervised data augmentation. *arXiv preprint arXiv:1904.12848*, 2019.

[21] S. Zagoruyko and N. Komodakis. Wide residual networks. *arXiv preprint arXiv:1605.07146*, 2016.

[22] H. Zhang, M. Cisse, Y. N. Dauphin, and D. Lopez-Paz. Mixup: Beyond empirical risk minimization. *arXiv preprint arXiv:1710.09412*, 2017.

[23] L. Zhang, G.-J. Qi, L. Wang, and J. Luo. Aet vs aed: Unsupervised representation learning by auto-encoding transformations rather than data. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 2547–2555, 2019.

[24] R. Zhang, P. Isola, and A. A. Efros. Colorful image colorization. In *European conference on computer vision*, pages 649–666. Springer, 2016.