

氏 名 村瀬 博典

学位(専攻分野) 博士(統計科学)

学位記番号 総研大甲第 2355 号

学位授与の日付 2022 年 9 月 28 日

学位授与の要件 複合科学研究科 統計科学専攻
学位規則第6条第1項該当

学位論文題目 Anomaly Detection by Generating Pseudo Anomalous Data

論文審査委員 主 査 吉田 亮
統計科学専攻 教授
藤澤 洋徳
統計科学専攻 教授
福水 健次
統計科学専攻 教授
山田 誠
京都大学 大学院情報学研究科 准教授

(様式3)

博士論文の要旨

氏名 村瀬 博典

論文題目 Anomaly Detection by Generating Pseudo Anomalous Data

Closely related to outlier and novelty detection, anomaly detection refers to the technique of distinguishing between unexpected and normal data. Practical examples include fraud detection, medical diagnosis, surveillance, and optical inspection, and a common feature of these applications is the discovery of undesirable data.

The difficulty with anomaly detection is that, in many cases, anomalous data are rarely observed and are of a wide variety; hence, the learning of anomaly detection models suffers from the difficulty of imbalanced or one-class classification. Additionally, as the preparation of large amounts of anomalous data is difficult, training without anomalous data is a preferable approach. Therefore, the focus of this thesis is upon anomaly detection using only normal training data. A wide variety of methods have already been proposed in this field based on traditional machine learning and statistical techniques, such as one-class classification, likelihood, nearest neighbors, and clustering.

Recently, deep learning methods such as representation learning have been successfully applied to anomaly detection without using anomalous data for training. Taking advantage of the effective representation of deep learning, the features obtained by a pre-trained model, such as VGG and ResNet, can also be applied to unsupervised anomaly detection. Since deep generative models are able to learn probability distributions of normal data, they have been combined for anomaly detection in various ways.

Generative models approximate the true data distribution of observed samples with probabilistic models. However, generative modeling of high-dimensional data distributions such as images is difficult, and hence generative models using deep learning methods have been studied. Most previous anomaly detection studies using deep generative models have taken advantage of the model characteristic of generating only normal samples. By contrast, only a few have focused on generating outlier samples and adding them to training. In addition to the generative model network, some deep generative models also use subnetworks such as an encoder and a discriminator for training. We aim to utilize these subnetworks to improve the efficiency of anomaly detection.

In this thesis, we propose a method that improves anomaly detection performance by generating pseudo-anomalous data from only normal training data using Generative Adversarial Networks (GANs). Unlike the standard usage of GANs, the generator used in the proposed method provides pseudo-anomalous data and fake-normal data by introducing anomalous states in the latent variable; this model is known as Anomalous Latent GAN (ALGAN). Note that the discriminator of a standard GAN is not necessarily suitable for distinguishing between normal and anomalous data. It is trained to discriminate between real and fake data such that in successful learning, the two classes are almost similar. By contrast, when training is successful, the discriminator of ALGAN distinguishes between the group of real-normal data and the group of fake-normal and pseudo-anomalous data.

We introduce two types of pseudo-anomalous data for training. The first type of pseudo-anomalous data is called fake-anomalous data. ALGAN utilizes the anomalous latent variables with a larger variance to generate fake-anomalous data. The other type of pseudo-anomalous data is called buffered data, which are defined as generated samples during the early stage of the training process. These are expected to differ from the normal training (real-normal) data.

The proposed method follows an adversarial training procedure. It provides a discrimination boundary not only for the real-normal and fake-normal data but also for the real-normal and pseudo-anomalous data, the latter of which has a broader support of the distribution. As the training progresses, the generator produces samples that resemble real-normal data, and the discriminator cannot distinguish between real-normal and fake-normal data. The pseudo-anomalous data are clearly different from the real-normal data; therefore, the discrimination boundary of the discriminator is used to classify them.

The proposed method for generating pseudo-anomalous data can be applied to both images and feature vectors. We applied it to three anomaly detection benchmarks and demonstrated its high accuracy. On MVTEC-AD, ALGAN-image achieved more than 10% higher average accuracy than conventional image-based methods, and ALGAN-feature exhibited comparable ability to the feature-based methods. On the COIL-100 dataset, ALGAN performed almost perfectly.

Real-time prediction is significant to apply anomaly detection in the real world, where the data generation speed has increased. Reducing computational costs will contribute to the expansion of the application. The proposed ALGAN exhibited remarkably fast predictions. Compared with conventional methods trained on image data and features, ALGAN could predict up to tens of times faster while maintaining high performance.

博士論文審査結果

Name in Full
氏名 村瀬 博典

Title
論文題目 Anomaly Detection by Generating Pseudo Anomalous Data

2022年8月23日午後3時から約2時間にわたり村瀬博典氏の博士論文審査委員会を開催した。出願者による1時間の公开发表による概要説明と質疑応答、さらに約1時間の審査委員のみによる審査を行った結果、審査委員会は本論文が学位の授与に値すると判断した。

[論文の概要]

提出された論文は、深層生成モデルを用いた異常検知の方法に関して論じたもので、英文で書かれており全6章74頁からなる。

1章は本論文の序章であり、本論文が議論する、正常データのみからの異常検知の学習に関して背景、動機付け、および目標が述べられている。

2章は準備であり、本論文で提案する方法に用いられる生成モデルおよび敵対的生成モデル (GAN) に関して説明がなされている。

3章は本論文の主題である異常検知に関して、過去の研究を論じている。尤度や距離などに基づく伝統的な方法を述べた後、より最近の関連手法として敵対的生成モデルを用いた異常検知の方法が紹介されている。また、特に画像データに対する異常検知に対して最近研究がさかんな、深層モデルによって ImageNet を事前学習して得られる特徴量を用いた異常検知の方法に関して説明がなされている。また、異常検知法を比較する際のメトリックである AUROC に関して説明されている。

4章では、本論文で提案する手法である、異常検知法 Anomalous Latent Generative Adversarial Networks (ALGAN) を論じている。GAN は、標準正規分布によるサンプルを深層ニューラルネットに変換することによって、与えられた訓練データに近い分布を得ようとするモデルであるが、ALGAN ではこれに加えて、より分散の大きい正規分布からのサンプルから疑似異常データを生成させることにより、GAN の学習に用いられる判別機が正常と疑似異常を判別するよう学習を行う。その結果として ALGAN は、画像などに特化した方法とは異なりデータタイプに依らない汎用的方法であり、判別機による計算量の低い異常検知を実現することが述べられている。

5章では、数値実験によって ALGAN と関連手法を比較した結果が述べられている。画像からの製品検査を目的とした標準的データセット MVTEC-AD を含む3種類の実画像データを用いて比較した結果、GAN を用いた異常検知の既存手法と比べ、ALGAN は AUROC による検知性能でこれらを上回る結果を示し、画像からの製品検査データに特化した最良の既存手法と比較して、検知性能では同等に近い性能ながら検知時間は10分の1以下であることが示されている。また、学習時に出現しないような異常データに対する能力、ハ

イパーパラメータ選択法，潜在変数を生成する分布の影響に関しても，それぞれ論じられている．

6章は本論文のまとめである．

[論文の評価]

本論文は，正常データだけを用いて学習を行う異常検知の問題に対して，近年発展した深層生成モデルを適切に利用して疑似異常データを生成させ，複雑なモデル構成を使うことなく識別機による異常検知を可能とする方法を提案し，高い検知性能と高速な検知時間を両立させており，統計科学の博士論文として十分な意義を持つと考える．

なお，3章と4章の内容をまとめた論文が査読付き国際論文誌 [IEEE Access](#)（第一著者）に採択されている．