Image Clustering using an Augmented Generative Adversarial Network and Information Maximization

Foivos Ntelemis, Yaochu Jin, Fellow, IEEE, Spencer A. Thomas

Abstract—Image clustering has recently attracted significant attention due to the increased availability of unlabelled datasets. The efficiency of traditional clustering algorithms heavily depends on the distance functions used and the dimensionality of the features. Therefore, performance degradation is often observed when tackling either unprocessed images or high-dimensional features extracted from processed images. To deal with these challenges, we propose a deep clustering framework consisting of a modified generative adversarial network (GAN) and an auxiliary classifier. The modification employs Sobel operations prior to the discriminator of the GAN to enhance the separability of the learned features. The discriminator is then leveraged to generate representations as the input to an auxiliary classifier. An adaptive objective function is utilised to train the auxiliary classifier for clustering the representations, aiming to increase the robustness by minimizing the divergence of multiple representations generated by the discriminator. The auxiliary classifier is implemented with a group of multiple cluster-heads, where a tolerance hyper-parameter is used to tackle imbalanced data. Our results indicate that the proposed method significantly outperforms state-of-the-art clustering methods on CIFAR-10 data. Our results indicate that the proposed method significantly outperforms state-of-the-art clustering methods on CIFAR-10 and CIFAR-100, and is competitive on the STL10 and MNIST datasets.

Index Terms—Deep neural models, generative adversarial network, mutual information maximization, unsupervised learning, virtual adversarial training.

I. INTRODUCTION

NOWADAYS an increasing amount of large-scale unlabelled visual data has been made available. However, most existing learning algorithms are either designed for supervised learning where the ground truth is known, or for unsupervised learning using distance measurements. As for supervised approaches, manual annotation is a time-consuming task and can provide a temporary solution only since the labels correspond exclusively to a specific dataset [1].

Clustering tasks have been widely studied from feature extraction [2, 3], to grouping algorithms [4–6] and distance measurements [7–10]. Regarding the grouping algorithms, a range of breakthrough approaches from different perspectives has been proposed in the literature, such as centroid [4, 5], [11], hierarchical [12, 13] and graph-based [14]. However, their effectiveness heavily depends on the dimensionality of the training data as well as the defined distance functions [9]. Therefore, the usefulness of most existing clustering approaches is limited when handling high-dimensional data [15–17]. Several studies address these concerns by means of linear data reduction [18–20], which theoretically resolves the issue of the features scale. Decomposition methods such as principal component analysis (PCA) [21] and non-negative matrix factorization (NMF) [22] are restrictive when handling complex data types such as images, since the semantic information can be located in any position of the image and often a priori texture analysis is required [23, 24]. One may face similar challenges when using distance functions, since it is difficult to define such a measure [16, 17].

Recent studies address dimensionality reduction and semantic issues with the help of deep learning techniques that replace the traditional data reduction and feature extraction methods [25–28]. These studies demonstrate that neural network models are powerful tools for learning representations and extracting features. Despite their success and significant advantages, the clustering process is frequently applied using traditional algorithms, which often leads to degenerate solutions or leaves no space for further improvement [26]. Few studies propose comprehensive solutions [16, 25, 29], based on a deep convolutional architecture, which, however, often are either applicable to well-known benchmark datasets only, or computationally very intensive. Recently, generative adversarial networks (GANs) have attracted significant attention [32–34] in representation learning in an unsupervised manner, either for generating synthetic samples or for distinguishing between the training set and fake samples.

In order to deal with these challenges, this work introduces a deep learning method composed of two separate training phases. At the first phase, a modified generative adversarial network (GAN) [32] is trained to learn the representation of the dataset in a self-supervised learning manner. The Sobel filters are introduced prior to the discriminator of the GAN proposed in [33], which aims to enhance the capacity of the discriminator in learning image representation and extracting meaningful features. Afterwards, the generator part is discarded and the discriminator implements a feature extraction pipeline as an input into an auxiliary classifier. At the second phase, the auxiliary classifier consists of an additional neural net, which is trained separately from the GAN according to a modified clustering objective originally introduced for information maximizing self-augmented training (IMSAT) [35]. We extend the loss function in the original IMSAT, which utilizes a single cluster-head, by adopting a set of multiple cluster-heads, each being trained independently. We therefore
parameterize the initial function to deal with the combined cluster-heads, allowing a higher degree of flexibility leading to an improvement in clustering accuracy as demonstrated by the experimental results. Furthermore, we introduce a penalty term to minimize the divergence across invariant generated representations derived by the GAN framework.

The main contributions of this work are summarized below.

- A comprehensive deep learning framework is proposed for solving binary pairwise clustering problems for image data without relying on domain-specific augmentation operations.
- The Sobel filter is introduced into the discriminator of the GAN framework to enhance the ability of the discriminator for learning disentangled representations.
- An extended auxiliary classifier is proposed, which is optimized via a modified loss function by adding a penalty term measuring the divergence across invariant representation derived by the discriminator.

The rest of the paper is organized in four main sections. Related work including a brief literature review is presented in Section II. The proposed end-to-end deep clustering method is detailed in Section III. Section IV describes the experimental results and comparisons across a range of competitive methods. Conclusion and future work are given in Section V.

II. RELATED WORK

Data clustering has attracted much research effort over the last decades [5], [6], [16], [25], [29]–[31], [35]–[37]. In general, traditional clustering methods are divided into two main categories: 1) Generative methods, such as Gaussian mixture models [37], learn the class-conditional probability of each class individually, and the prediction process is formulated with the direct application of Bayes’ Theorem, where the prior and posterior probabilities are derived [38]. On the other hand, the discriminative models explicitly learn posterior probabilities by defining hyperplanes and decision boundaries in the training samples [39].

Over the last decade, a large body of research on deep learning based image clustering methods has been reported [16], [25], [29]–[31], [35], [36]. Early studies proposed the combination of a deep autoencoder with k-means in order to eliminate the linearity [29], [39]. Xie et al. [29] presented a comprehensive solution named deep embedding clustering (DEC), where an autoencoder projects the training samples into a lower domain space via a bottleneck layer. Regardless of the functionality of the neural networks, the clusters’ centroids are initialized with the help of k-means and a loss function depending on the distance measurement. However, DEC performance is limited to image data, since it requires the utilization of histogram oriented gradients (HOG) [40] for relevant feature extraction. Inspired by the agglomerative methods, joint unsupervised learning (JULE) [25] was proposed to tackle image clustering from a different perspective, since distance functions are difficult to define. Despite its success, the applicability of JULE is restricted due to the recurrent framework which requires high computational cost and memory sources [30]. In deep subspace clustering networks (DSC-Nets), an autoencoder architecture is leveraged to express a lower domain subspace. The clustering phase is achieved through a self-expressing matrix, which is of a dimension of \( \mathbb{R}^{n \times n} \), where \( n \) denotes the size of training set. Although the idea is very interesting, its applicability to large datasets is limited due to memory restrictions.

More recently, mutual information theory was introduced into deep learning based clustering methods [31], [35], [41]. Gomes et al. [42] initially presented regularized information maximization (RIM), a discriminative approach where a conditional entropy term is used to maximize the confidence in clustering assignment of each element to the relevant class. The second term of marginal entropy naturally regularizes the model to evenly assign the training samples in relevant clusters. In addition to the entropy terms, an extra regularization term is proposed [42] to enhance the parametric model’s ability to identify sensible decision boundaries within the given set.

An application of RIM to a deep method was proposed by Hu et al. [35], which introduced IMSAT, with the direct application of two entropy terms as a loss function. In IMSAT, the additional penalty term is replaced by an alternative self-regularization method proposed for virtual adversarial training (VAT) by Miyato et al. [43]. The combination of RIM and VAT in a multilayer perceptron net produces impressive clustering capability on the MNIST dataset [35]. Note that in IMSAT, a prior feature extraction is required by an external pre-trained model when dealing with multi-dimensional images (RGB) or an affine transformation together with VAT. Affine transformation is a stochastic process, therefore its performance heavily depends on the augmented function and their hyper-parameters, such as the translation range, the degree of rotations, and the scales of color jittering.

Studies that exclusively apply image transformation/augmentation techniques to clustering have also been reported in [26], [31], [44]. In invariant information clustering (IIC) [31], mutual information is explicitly maximized with respect to the original data and several augmented transformed versions. A set of cluster heads and a set of over-cluster heads are developed to improve the robustness in assigning the corresponding cluster index. Deep InfoMax (DIM) [41] is essentially an implicit measure of mutual information, maximizing the lower bound between a group of spatial representations and a global representation. Despite the encouraging results, DIM requires to compute multiple complex estimations.

In contrast to [41], the measurement of mutual information’s lower bound, particular in Donsker-Varadhan [45], may have statistical limitations, as pointed out by McAllester and Statos [46]. Here, we employ a GAN framework, originally designed for learning the data distribution for feature extraction. Furthermore, during the clustering process, we extend the functionality of IMSAT to cluster the learned features without the implementation of an external model. Inspired by [31], we adopt a large number of probabilistic outputs and over-cluster heads, which is combined with a tolerance hyper-parameter in the proposed methodology to allow for flexibility on imbalanced datasets and to achieve better clustering accuracy. Details of the implementation are provided in Section III.
defined as \( D \) with respect to the model’s parameters \( \theta \). The output conditioned on parameters \( \theta \) is available in all points with its input being a prior noise \( z \).

Images. Our clustering process consists of two learning stages:

A. Learning Deep Representation

In the following, we detail these training phases.

\( \text{METHOD} \)

III. M

In this section, we outline the general framework of the proposed deep framework for image clustering, as illustrated in Fig. 1. Initially, we make an assumption that for each given element in the unlabeled dataset \( x \in X \), a binary pairwise relation holds to a discrete finite set such as \( X \rightarrow Y \). In this case, \( y \in \{1, 2, \ldots, k\} \) and \( k \) is a predefined hyper-parameter which indicates the number of classes in the set of \( X \).

The goal of our approach is to define a parametric model that satisfies the described relation \( f_\theta : X \rightarrow Y \). In this work we assume that \( X \) is a dataset comprised of multi-dimensional images. Our clustering process consists of two learning stages:

- **Learning deep representation**: A convolutional GAN [32] is implemented to learn the distribution of the data to be clustered. This way, bottleneck feature extraction is achieved by leveraging the last layer of the discriminator model.

- **An Auxiliary Classifier**: An auxiliary classifier network is introduced at the output of the discriminator. The parameters of this additional network are optimised by applying IMSAT [35], a combination of the loss function of RIM [42], with an extra penalty term for virtual adversarial training [43].

In the following, we detail these training phases.

A. Learning Deep Representation

The GAN framework [32] was proposed as a straightforward technique for training deep generative models. The architecture consists of two main components: 1) a generator denoted as \( G(z; \theta_g) \), where \( G \) is a multi-layer model, differentiable in all points with its input being a prior noise \( z \) and an output conditioned on parameters \( \theta_g \); and 2) a discriminator defined as \( D(x; \theta_d) \), where \( x \) denotes an input tensor with respect to the model’s parameters \( \theta_d \). Both models are optimised simultaneously with back-propagation via a minmax game, with the intention of approximating the parametric density \( p_g(x) \) to the real distribution \( p_r(x) \). The discriminator aims to distinguish the source of the input element by assigning the relevant probability. More formally, the minmax training function \( V(D, G) \) of an adversarial model can be expressed as follows [32]:

\[
\min_G \max_D V(D, G) = E_{x \sim p_{\text{data}}(x)} \left[ \log(D(x)) \right] + E_{z \sim p_z(z)} \left[ \log(1 - D(G(z))) \right] \tag{1}
\]

Several studies have introduced alternative methods for training GANs [37]–[50]. Differing from the methodologies presented in these studies which mainly consider the quality of the generated sample, this work focuses on learning the distribution of training samples via a self-training process. The discriminator model is transformed into a feature extraction pipeline for clustering. Hence, the training strategy is not chosen with respect to the quality of generated samples; instead, it concentrates on the performance of the discriminator. For this reason, we adopt the deep convolutional generative adversarial network (DCGAN) [33], whose discriminator has been demonstrated to have a strong capability of extracting relevant features in imaging data [33], [51]. Additionally, in [52], the discriminator is utilised by extracting features from each convolution layer, and a similar approach is adopted in [53] for hyper-spectral image dataset.

Compared to the original structure of DCGAN, the discriminator of the GAN proposed in this work is forced to capture information such as saturation and colours by applying convolutional operations to the original image. Here, we apply the Sobel operators prior to the discriminator, which encourages the discriminator to capture as much detail as possible in terms of edges and shapes [26], [31], [54]. The Sobel operator begins by applying a simple pointwise convolutional layer which converts the red green blue (RGB) input into grayscale. This is followed by a depthwise convolutional layer with predefined Sobel constant weights in both directions (\( dx, dy \)). The produced edges are concatenated with the original RGB sample and inputted to the discriminator model, as shown in Fig. 2. Since in both parts all layers are fully differentiable, the generator model can also be optimised in a similar way to back-propagation. This is also found to boost the already competitive learning performance of GANs.

The new domain space of the extracted features is flattened and defined as \( M \) hereafter. To avoid extremely large values in the generated domain \( M \), a \( L_1 \) regularization is added to the loss function in Equation (1) when training the flattened layer prior to the activation function of the discriminator. The regularization term is defined as \( L_1(M) = \sum \max(|M| - 20, 0) \) to penalize the output of the flatten layer if its value is outside [-20, 20].

B. Auxiliary Classifier

Further to the above architecture, we train an auxiliary classifier network to cluster the features extracted by the
trained discriminator. Our clustering strategy is based on IMSAT [35] which implements RIM [42].

Before explaining the training process, we briefly describe the mutual information and its application in RIM. Mutual information is defined by

$$I(X;Y) = H(Y) - H(Y|X),$$

which encourages the increased discrepancy between the two entropy terms for different perspectives. According to the conditional entropy $H(Y|X)$, the model is driven to reduce the uncertainty by assigning the corresponding class index with higher confidence. This is achieved by minimizing the conditional entropy. On the other hand, the aim of maximizing the marginal entropy $H(Y)$ is to evenly distribute the model’s class assignment. This avoids degenerate solutions, which are often observed in clustering tasks. According to information theory [55], the marginal entropy follows an upper bound $H(Y) \leq \log(k)$. Therefore, instead of maximizing the marginal entropy, this can be transformed into minimization, where the following expressions are applicable [35]:

$$D_{KL}(p(y)||u) = \sum p(y) \log \frac{p(y)}{u(y)} = \log(k) - H(Y)$$

which $D_{KL}$ denotes the Kullback–Leibler divergence function, and $u$ is a uniformly distributed prior. Here, we combine the conditional entropy and Equation (4). Consequently, we aim to minimize the following term as the RIM part of the objective function [35].

$$I_\psi(M,Y) = \max[[D_{KL}(p_\psi(y)||u(y)) - \delta], 0] + H_\psi(Y|M)$$

where $\delta \geq 0$ denotes an introduced tolerance factor which encourages the model’s cluster distribution $p_\psi(y)$ to approximate the uniform prior within a defined tolerance level, and $\psi \in R$ is the auxiliary classifier parameters. The application of $\delta$-tolerance increases the model’s capability of avoiding degenerate solutions, without which the model will be forced to balance the training samples, resulting in the assignment of trivial solutions in the case of imbalanced data. We found that by introducing a tolerance factor in optimizing the model’s parameters using the gradient descent, we are able to enhance the accuracy of the model, as indicated by our experimental results presented in Subsection IV-V.

In the following, we elaborate the loss function to be used for training the auxiliary classifier. Here, we borrow and extend the idea of self-augmented training (SAT) initially introduced in IMSAT [35]. The regularized term in IMSAT is described as [35]:

$$R_{SAT}(\psi; T) = \frac{1}{N} \sum_{n=1}^{N} R_{SAT}(\psi; m_n, T(m_n))$$

where $T(m) = m + r$ denotes a transformed function with input $m$ and a perturbation $r$. The regularized function is defined using Kullback–Leibler (KL) divergence, and theoretically the model’s predictions will be invariant to data transformation. In this work, we make use of the virtual adversarial training (VAT) [43] methodology as adopted in IMSAT as an implementation of $R_{SAT}:$

$$L_{adv}(x, \psi) = D_{KL}(p(y|m, \psi), p(y|m + r_{adv}, \psi))$$

where $r_{adv} := \text{argmax}_{r: ||r||^2 \leq \epsilon} \{D_{KL}(p_\psi(y|m), p_\psi(y|m + r))\}$

where $r$ denotes random perturbations and $r_{adv}$ the adversarial perturbations. Similar to [43], we approximate $r_{adv}$ based on the $L_2$ norm, i.e., $r_{adv} \approx \epsilon \frac{g}{||g||^2}$, where $g$ denotes the computed gradient with respect to the relevant point. We adapt $\epsilon$ for both rounds of the VAT process to be proportional to the norm of each generated representation as $\epsilon_i = \alpha \cdot ||m_i||^2$, where $\alpha$ is a constant scalar and $i$ is the index of the corresponding feature. We denote the constant scalar as $\alpha_r$ in the first round.

Fig. 2: An illustration of the modified discriminator of the GAN framework in which two convolutional layers operate in front of the discriminator input. Initially, the three image layers (RGB) are converted into a gray-scale version via the application of pointwise layer. Afterwards a depthwise convolutional with a constant kernel implements the two directions of the Sobel’s operations. The generated domain is concatenated with the original input and forwarded to the discriminator model.
of random perturbation, and $\alpha_{adv}$ for the second round of adversarial perturbation.

The process was adapted from the clustering strategy in IMSAT implementing regularized information maximization [42] and VAT [43]. In this work, we aim to further enhance the robustness of the proposed method, which is achieved by minimizing the KL divergence of the classifier’s prediction for various representations of the same original attribute $X$. Additional representations are obtained by adopting dropout when training the discriminator. This way, we are able to include an additional term in the loss function for training the auxiliary classifier, which is defined as follows:

$$L_d(\psi, m, m') = D_{KL}(p_\psi(y|m), p_\psi(y|m'))$$  \hspace{1cm} (8)

where $m$ is the extracted features without using dropout, and $m'$ denotes those generated by the discriminator with a low dropout rate. In this work, $y$ is a probabilistic output of the softmax distribution function. In addition, we make use of multiple cluster heads (softmax layers) that are described as follows:

$$L(\psi; m) = \frac{1}{C} \sum_{j=1}^{C} \sum_{n=1}^{N} \sum_{i=1}^{1} 2R_{SAT}(\psi; m_n, T(m_n))$$

$$+ \frac{1}{2} \sum_{i=1}^{1} L_d(\psi, m, m') + \lambda I_\psi(M, Y)$$  \hspace{1cm} (9)

where $C$ indicates the implemented number of cluster heads, $\lambda$ is a weight parameter, and $M$ is the new domain space produced by the discriminator. Instead of using a single cluster head, this work adopts multiple cluster heads together with the introduced tolerance factor, which is found to be able to significantly enhance the model’s performance and robustness, in particular, when the tolerance factor $\delta$ is set to be small. This can be attributed to the fact that with the help of multiple cluster heads, the probabilistic outputs are simultaneously optimised with a variety of random parameters. In addition, we also included a few overcluster heads, whose outputs are larger than the predefined number $k$, in order to capture more details such as variations or sub-classes, within similar classes. Note that in this work, we assume $k$ is a hyper-parameter to be defined prior to the model training.

By modifying the loss function and introducing multiple cluster heads, we are able to enhance the efficiency of the auxiliary classifier for clustering using the features generated by the discriminator, which is confirmed by our experimental results. In the case of a high $k$ value, $\delta$-tolerance is initialised with a larger value, since we assume that training samples within sub-classes are not evenly distributed. The effects of the parameter setting of $\delta$ and the use of multiple cluster heads on the performance of the classifier are presented in Tables [V] and [V]

Algorithm 1 describes in detail the overall training process comprised of two consecutive learning phases. Note that neither stage in the proposed framework requires any labels for the data.

### IV. EXPERIMENTS

In this section we evaluate the proposed clustering method on a range of datasets and compare it to several state-of-the-art methods. We demonstrate that our method is capable of handling imbalanced datasets and classification tasks. Additionally we evaluate our method under different parameter settings and configurations, including the use of single or multiple cluster heads.

**A. Datasets**

We evaluate our algorithm on four popular benchmark image datasets, MNIST, CIFAR-10, CIFAR-100-20 and STL (a smaller subset of ImageNet). All relevant details in terms of the training samples, number of clusters and image resolution are presented in Table [I].

| Dataset       | Training Samples | No. Clusters | Resolution   |
|---------------|------------------|--------------|--------------|
| MNIST         | 70000            | 10           | 28x28x1      |
| CIFAR-10      | 60000            | 10           | 32x32x3      |
| CIFAR-100/20  | 60000            | 20           | 32x32x3      |
| STL10*        | 113000           | 10           | 96x96x3      |

*STL10 is evaluated only for the labelled subset of 13000 images.

In order to reduce the model’s parameters, and consequently the duration of training phases, the following re-scales or crops...
have been applied. 1) MNIST training samples are center cropped to the dimensions of 24x24x1, 2) STL10 images are resized to 48x48x3, without additional transformation functions being applied. Furthermore, STL10 is evaluated only for the labelled subset whereas the model is trained across the complete dataset. For the CIFAR-10/20 dataset, we evaluated our proposed model based on 20 super-classes also called 'coarse' across all experiments.

B. Evaluation Metric

In order to evaluate the performance of the proposed framework, we use a traditional metric function for clustering, namely absolute accuracy (ACC), which is expressed as follows:

\[
ACC = \max_{m \in M} \frac{\sum_{i=1}^{N} \mathbb{1}[l_i = m(c_i)]}{N} \quad (10)
\]

where \( N \) denotes the number of testing samples, \( l \) is the ground truth, \( c \) is the model’s assigned cluster, and \( M \) is the set of all available one-to-one mappings. Upon the completion of the above metric, the accuracy is computed with the best matching between the cluster assignment and the given ground truth. This can be efficiently computed using the Hungarian algorithm [56].

C. Implementation Details

All experiments were based on an implementation of the DCGAN with a convolutional architecture. Here, we replace the ReLU [57] activation of the generator with the Leaky ReLU [58], where the parameter of the Leaky ReLU activation function is set to 0.2 for both nets. As designed in DCGAN, every convolutional operation is followed by a batch normalization layer in both nets of the framework. Additionally, similar to [32], we found it beneficial to use dropout [59] to stabilize the training in the discriminator. The dropout rate is set to 20\% across all implementations. The last convolutional layer of the original discriminator in DCGAN is flattened and directly forwarded to the discriminator’s probabilistic output. In our approach, an intermediate fully connected layer is employed between the last convolutional operation and the output layer of the discriminator to reduce the dimensionality of vector \( M \). Further details regarding the discriminator structure are presented in Table II while the model’s parameters for the corresponding structure are included in Table III.

The auxiliary classifier is based on a fully connected architecture. For the experimental results presented in Table IV the auxiliary net consists of two hidden layers, and a ReLU activation is applied. The probabilistic outputs are determined via the softmax function. We implement five cluster heads in total in the experiments, and one over cluster head (i.e., with a larger \( k \)). Weight regularization is not implemented in this net. Inspired by [31], we generate a number of replications of the adversarial transformed features within each mini-batch in order to learn invariant representations of the data. We found that a higher number of replications leads to a faster convergence of the classifier model and increases the clustering performance. In our experiments, the input data is replicated five times with alternative transformations and all six instances are propagated to the model in a single batch. The code is implemented in python using Tensorflow and can be made available upon request.

D. Experimental Settings

In this subsection, we discuss the settings for the hyper-parameters to be used in the experiments. We followed the recommendations in [33] regarding weights initialization, the optimizer, and the mini-batch size in training the DCGAN. Specifically, the model parameters of the GAN are initialized with a Gaussian distribution of a standard deviation of 0.02. Both the generator and discriminator are trained by Adam [60] with a learning rate of \( 10^{-4} \) and \( \beta_1 = 0.5 \). Both the generator and discriminator are trained for a total of \( 10^5 \) iterations.

For the clustering process, we set the weight parameter \( \lambda \) in Equation (9) to 0.2 across all experiments. The tolerance factor \( \delta \) is defined to be \( 10^{-4} \cdot \log(k) \), where \( k \) is equal to the predefined number of clusters. The value of \( \delta \) is chosen considering the imbalanced distribution within mini-batches. In the experiments, one overcluster head is used, for which we set \( \delta = 10^{-2} \cdot \log(k') \), where \( k' \) is set to be larger than the predefined number of clusters, since we expected that the sub-clusters are not evenly distributed.

For computing the adversarial transformation \( m + r_{adv} \), we set \( \alpha_r \) of the first round of random perturbation to 0.3 for CIFAR-10/100, and STL, and to 1.0 for MNIST, respectively. In the second round of VAT process, \( \alpha_{adv} \) is set to 0.15 for CIFAR-10/100 and STL, while it is set to 0.2 for MNIST.

| Dataset | Discriminator | Generator |
|---------|---------------|-----------|
| MNIST   | 167K          | 289K      |
| CIFAR10-100 | 4.85M  | 4.40M |
| STL10* | 10.10M         | 11.99M    |

\( K \) denotes thousands, and \( M \) millions respectively.
for the training process with a learning rate of \(10\) initialized based on a Gaussian distribution with a standard deviation \(10\). Similar to the GAN, the Adam optimizer is selected that is pre-trained using supervised learning on Imagenet. The weight parameters of the auxiliary are auxiliary classifier is fine tuned with a mini-batch size of 500. Since the proposed strategy can be extended to non-image data. This leads to a notable advantage in bold font. From the results presented in Table IV, we can find that our approach exhibits competitive clustering performance compared to the state-of-the-art techniques. On some benchmark datasets, the proposed method outperforms all other methods under comparison. In particular, the proposed algorithm (average performance) reaches a margin of 7.5% improvement on CIFAR-10 and 5% on CIFAR-100 in comparison with the state-of-the-art. Recall that the proposed method does not perform any direct image augmentation to the original data; instead, it relies on transformations that are not specific to image data. This leads to a notable advantage since the proposed strategy can be extended to non-image data. It should be pointed out that although VAE and IMSAT outperform all other algorithms under comparison on the STL10 dataset, they both use features extracted by a model that is pre-trained using supervised learning on Imagenet.

Figure 3 illustrates the results of the proposed algorithm (indicated by the relevant probabilities predicted by the model) for CIFAR-10 and MNIST experiments. As can be observed, on the MNIST dataset (lower panel), our model successfully assigned the right label on the majority of the corresponding images, although one inaccurate prediction is made for class ‘two’ (third column), where an element from class ‘one’ with some common spatial lines were picked. By looking at the results on the CIFAR-10 dataset (upper panel), we find that our model is able to distinguish the classes surprisingly well with few cases of inaccurate predictions. We see that clusters with common patterns, i.e., ‘Automobile’ with ‘Truck’ and ‘Horse’ with ‘Deer’ are successfully clustered. The lowest performance can be seen on class ‘Cat’ which represents an uncertainty in bold font. From the results presented in Table IV, we can find that our approach exhibits competitive clustering performance compared to the state-of-the-art techniques. On some benchmark datasets, the proposed method outperforms all other methods under comparison. In particular, the proposed algorithm (average performance) reaches a margin of 7.5% improvement on CIFAR-10 and 5% on CIFAR-100 in comparison with the state-of-the-art. Recall that the proposed method does not perform any direct image augmentation to the original data; instead, it relies on transformations that are not specific to image data. This leads to a notable advantage since the proposed strategy can be extended to non-image data. It should be pointed out that although VAE and IMSAT outperform all other algorithms under comparison on the STL10 dataset, they both use features extracted by a model that is pre-trained using supervised learning on Imagenet.

### Table IV: Comparative results on benchmark clustering problems.

| Method          | MNIST    | CIFAR-10 | CIFAR-100-20 | STL10  |
|-----------------|----------|----------|--------------|--------|
| AE [61] †       | 81.23%   | 31.35%   | 16.45%       | 30.3%  |
| VAR [62] †      | 83.17%   | 29.08%   | 15.17%       | 28.15% |
| DEC [33] †      | 84.30%   | 30.10%   | 18.50%       | 35.90% |
| DCGAN ours ‡    | 82.80%   | 31.50%   | 15.10%       | 29.80% |
| DCGAN ours ‡ ±  | 88.40%   | 52.36%   | 28.04%       | 43.91% |
| JULE [25]       | 96.40%   | 27.15%   | 13.67%       | 27.69% |
| DAC [16]        | 97.75%   | 52.18%   | 23.75%       | 46.99% |
| VAE [56]        | 95.00%   | 52.36%   | 23.75%       | 46.99% |
| IMSAT [30]      | 98.40%   | 45.60%   | 27.50%       | 94.10% |
| ADC [30]        | 99.20%   | 32.50%   | 18.90%       | 53.00% |
| IIC [31]        | 99.20%   | 61.70%   | 25.70        | 59.60% |
| OURS (best)     | 99.02%   | 70.04%   | 32.44%       | 58.65% |
| OURS (avg)      | 98.85% (±0.14%) | 69.22% (±0.83%) | 30.88% (±1.11%) | 55.87% (±1.81%) |

† Methods perform feature extraction followed by K-means clustering.
‡ Combination of a deep method and K-means.
± A pre-processing application of HOG is used.
* Feature extraction is performed through a neural network model trained on Imagenet.
§ Results obtained from table by [31].

We set the dropout rate \(m'\) in Equation (8) to 10%. The auxiliary classifier is fine tuned with a mini-batch size of 500 training samples. The weight parameters of the auxiliary are initialized based on a Gaussian distribution with a standard deviation \(10^{-3}\) for CIFAR-10/100, and \(10^{-2}\) for STL and MNIST. Similar to the GAN, the Adam optimizer is selected for the training process with a learning rate of \(10^{-4}\). The auxiliary classifier is trained for \(10^3\) epochs in total in each experiment.

### E. Clustering Results

In Table IV, we demonstrate the performance of the proposed method by comparing it with state-of-the-art methods. We report the accuracy scores of the best performed experiment of our method and the average performance with the corresponding standard deviation of five independent runs. Note that the reported predictions were made by the best performing cluster head having the lowest loss. All evaluations were made over the complete dataset except for STL10, which is evaluated only for the labelled subset. For convenience, the top three methods for each experiment are highlighted in bold font. From the results presented in Table IV, we can find that our approach exhibits competitive clustering performance compared to the state-of-the-art techniques. On some benchmark datasets, the proposed method outperforms all other methods under comparison. In particular, the proposed algorithm (average performance) reaches a margin of 7.5% improvement on CIFAR-10 and 5% on CIFAR-100 in comparison with the state-of-the-art. Recall that the proposed method does not perform any direct image augmentation to the original data; instead, it relies on transformations that are not specific to image data. This leads to a notable advantage since the proposed strategy can be extended to non-image data. It should be pointed out that although VAE and IMSAT outperform all other algorithms under comparison on the STL10 dataset, they both use features extracted by a model that is pre-trained using supervised learning on Imagenet.

### F. Ablation Studies on Auxiliary Classifier

To demonstrate the advantage of the proposed auxiliary classifier, and to evaluate the behaviour of each regularization component, we conduct a range of experiments based on Equation 9 on the CIFAR-10 dataset. In the first group of evaluations, the following settings apply across all experiments: the deployed model uses a single cluster head and the MI (Equation 4) part of Equation 9 remains unchanged. We compare the following three variants of the regularization term: 1) the VAT component (Equation 5) is switched on and the dropout part (Equation 8) is switched off; 2) the VAT component is switched off and the dropout part is switched on; and 3) Both components are switched on using the default parameters in Equation 9. In the second group of experiments,
we use a set of five cluster heads for each model and one over-cluster head. The training methodology remains the same as in the first group. In all experiments, the scale factor remains constant as \( \delta = 10^{-4} \cdot \log(k) \) for all single-cluster heads and \( \delta = 10^{-2} \cdot \log(k') \) for the over-cluster head if this is involved.

Note that for the VAT evaluation of the single-cluster head we decrease the value of \( a_{adv} \) from 0.15 to 0.1. The results obtained for the single-cluster head and the multiple cluster heads are presented in Fig. 4(a) and Fig. 4(b), respectively. As can be observed from these plots, the use of both VAT and dropout terms performs the best.

Additionally, we examine the impact of the scale factors \( a_r \) and \( a_{adv} \) on the final performance of the model. They both are hyper-parameters indicating the impact of the produced adversarial noise on the representations. The performance is illustrated in Fig. 4(c) for \( a_r \in \{0.1, 0.2, 0.3, 0.4\} \) and \( a_{adv} \in \{0.05, 0.10, 0.15, 0.20, 0.25\} \). In these figures, the range of \( a_r \) is denoted by different shapes and colours and \( a_{adv} \) is the x-axis. From these results, we see the performance of the model is relatively insensitive to the perturbation noise when \( a_{adv} \) is in the range of \([0.1, 0.2]\) and it achieves the best robustness when \( r_{adv} = 0.15 \).

As the last part of experiments on the hyper-parameters, we compare the auxiliary classifier with three of its variants on the CIFAR-10 dataset and the results are presented in Table VI. The first variant has one single cluster head only and is trained by minimizing the proposed objective function with \( \delta = 0 \). The second variant also has a single cluster head, however,
TABLE V: Predicted accuracy per class in CIFAR-10

| Dropped     | constant δ-tolerance | variable δ-tolerance |
|-------------|-----------------------|----------------------|
|             | 0%  | 10%  | 20%  | 30%  | 40%  | 10%  | 20%  | 30%  | 40%  |
| airplane    | 78.4% | 75.3% | 78.1% | 77.9% | 77.3% | 76.2% | 76.9% | 73.5% | 74.4% |
| automobile  | 89.3% | 88.9% | 88.7% | 88.6% | 89.2% | 88.7% | 89.5% | 90.1% | 89.0% |
| bird        | 50.7% | 52.8% | 41.8% | 39.3% | 11.6% | 45.4% | 44.9% | 9.4%  | 10.6% |
| cat         | 23.4% | 43.7% | 20.3% | 24.4% | 40.3% | 23.9% | 25.7% | 44.9% | 44.8% |
| deer        | 72.0% | 71.0% | 70.8% | 71.8% | 72.5% | 70.5% | 71.5% | 72.5% | 72.9% |
| dog         | 59.6% | 50.6% | 51.7% | 47.7% | 45.5% | 59.8% | 56.6% | 49.4% | 47.4% |
| frog        | 84.5% | 83.2% | 84.0% | 83.7% | 83.6% | 84.1% | 83.7% | 83.5% | 82.9% |
| horse       | 69.9% | 69.8% | 69.7% | 69.7% | 69.0% | 70.5% | 69.6% | 67.1% | 67.4% |
| ship        | 89.7% | 89.0% | 89.3% | 90.5% | 90.2% | 89.8% | 89.1% | 88.9% | 88.2% |
| truck       | 82.7% | 81.8% | 82.6% | 81.8% | 81.3% | 83.1% | 82.9% | 82.9% | 82.9% |

Clustering performance of the auxiliary classifier with dropped features from the following classes: Airplane, Automobile and Bird. The dropout rates are mentioned on top of each column (where 10% represents 600 elements).

\[ \delta = 10^{-4} \cdot \log(k) \]. The third and fourth variants of the proposed auxiliary classifier have five cluster heads with \( k = 10 \) outputs and one additional over-cluster heads with \( k' = 50 \) outputs. The main difference between the third and fourth is that the former is trained with \( \delta = 0 \) for all cluster heads, while for the latter, \( \delta = 10^{-4} \cdot \log(k) \) for the five cluster heads with ten outputs and \( \delta = 10^{-2} \cdot \log(k') \) for the one over-cluster heads with 50 outputs. Note that the fourth variant is the standard one used in all the previous experiments and its parameter setting are listed in Table IV. The softmax activation is applied for all probabilistic outputs in the set of experiments here. All experiments have taken place in the same generated domain. The auxiliary classifier has two hidden layers, each consisting of 1024 units. The mini-batch size is set to 500 in each training round. In all the above four variants, the classifier is optimized for 200 iterations on the full dataset. Three independent runs are performed and the best performances are reported in Table VI. Note that for the variants with multiple cluster heads, we present the accuracy of the best cluster head, together with the mean accuracy averaged over all heads and the lowest performance.

TABLE VI: Effects of multiple cluster-heads and δ-tolerance

| Method | Single Output | Multiple Outputs |
|--------|---------------|------------------|
|        | 65.71%        | 66.59%           |
|        | 66.31%        | 66.31%           |
|        | 54.7%         | 57.4%            |
|        | 68.20%        | 70.04%           |
|        | 69.64%        | 68.68%           |
| \( \delta = 0 \) |               |                  |
| \( \delta > 0 \) |               |                  |

From the results in Table VI we can conclude that the auxiliary classifier proposed in this work with multiple cluster heads and \( \delta > 0 \) in the loss function has resulted in the best performance among all four compared variants. Meanwhile, the classifiers with multiple heads performed better than those with a single head. Note, however, that the variants with a single cluster head demonstrate lower performance on \( \delta > 0 \), in comparison with the multiple heads variants. These results confirm the benefit of using multiple clusters and modifying the loss function.

G. Evaluation on Imbalanced Data

We further evaluated the effectiveness of the proposed auxiliary classifier on imbalanced datasets and the results are listed in Table V. Note that CIFAR-10 is a perfectly balanced dataset, where each class contains exactly 6000 training samples. Specifically, we examine the influence of the tolerance factors on the performance of the auxiliary classifier by randomly dropping some data from the three classes: ’airplane’, ’automobile’ and ’bird’. The dropping rate is increased by 10% in each experiment as follows: 0%, i.e., no data is dropped; 10%, with 600 data pairs being dropped; 20%, 1200; 30%, 1800; and 40%, 2400. Two sets of experiments are conducted, one with \( \delta \) being fixed, and the other with \( \delta \) being varied. Detailed settings of the hyper-parameters are described below.

- **Constant tolerance rates.** In this set of experiments, the tolerance rate is kept constant while the dropping rate is changed. Note that for the cluster heads with 10 outputs, \( \delta = 10^{-4} \) and for the overcluster heads with 50 outputs, \( \delta = 10^{-2} \).
- **Variable tolerance rates.** In this set of experiments, the tolerance factors vary together with the drop rate. The drop rate, the tolerance for the cluster heads, and the tolerance rate for the overcluster heads are: 10%, 10^{-4}; 2 \cdot 10^{-2}; 20%, 10^{-3}; 2 \cdot 10^{-2}; 30%, 10^{-3}; 5 \cdot 10^{-2}; and 40%, 2 \cdot 10^{-3}; 5 \cdot 10^{-2}, respectively.

The classifier consists of five cluster-heads with 10 outputs and two over-cluster-heads with 50 outputs. In Table V the results of the best-performing cluster-head after 200 iterations are presented.

As we can see from Table V, the auxiliary classifier is considerably robust to the imbalanced data. The accuracy slightly deteriorates in the cases with data being dropped. More specifically, the worst performance is observed for the ’bird’ class, as the accuracy achieved on this class was the lowest among the three dropped classes, even without removing any data. Furthermore, as presented in Fig. 6 (A), classes ’cat’ and ’bird’ share some similarities in the generated features, and therefore the performance of these two classes is similar when the drop rate increases. It is surprising to see that the accuracy is improved when the drop rate is set to 10% or 40%, whereas the performance remains unchanged for the settings. From these results, we can conclude that the overall performance of the classifier is satisfactorily high on all imbalanced datasets. Additionally, consistently high accuracy is observed across all classes, although, surprisingly, an extra term in the loss function for the tolerance has made little impact on the accuracy.
Fig. 5: Comparison of the discriminator’s performance with or without the Sobel operation. The plots in the top row show the absolute accuracy achieved with the features extracted by k-means calculated in every 20 epochs (the blue line indicates the Sobel filter operation). The bottom row visualizes the errors of the discriminator and the generator, implying that adding the Sobel filters in the discriminator does not impair the training performance.

H. Feature Extraction Validation

1) Influence of Sobel filter: Figure 5 illustrates the benefit of integrating a Sobel filter in the discriminator for feature extraction. Here, we implement two similar architectures, one with and the other without a Sobel filter. Firstly, we can observe from the plots in the bottom row that the additional constant filters have no effect on the already competitive training phase of the GAN framework across the three training sets. The plots in the top row visualize the accuracy achieved using the features extracted by k-means in every 20 epochs. The dimension of the extracted representations is reduced to 20 with PCA. The higher margin between the architectures can be attributed to the challenging nature of the dataset (STL10) with a mean accuracy of 39.61% and 38.10%, respectively, with and without the Sobel operator. Note that the algorithm without the Sobel filters requires 33.4sec for each epoch on STL10 on Nvidia RTX 2080Ti, and an additional 0.4sec is needed when the Sobel filters is used.

2) Classification: In the previous results, we have show the promising performance of the proposed model for data clustering. Here, we want to demonstrate the capability of the modified discriminator in the proposed model for classification. To do so, we evaluated our approach by comparing it with a list of benchmark representation learning techniques, namely autoencoders, the original DCGAN with an intermediate hidden flatten layer similar to our proposed architecture, a bidirectional GAN model, and the Deep InfoMax. Note that none of the compared methods relies on image augmentation operations. Instead, the representation is learnt directly from the original training set.

All experiments have been conducted on CIFAR-10, which consists of 50000 training and 10000 testing samples. Similar to [41], the produced features were evaluated against the following two approaches:

- Linear-SVM. Firstly, the generated features of the flatten layer are reduced to 50 components via PCA. Then, a linear L2-SVM is trained on this reduced domain.
- Non-Linear model. A single hidden layer network of 200 units is built on top of the main framework. During the training, the weight parameters are optimized separately from the main framework. A dropout technique is introduced to alleviate over-fitting in the training phase with a dropout rate of 40%.

| CIFAR-10 | Model | L2-SVM | Non-Linear Model |
|----------|-------|--------|------------------|
| VAE      | 42.58%| 58.61% |
| AE       | 40.58%| 55.02% |
| AAE †    | 43.34%| 57.19% |
| BiGAN †  | 38.42%| 62.74% |
| DIM(L) † | 54.06%| 75.57% |
| DCGAN ‡  | 54.70%| 70.61% |
| DCGAN *  | 61.06%| 74.45% |
| DCGAN * ‡| 71.22%| 78.25% |

† denotes the initial DCGAN architecture evaluated only in the last convolutional layer.  
* DCGAN architectures with a fully connected hidden layer prior to the probabilistic output.  
| Due to the high processing demand of the above experiments, the results of BiGAN, DIM(L) and AAE are taken from [41].

TABLE VII: Classification of Extracted Features
Table VII presents the prediction results of the two techniques on the testing data. From these results, we can see that our approach exhibits a superior performance on both classification tasks, where a significant margin is observed when using the linear SVM model. Notably, the result of the auxiliary classifier in Table IV achieved its best accuracy of 70.04% in an unsupervised manner, outperforming the majority of the methods under comparison in Table VII. In these compared methods, feature extraction is accomplished via unsupervised learning followed by the classification task, reached in a supervised manner with the relevant labels to be provided during the training. Finally, we can observe from these results that the Sobel filter is able to enhance the classification accuracy of the linear SVM by a large margin of 10%.

3) Visualization: In this phase, we initially reduce the generated features ($M$) via PCA, equivalently to the classification task, and select only the 50 components with the largest variance. The data reduced by PCA is further reduced into a two-dimensional embedding space via t-SNE, a state-of-the-art visualization technique [63].

The results of t-SNE are presented in Fig. 6(A). The visualization is colored according to the ground truth label, where each color represents one particular class. In addition, Table V presents the prediction accuracy on CIFAR-10 when the tolerance rate varies, and when a certain percentage of the data is dropped. By observing the results in Table V and the visualization in Fig. 6(A) (which is based on ground truth),

We can note that there is a correlation between the visualized data and classifier’s predictions. From Fig. 6(A), we recognize that similar classes are placed in the neighbourhood in the scatter plot. For example, ‘automobile’ (notated as ‘auto’, purple) and ‘truck’ (red), ‘deer’ (light green) and ‘horse’ (yellow). Additionally, the subsets of ‘ship’ and ‘airplane’ share the same cyan background, indicating that ‘airplane’ instances are placed in the ‘ship’ cluster neighbourhood. On the other hand, classes such as ‘dog’ (dark green), ‘cat’ (cyan), and ‘bird’ (dark blue) are mixed in the scatter plot. Therefore, the performance of the auxiliary classifier heavily relies on the quality of the features generated by the discriminator. Refer also to the top panel of Fig. 3 for the predicted results on CIFAR-10.

V. CONCLUSION

In this work, we present a deep framework for image clustering. Experimental results show very competitive performance of the proposed framework compared with state-of-the-art deep clustering techniques. Even with a single cluster head, the proposed framework is able to achieve surprisingly high accuracy, and with multiple cluster heads, the performance is further enhanced. Finally, we demonstrate the robustness of the proposed framework for clustering imbalanced data.

Despite the promising results, the effectiveness of the auxiliary classifier in the proposed framework highly relies on the separability of the features generated by the discriminator. Additionally, large-scale GAN models may suffer from unstable performance during the training process, as well as the high computational cost for the optimization of the generator. Thus, our future work will investigate new techniques for reducing the computational cost. In addition, we intend to extend the proposed framework to other types of high-dimensional data such as audio and spectral data, since its internal mechanisms for data augmentation do not rely on any image augmentation techniques.
[46] D. McAllester and K. Stratos, “Formal limitations on the measurement of mutual information,” 2019. [Online]. Available: https://openreview.net/forum?id=BkedwoC5t7

[47] I. Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin, and A. C. Courville, “Improved training of wasserstein gans,” CoRR, vol. abs/1704.00028, 2017.

[48] M. Arjovsky, S. Chintala, and L. Bottou, “Wasserstein gan,” 2017.

[49] X. Mao, Q. Li, H. Xie, R. Y. K. Lau, Z. Wang, and S. P. Smolley, “Least squares generative adversarial networks,” 2016.

[50] J. J. Zhao, M. Mathieu, and Y. LeCun, “Energy-based generative adversarial network,” CoRR, vol. abs/1609.03126, 2016.

[51] A. Krizhevsky, “Learning multiple layers of features from tiny images,” MIT and NYU, Tech. Rep., 2009.

[52] J. Zhang, L. Chen, L. Zhao, X. Liang, and J. Li, “An efficient hyper-spectral image retrieval method: Deep spectral-spatial feature extraction with dcan and dimensionality reduction using t-sne-based nm hashing,” Remote Sensing, vol. 10, p. 271, 02 2018.

[53] L. Chen, J. Zhang, X. Liang, J. Li, and L. Zhuo, “Deep spectral-spatial feature extraction based on dcan for hyperspectral image retrieval,” in 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2017, pp. 752–759.

[54] P. Bojanowski and A. Joulin, “Unsupervised learning by predicting noise,” 2017.

[55] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York, NY, USA: Wiley-Interscience, 1991.

[56] H. W. Kuhn, “The hungarian method for the assignment problem,” Naval Research Logistics Quarterly, vol. 2, no. 1-2, pp. 83–97, 1955.

[57] Y. Nair and G. E. Hinton, “Rectified linear units improve restricted boltzmann machines,” in Proceedings of the 27th International Conference on International Conference on Machine Learning, ser. ICML’10, USA: Omnipress, 2010, pp. 807–814.

[58] B. Xu, N. Wang, T. Chen, and M. Li, “Empirical evaluation of rectified activations in convolutional network,” CoRR, vol. abs/1505.00853, 2015.

[59] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhudinov, “Dropout: A simple way to prevent neural networks from overfitting,” Journal of Machine Learning Research, vol. 15, pp. 1929–1958, 2014.

[60] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” in 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings, Y. Bengio and Y. LeCun, Eds., 2015.

[61] Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle, “Greedy layer-wise training of deep networks,” in Advances in Neural Information Processing Systems 19, B. Schölkopf, J. C. Platt, and T. Hoffman, Eds. MIT Press, 2007, pp. 153–160.

[62] D. P. Kingma and M. Welling, “Auto-encoding variational bayes,” 2013.

[63] L. van der Maaten and G. Hinton, “Visualizing data using t-SNE,” Journal of Machine Learning Research, vol. 9, pp. 2579–2605, 2008.