OCFormer: One-Class Transformer Network for Image Classification

Prerana Mukherjee*, Chandan Kumar Roy†, Swalpa Kumar Roy‡

*School of Engineering, Jawaharlal Nehru University, Delhi, India
†Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, AP, India
‡Jalpaiguri Government Engineering College, West Bengal, India

Abstract—We propose a novel deep learning framework based on Vision Transformers (ViT) for one-class classification. The core idea is to use zero-centered Gaussian noise as a pseudo-negative class for latent space representation and then train the network using the optimal loss function. In prior works, there have been tremendous efforts to learn a good representation using varieties of loss functions, which ensures both discriminative and compact properties. The proposed one-class Vision Transformer (OCFormer) is exhaustively experimented on CIFAR-10, CIFAR-100, Fashion-MNIST and CelebA eyeglasses datasets. Our method has shown significant improvements over competing CNN based one-class classifier approaches.

Index Terms—one-class classifier, transformer networks, outlier detection

I. INTRODUCTION

The primary objective for multi-class classification is to label a given object class from a predefined set of object categories. On the contrary, one-class classification attempts to model the samples from the positive or the normal class in order to classify new samples as not belonging to the set of target class. There is complete absence of negative class (as in case of binary classification) making the classification more complex. Such classification could be highly effective in cases where there is highly imbalanced or skewed dataset i.e. there are very few examples in the minority class or in cases where no supervised algorithm can learn effectively the coherent structure of the object classes. One-class classification variants include anomaly identification, outlier or novelty detection.

Kernel density based generative methods [1], [2] are highly popular for modeling anomalous data. They assign high density to train set while low density data are identified as outliers during testing. It suffers from the curse of dimensionality issue as it may assign high density to background as well and thus density estimation is not performed accurately [3]. Discriminative methods including one-class SVM (OC-SVM) [4], one-class CNN (OC-CNN) [5] or support vector data descriptor (SVDD) [6] utilize the non-linear kernels for outlier detection. The bottleneck in both the generative and discriminative methods is that they cannot learn the high dimensional data well and have poor input data representational ability. Thus, deep learning based one-class classifier methods [5], [7]–[10] have been quite successful in learning the data representation. Although the naive learning of deep features often falls prey to “hypersphere collapse” [7]. These problems were circumvented by contrasting network architectures [7].

Attention based models like transformers [17] quite popular in natural language processing (NLP) however of late their usage in computer vision problems have also become manifold. The dominant approach is to pretrain on the large-corpus and fine-tune on the smaller dataset [18]. Inspired by transformer scaling success in NLP, Dosovitskiy et al. [19] proposed a method where they applied transformer directly to images with fewest possible modifications and were able to beat the state of the art benchmark. In this work, we propose a novel pipeline with vision transformer (ViT) based one-class classifier that maps the input image features to a latent space where they are concatenated with zero-centered Gaussian data and fed through the classifier. To the best of authors knowledge we are the first to explore ViT in one-class classification application. Exhaustive experiments on benchmark classification datasets validated that the proposed approach has superior performance over other competing one-class classifiers.

II. RELATED WORKS

Most of the anomaly detection, novelty detection tasks perform the one-class classification under the hood. The early works in this anomaly detection used a probabilistic approach to score the anomaly with low probability [20]–[22] as compared to positive class data. Statistical methods like OCSVM [4] are closely related to SVM where the classifier finds the suitable hyperplane separating the data from different classes. Since in one-class classification, data from the negative class is absent, it is assumed that the negative class is the origin of the coordinate axis and the classifier finds a hyperplane that best separates the positive class from the origin. Another statistical method similar to OCSVM that uses kernel trick is SVDD [6], which tries to find the hypersphere that encloses positive data (inliers) completely. Similar to OCSVM [4], there is another method one-class Minimax probability machine (OCMPM) [23] which attempts to maximise the distance between origin and learned hyperplane by achieving a tighter lower bound of the training data. Another method Dual Slope Minimax Probability Machine (DS-OCMPM) [24] which is an extended version of OCMPM [23], considers two hyperplanes and availability of clusters. It finds the second hyperplane by projecting the data onto it such that data projected have largest possible variance. Generalised one-class Discriminative
Subspace(GODS) \cite{25} extends the OCSVM formulation into two hyperplanes. Deep learning based methods learn the distribution using neural networks. There are discriminative methods that are inspired from OCSVM and SVDD in terms of loss functions. They use regularization techniques to make themselves more powerful. Methods like one-class CNN (OC-CNN) \cite{5} comprises of two subnetworks, one is feature extractor and another is classifier. The classifier is trained using Out-of-distribution (OOD) datasets. Feature extractor could be any CNN model and classifier could be a MLP or OCSVM. Our work is mostly inspired from OC-CNN \cite{5}. Other deep learning based approaches are generative methods \cite{29}-\cite{28} based on denoising-autoencoders, generative adversarial networks, auto-regressive models etc. Self-supervision based methods have also gained popularity in the field of one-class classification. \cite{29} learns and evaluates the deep feature representation in a self-supervised way. It first learns the self-supervised representation of one-class data and then builds a classifier on the learnt representation. Adapting Pretrained Features for Anomaly Detection (PANDA) \cite{30} introduces a method to combat catastrophic collapse(feature deteriorating) in pretrained transfer learning for one-class classification using early stopping and elastic regularization techniques. Inspired by \cite{5}, we have used a ViT instead of CNN that significantly outperforms many of the state of the art one-class classifiers by a large margin.

III. PROPOSED METHODOLOGY

We provide a detailed architecture of the proposed OCR-Former, a one-class image classification approach in Fig. \[1\]. The network architecture consists of two key modules : i) feature extractor network and ii) classifier network. The feature extractor module basically maps the input target class images into a D dimensional feature space. Following the concatenation of these projected features with zero-centered Gaussian in the feature space, the features are fed into a classifier head which is typically a fully connected (FC) neural network. Classification scores are then assigned to each image by the classifier. The classification network returns either 0 or 1, with 0 representing positive class and 1 representing negative class. This notation assignment makes sense as we are essentially trying to recognise the abnormal one.

A. Feature Extraction

In ViT \cite{19}, an image, \(X\) is first divided into a sequence of patches \(X_{\text{patches}}\) using a 2D convolution operation having same kernel size and stride which ensures extracted features are non-overlapping in nature. Additionally, a classification token (CLS), \(X_{\text{cls}}\) is appended to the patches. CLS is essential because its responsible for learning the abstract feature representation across the patches. To retain the positional information of the input patches with respect to the entire image, a positional embedding, \(X_{\text{pos}}\) is added to all the patches including the CLS to obtain the input patch tokens, \(X_{\text{tokens}}\).

\[ X_{\text{tokens}} = [X_{\text{cls}}||X_{\text{patches}}] \oplus X_{\text{pos}} \quad (1) \]

These tokens are passed through sequential transformer encoder blocks. Transformer encoders are composite of blocks containing multiheaded self-attention (MSA) with a multi layer perceptron (MLP). In MLP, two multilayer perceptrons are used having an expanding ratio \(r\) at the hidden layer, and one Gaussian Error Linear Unit (GELU) activation is appended following the first linear layer. A layer normalization (LN) step precedes every block and residual shortcuts follow every block.

\[ X_{\text{att}} = X_{\text{tokens}} \oplus \text{MSA}(\text{LN}(X_{\text{tokens}})) \]
\[ X' = X_{\text{att}} \oplus \text{MLP}(\text{LN}(X_{\text{att}})) \quad (2) \]

where \(X'\) is the output of a transformer encoder block. After multiple transformer encoder blocks, the CLS token is sufficiently enriched with contextual information which can be used for the downstream tasks.

In this paper, we utilize the pre-trained ViT \cite{19} network where 12 transformer encoder blocks are used in ViT (base) and 24 transformer encoder blocks are used in ViT (large). The embedding dimensions used are 768 and 1024 for ViT (base) and ViT (large) respectively. During the feature extraction phase, we freeze all layers except the classification head (i.e the last linear layer). The underlying assumption is that mapped features have D dimensions and are appended to the pseudo-negative data having Gaussian distribution \(N(\mu, \sigma^2, I)\), where \(\mu\) and \(\sigma^2\) correspond to the parameters of the Gaussian distribution, and \(I\) corresponds to a \(D \times D\) identity matrix. Here the distribution generates \(D\) independent \(1 - D\) Gaussian with standard deviation.

B. Classification Network

As we append the pseudo-negative data, the classifier network observes the data in twice the batch size of the initial. So, if the initial input has a batch size of \(B\), then the classifier will get the input features having size of \(2B\). An FC layer and a softmax regression layer are used together in a sequence which act as the classifier layer. The FC layer has the same dimensionality as the input feature. The output of the softmax layer is two.

C. Loss Function

To train the network, we have utilized binary cross entropy loss given as, \(L_c = -\frac{1}{2K} \sum_{j=1}^{2K} (y \log(p) + (1-y) \log(1-p))\) where \(y \in (0,1)\) and \(y = 0\) indicates the classifier input comes from the feature extractor, and \(y = 0\) denotes that the classifier input is sampled from Gaussian distribution. \(p\) denotes the softmax probability with \(y = 1\). We utilized Adam optimizer \cite{31} with standard learning rate and the weight decay is set as \(1e-4\). The batch size for the input images is set to 64. \(\mu\) is set to 0 and \(\sigma^2\) is set to 0.01. In order to stabilise the training process, we utilized instance normalization \cite{32}. We fixed the latent dimension D as 1000, as it was found to be more promising.
IV. EXPERIMENTS

A. Datasets

In congruent lines with [29], we have evaluated our proposed approach on four one-class classification benchmark datasets including CIFAR-10, CIFAR-100 [33] and Fashion-MNIST [34] and CelebA Eyeglasses [35] dataset. Here in order to detect the abnormal class, we have used a one-vs-all approach. The anomaly class was one-class from all the classes and the normal class was taken randomly from the remaining classes equal to the normal class number. Random selection of training data points slightly introduces class imbalance problem that makes this more challenging. CIFAR10 consists of 60,000 colour images with 32x32 dimensionality across 10 classes (6000 images per class). 50000 are training images and rest are used as testing images. Using leave one out approach, 10 different classes of anomaly and normal classes were constructed. For each combination, there were 5k training examples and 1k testing examples per class. CIFAR100 consists of 60,000 colour images with 32x32 dimensionality (600 images per class). 500 are used as training images and 100 testing images per class. Using leave one out approach, 20 different classes of anomaly and normal classes were constructed. Fashion-MNIST consists of 60,000 gray scale images with 28x28 dimensionality across 10 different classes, along with a set of 10000 testing images. For this dataset too, 10 different combinations of training and testing sets were considered using the same leave one out method. For each training sample there were 6k training samples and 1k testing samples for each class. CelebA eyeglasses consists of 202599 images of celebrities out of which 13193 images are of celebrities with eyeglasses that are treated as outliers. A
total of 17163 images without eyeglasses are included in the training dataset and 26386 images in the test data having equal proportion of both the outliers and the inliers data.

**B. Baseline methods**

We utilized the following baselines to compare with our model. HRN [36] that uses holistic regularization applied for one class learning. DSVDD [7] a deep learning based kernel method which learns a deep representation in order to enclose the embeddings of positively labeled data (inliers) contained within the smallest possible hypersphere. To discriminate between transformations applied to images, Golan et al. [12] trained a multi-class model. Bargman and Hoshen [15] unifies the transformation and classification based methods and extends them for a broad range of applications on non-image data. Hendrycks et al. [37] proposed a self supervised technique. Huang et al. [38] proposed a transformation based method in which a certain information from the normal image is erased based on human priors and expects an inverse-transform model to predict the missing information. HRN [36] adds an additional regularization parameter to negative log likelihood loss. PANDA [30] is a transfer-learning approach that deals with some of the drawbacks of supervised-learning methods using early stopping and elastic regularization by continual learning. MSCALD [35] utilized the catastrophic failures of other anomaly detection methods by using a new loss function that overcomes failure mode of both contrastive and center loss.

**C. Training details and hyperparameters selection**

OCFormer utilizes a pre-trained feature extractor (ViT) to learn the latent mapping of normal images. Latent features are concatenated with pseudo negative data that is zero centered gaussian noise. It uses a MLP layer as a classifier (only 1 layer in our case). It uses Base-ViT (86M parameters) as standard feature extractor but we extend it further to ViT (307M parameters). We use Adam optimizer with weight decay fixed as 1e-4. For each normal class of CIFAR10, CIFAR100 and Fashion-MNIST, we train it for over 15 epochs (where for CIFAR10 and CIFAR100, each epoch consists of 71 uniform steps and for the Fashion-MNIST, each epoch consists of 85 steps) and for the CelebA eyeglasses dataset, we train it for 10 epochs (each epoch consists of 2616 steps) with batch size of 64 as beyond 10 epochs, model starts overfitting and performance decreases significantly. We use input image size of 224×224 to match the input size of pretrained ViT. We fix the latent dimension (D) representation to 1000.

**D. Quantitative and Qualitative Results**

We report the results on four image datasets namely CIFAR-10, CIFAR-100, F-MNIST and CelebA eyeglasses. We report area under curve (AUC-ROC which is a benchmark evaluation metric for one-class classification) for each of the dataset averaged over all the classes. Each column in Table I represents the mean AUC-ROC (%) with the standard deviation (std) calculated over 5 runs. In Table II our proposed method OCFormer outperforms all the existing state-of-the-art one-class classification approaches. PANDA [30] and MSCALD [38] are competitive to our method. However when ViT-large with more parameters is used, it outperforms existing methods. This generalization of ViT can be explained as the number of parameters gets increased, the model is open to learn all the complex functions though there is a slight chance of overfitting but it can be avoided by using regularization techniques. HRN [36] performs similar to our model in case of f-MNIST but it can be avoided by using regularization techniques. OCFormer (ViT-base) is erased based on human priors and expects an inverse transform model to predict the missing information. HRN [36] performs similar to our model in case of f-MNIST but it fails when it comes to CIFAR10 and CIFAR100. Other methods like Deep-SVDD [7] performs reasonably poorly on CIFAR-10 dataset. Bargman and Hoshen [15] is quite close in performance with OCFormer on f-MNIST dataset but it is outperformed by OCFormer in CIFAR-10.

We compare our model performance with the results in Table II. The mean of each dataset is weighted by the number of classes. It can be observed that OCFormer (ViT-base and ViT-large) consistently outperforms all other methods in terms of mean AUC% in CIFAR10 and CIFAR100 using MLP and SVM as classifiers by a relative margin of 6.7%. For CelebA eyeglasses dataset OCFormer achieves best performance with other compared methods with MLP (in both ViT-base and ViT-large), SVM (in both ViT-base and ViT-large) and KDE (in ViT-base). In Fig. 4 we provide visual explanations using GradCam activations which shows that the attention is on the eyeglasses worn by people (which is the abnormal class).

**1)ABLATION STUDY AND ANALYSIS:** We analyse the behaviour and performance of one-class classification and in
The performance could be explained as the number of parameters the mean AUC comes out to be 96.58. This difference in the terms) as a feature extractor with a similar set of experiments, improves when we use pre-trained ViT-large (307M parameters) shows the mean AUC of 91.16 over all the four datasets with MLP head as classifier while the performance initially drops with the increase in MLP classifier's depth.

Latent dimension augmentation. With latent dimension as 4096, it performs poorer than latent dimension as 1000. It can be seen clearly in Fig. 3(a), the red colored line represents D as 1000 and blue line represents D as 4096. Irrespective of the batch size being used, the red colored line always outperforms the blue curve. In Fig. 3(b) D as 1000 achieves its high performance as high as 98.72% AUC-ROC on CIFAR-10 while in Fig. 3(c) D as 4096 is able to achieve its high performance AUC-ROC as 97% even on larger base feature extractor.

MLP Depth. It can be observed in Fig. 3(d) that the performance initially drops with the increase in MLP classifier's for both the feature extractors. But as we go deeper in the classifier network, model's performance starts improving.

V. CONCLUSION
In this letter, we present a simple yet powerful two stage transformer based one-class classifier. The idea of latent dimension augmentation of features for abnormal classes opens avenues for traditional classifiers such as SVM, KDE into the domain of one-class classification. The proposed model outperformed compared one-class classifier approaches conveniently. A visual representation of the class activation maps is also included to explain the proposed model’s performance.

REFERENCES
[1] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, “Lof: identifying density-based local outliers,” in Proceedings of the 2000 ACM SIGMOD international conference on Management of data, 2000, pp. 93–104.
[2] L. J. Latecki, A. Lazarevic, and D. Pokrajac, “Outlier detection with kernel density functions,” in International Workshop on Machine Learning and Data Mining in Pattern Recognition. Springer, 2007, pp. 61–75.
[3] W. Morningstar, C. Ham, A. Gallagher, B. Lakshminarayanan, A. Alemi, and J. Dillon, “Density of states estimation for out of distribution detection,” in International Conference on Artificial Intelligence and Statistics. PMLR, 2021, pp. 3232–3240.
[4] B. Schölkopf, R. C. Williamson, A. J. Smola, J. Shawe-Taylor, J. C. Platt et al., “Support vector method for novelty detection.” in NIPS, vol. 12. Citeseer, 1999, pp. 582–588.
[5] P. Oza and V. M. Patel, “One-class convolutional neural network,” IEEE Signal Processing Letters, vol. 26, no. 2, pp. 277–281, 2018.
[6] D. M. Tax and R. P. Duin, “Support vector data description,” Machine learning, vol. 54, no. 1, pp. 45–66, 2004.

[7] L. Ruff, R. Vandermeulen, N. Goernitz, L. Deecke, S. A. Siddiqui, A. Binder, E. Müller, and M. Kloft, “Deep one-class classification,” in International conference on machine learning, PMLR, 2018, pp. 4393–4402.

[8] R. Chalapathy, A. K. Menon, and S. Chawla, “Anomaly detection using one-class neural networks,” arXiv preprint arXiv:1802.06360, 2018.

[9] H. Ji, C. Hou, Y. Yang, F. Fioranelli, and Y. Lang, “A one-class classification method for human gait authentication using micro-doppler signatures,” IEEE Signal Processing Letters, vol. 28, pp. 2182–2186, 2021.

[10] Z. Lu, X. Jiang, and A. Kot, “Deep coupled resnet for low-resolution face recognition,” IEEE Signal Processing Letters, vol. 25, no. 4, pp. 526–530, 2018.

[11] D. Hendrycks, M. Mazeika, and T. Dietterich, “Deep anomaly detection with outlier exposure,” arXiv preprint arXiv:1812.04606, 2018.

[12] I. Golan and R. El-Yaniv, “Deep anomaly detection using geometric transformations,” arXiv preprint arXiv:1906.12340, 2019.

[13] I. Golan and R. El-Yaniv, “Deep anomaly detection using geometric transformations,” arXiv preprint arXiv:1805.10917, 2018.

[14] D. Hendrycks, M. Mazeika, S. Kadavath, and D. Song, “Using self-supervised learning can improve model robustness and uncertainty,” arXiv preprint arXiv:1906.12340, 2019.

[15] S. K. Roy, G. Krishna, S. R. Dubey, and B. B. Chaudhuri, “Hybridsn: Exploring 3d–2d cnn feature hierarchy for hyperspectral image classification,” IEEE Geoscience and Remote Sensing Letters, vol. 17, no. 2, pp. 277–281, 2020.

[16] L. Bergman and Y. Hoshen, “Classification-based anomaly detection for general data,” arXiv preprint arXiv:2005.02159, 2020.

[17] Y. Zhang, F. Jiang, and Z. Duan, “One-class learning towards synthetic voice spoofing detection,” IEEE Signal Processing Letters, vol. 28, pp. 937–941, 2021.

[18] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, “Attention is all you need,” in Advances in neural information processing systems, 2017, pp. 5998–6008.

[19] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “Bert: Pre-training of deep bidirectional transformers for language understanding,” arXiv preprint arXiv:1810.04805, 2018.

[20] A. Dosovitskiy, L. Beyer, A. Kolesnikov, D. Weissenborn, X. Zhai, T. Unterthiner, M. Dehghani, M. Minderer, G. Heigold, S. Gelly et al., “An image is worth 16x16 words: Transformers for image recognition at scale,” arXiv preprint arXiv:2103.10300, 2021.

[21] K. Yamashishi, J.-I. Takeuchi, G. Williams, and P. Milne, “On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms,” Data Mining and Knowledge Discovery, vol. 8, no. 3, pp. 275–300, 2004.

[22] E. Eskin, “Anomaly detection over noisy data using learned probability distributions,” 2000.

[23] H. Xu, C. Caramanis, and S. Sanghavi, “Robust pca via outlier pursuit,” arXiv preprint arXiv:1010.4237, 2010.

[24] G. R. Lanckriet, L. El Ghaoui, and M. I. Jordan, “Robust novelty detection with single-class mpm,” Advances in neural information processing systems, pp. 929–936, 2003.

[25] P. Perera and V. M. Patel, “Dual-minimax probability machines for one-class mobile active authentication,” in 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, 2018, pp. 1–8.

[26] J. Wang and A. Cherian, “Golds: Generalized one-class discriminative subspaces for anomaly detection,” in Proceedings of the IEEE/CVF International Conference on Biometrics Theory, Applications and Systems (BTAS), 2019, pp. 8201–8211.

[27] M. Z. Zaheer, J.-h. Lee, M. Astrid, and S.-I. Lee, “Old is gold: Redefining the adversarially learned one-class classifier training paradigm,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 14 183–14 193.

[28] M. Sabokrou, M. Khalooei, M. Fathy, and E. Adeli, “Adversarially learned one-class classifier for novelty detection,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 3379–3388.