汤文杰, 徐俊华, 付纯博, 等. 基于 DSVDD、对抗学习和紧密包裹学习的异常检测单阶段模型[J]. 智能计算机与应用, 2026,16(7):57-63. DOI:10.20169/j.issn.2095-2163.25102703

基于 DSVDD、对抗学习和紧密包裹学习的异常检测单阶段模型

汤文杰[1], 徐俊华[1,2], 付纯博[1], 杨国为[1,2]
(1 南京审计大学 计算机学院, 南京 211815; 2 南通理工学院 信息工程学院, 江苏 南通 226002)

摘 要: 深度支持向量数据描述(DSVDD)、变分自编码器(VAE)、生成对抗网络(GAN)和紧密包裹学习等方法在异常检测建模中发挥了重要作用,有效推动了该领域的研究取得显著进展。然而,单一方法构建的模型在检测精度和泛化能力方面仍存在局限性。为克服这些不足,本文提出了一种融合 DSVDD、对抗学习和紧密包裹学习的(双超球间隔最大博弈)异常检测单阶段模型。该模型创新性地结合了 DSVDD 的超球体学习、GAN 的对抗学习以及紧密包裹学习,通过双超球最大分隔博弈目标函数实现单阶段训练。其中,DSVDD 的超球体学习为正常样本提供紧凑的超球体表示,并增大异常样本与正常样本之间的分离度;GAN 的对抗学习增强了模型对特征表示的鲁棒性;紧密包裹学习则进一步优化了检测边界,使其更加清晰和准确。这些机制协同作用,提高了模式特征分布建模的精度,并显著增强了模型的泛化能力。实验结果表明,该模型在多个数据集上的表现优于多种现有的异常检测模型,展现出更高的检测精度和泛化能力。

关键词: 异常检测; 生成对抗网络; 紧密包裹学习; 支持向量数据描述; 对抗学习; 特征表示学习
中图分类号: TP18 **文献标志码**: A **文章编号**: 2095-2163(2026)07-0057-07

Anomaly detection single-stage model based on DSVDD, adversarial learning, and tightly-wrapped learning

TANG Wenjie[1], XU Junhua[1,2], FU Chunbo[1], YANG Guowei[1,2]
(1 School of Computer Science, Nanjing Audit University, Nanjing 211815, China;
2 School of Information Engineering, Nantong Institute of Technology, Nantong 226002, Jiangsu, China)

Abstract: Methods such as Deep Support Vector Data Description (DSVDD), Variational AutoEncoders (VAE), Generative Adversarial Networks (GAN), and tightly-wrapped learning have played significant roles in anomaly detection modeling, substantially advancing research in this field. However, models constructed using a single method still exhibit limitations in detection accuracy and generalization capability. To overcome these shortcomings, this paper proposes a single-stage anomaly detection model integrating DSVDD, adversarial learning, and tightly-wrapped learning, termed the dual-sphere margin maximization game model. This model innovatively combines the hypersphere learning of DSVDD, the adversarial learning of GANs, and tightly-wrapped learning, achieving single-stage training through a dual-sphere maximum margin game objective function. Specifically, the hypersphere learning of DSVDD provides a compact sphere representation for normal samples and increases the separation between anomalous and normal samples; the adversarial learning of GANs enhances the robustness of the model's feature representations; and tightly-wrapped learning further optimizes the detection boundary, making it clearer and more accurate. These mechanisms work synergistically to improve the accuracy of modeling feature distributions and significantly enhance the model's generalization ability. Experimental results demonstrate that the proposed model outperforms various existing anomaly detection models on multiple datasets, showcasing higher detection accuracy and generalization capability.

Key words: anomaly detection; Generative Adversarial Network; tightly-wrapped learning; support vector data description; adversarial learning; feature representation learning

基金项目: 国家自然科学基金(62172229); 江苏省自然科学基金(BK20211295); 南通理工学院科技创新基金(XYJS202501)。

作者简介: 汤文杰(2000—),男,硕士研究生。主要研究方向:模式识别; 徐俊华(2000—),男,硕士研究生。主要研究方向:模式识别;付纯博(2001—),男,硕士研究生。主要研究方向:模式识别。

通信作者: 杨国为(1964—),男,博士,教授,博士生导师。主要研究方向:模式识别,人工智能,机器学习。Email:ygw_ustb@163.com。

收稿日期: 2025-10-27

0 引 言

异常检测作为机器学习中的一项基础研究课题,在图像分析[1]、欺诈检测、网络入侵检测[2]、网络安全和医疗诊断[3]、工业故障诊断[4]等多个关键领域具有广泛的应用需求。其核心目标是从大量正常数据中识别出偏离正常模式的异常样本。传统方法如一类支持向量机(One-Class Support Vector Machine,OC-SVM)和核密度估计(Kernel Density Estimation,KDE)在处理低维数据时表现出色,然而,面对高维、复杂结构的数据(如图像、视频等),这些方法往往受限于特征表达能力和计算效率,难以捕捉语义层面的异常模式。

传统方法中,一类支持向量机、核密度估计及支持向量数据描述(Support Vector Data Description,SVDD)[5]应用广泛。OC-SVM 通过构建区分正常数据的超平面实现异常检测,但在处理高维或复杂数据时受限于其线性或核函数映射机制。相比之下,SVDD 作为 OC-SVM 的扩展,通过寻找最小体积超球体紧凑包围正常样本,在检测性能和实际应用灵活性方面通常表现更优。

近年来,深度学习通过多层次非线性变换实现了对复杂数据的高度抽象和特征自动提取[6],为异常检测提供了新的解决思路[7]。自编码器及其变体通过最小化输入与重构输出之间的误差进行训练,并假设异常样本无法被准确重构,但重构误差对网络结构[8]、降维程度[9]和噪声干扰极为敏感,且难以区分语义异常与轻微扰动。

在生成模型方面,生成对抗网络(Generative Adversarial Network, GAN)[10]展现出独特优势。GAN 通过判别器与生成器的对抗博弈[11],能够学习数据分布特征并生成高质量样本。但典型 GAN 异常检测方法、如 AnoGAN[12]需要在测试时进行潜在空间搜索,计算开销较大,限制了实际应用。

在判别式方法中,DSVDD 通过将正常样本映射到预定义超球体内的最小空间区域,实现了端到端的异常评分。该方法直接优化异常检测目标,具有理论优雅性。然而,DSVDD 存在以下局限:

(1)容易发生超球体坍塌,导致模型失效。

(2)对超球中心选择敏感,不同初始化策略影响显著。

(3)特征判别能力有限,处理复杂数据时泛化不足。

(4)缺乏额外监督信号来保证特征判别性。

紧密包裹学习作为新兴异常检测技术,在核心思想与 DSVDD 的超球包裹相似的基础上,更强调紧密性与间隔最大化,通过动态调整边界使正常样本形成更紧凑的聚集。然而现有方法多与传统浅层技术结合,缺乏与深度学习的深度融合,难以处理高维复杂数据。

为克服这一局限,本研究提出基于 DSVDD、对抗学习和紧密包裹学习的双超球间隔最大博弈异常检测模型。该模型通过三者的有机结合,充分发挥各自优势:DSVDD 与对抗学习相结合提供明确的优化目标并增强特征判别能力;紧密包裹学习机制则提升对复杂异常模式的识别精度。

本研究旨在构建高效准确的异常检测模型,通过深入探索 3 种技术的特性及其融合方式,设计出能适应不同领域需求的新方法,显著提升对异常样本的识别性能。

本文的主要贡献包括:

(1)模型融合创新。首次将 DSVDD、对抗学习和紧密包裹学习相结合,提出了双超球间隔最大博弈异常检测单阶段模型。

(2)单阶段训练架构。设计了一种新颖的单阶段训练架构,避免了多阶段训练中的误差累积和优化不一致问题。

(3)对抗训练提升特征质量。通过对抗训练机制,有效提升了特征的质量,增强了模型对复杂异常模式的识别能力,同时防止了超球体退化。

(4)自适应权重调整策略。提出了一种自适应权重调整策略,能够在训练过程中动态平衡超球体损失与对抗损失,使模型能够更好地学习到具有判别性的特征表示。

1 相关工作

1.1 异常检测

早期的异常检测方法主要基于统计分析和浅层机器学习模型。一类支持向量机(OC-SVM)通过在特征空间中寻找最优超平面以实现正常与异常样本的分离[13],其核函数版本能够处理非线性问题,但在高维数据上计算成本高昂且严重依赖核函数选择。支持向量数据描述(SVDD)是另一种经典方法,但其同样面临核函数选择和计算复杂度的问题。隔离森林(Isolation Forest,IF)[14]通过随机分割特征空间[15]来检测异常,虽然计算效率较高,但在高维数据上性能下降明显。这些传统方法通常需要精心设计的特征工程,且难以捕捉图像等复杂数据的语

义信息。

为克服这一局限，研究者提出了多种改进方案。变分自编码器（Variational AutoEncoder，VAE）[16] 通过引入概率编码提高了模型泛化能力，但其重构误差往往过于平滑，降低了异常检测的敏感性。去噪自编码器通过向输入添加噪声并训练网络恢复原始输入，增强了模型的鲁棒性。对抗自编码器（Adversarial AutoEncoder，AAE）结合了自编码器和 GAN 的优点，但仍未解决重构误差作为异常指标的固有缺陷。

1.2　深度单类分类

DSVDD[17] 代表了单类分类领域的一项重要突破，将传统的核方法推广到深度学习框架中。与基于重构或生成的方法不同，DSVDD 采用了一种直接的最小体积学习范式：通过深度神经网络将正常样本映射到输出空间中的一个预定义中心的超球体内，并通过最小化超球体体积来学习紧凑的特征表示。其数学目标函数可以表述为：同时优化超球体半径 R 和网络参数 W，使得大部分正常样本被包含在超球体内，而异常样本则落在超球体外。

DSVDD 是对经典核函数 SVDD 方法的深度扩展，其核心思想来源于 v-SVDD。该模型通过神经网络将输入数据映射到特征空间，并在此空间中学习一个体积最小的超球体。在特征空间中，正常样本被约束在超球体内部，而异常样本则位于超球体外部。超球体的位置和大小由球心 c 和半径 R 共同确定。

DSVDD 的目标函数定义为：

$$\min_{W,R} R^2 + \frac{\gamma}{m}\sum_{i=1}^{n}\max\{0, \|\phi(x_i;\boldsymbol{W}) - c\|^2 - R^2\} + \frac{\lambda}{2}\sum_{l=1}^{L}\|\boldsymbol{W}^l\|_F^2 \tag{1}$$

其中，$\boldsymbol{W}$ 表示网络权重矩阵，γ 和 λ 为超参数，用于平衡各项的贡献。该设计的合理性已得到理论证明。通过优化该目标函数，网络能够自主学习参数 $\boldsymbol{W}$，使正常样本在特征空间中紧密聚集周围中心点 c。

当训练数据中绝大多数样本都属于正类时，目标函数可简化为一类深度 SVDD 的形式：

$$\min_{W} \frac{1}{n}\sum_{i=1}^{n}\|\phi(x_i;\boldsymbol{W}) - c\|^2 + \frac{\lambda}{2}\sum_{l=1}^{L}\|\boldsymbol{W}^l\|_F^2 \tag{2}$$

但是上述这些方法中的 R 和 c 的更新都是不精确的，这对最后的识别效果会产生一定的不利影响。

1.3　基于 GAN 的异常检测

生成对抗网络（GAN）通过生成器与判别器之间的对抗性训练，为异常检测提供了全新的技术路径。生成器致力于生成与真实样本高度相似的数据，而判别器则不断提升区分真实样本与生成样本的能力。这种对抗机制使 GAN 能够无监督地学习正常数据的本质特征和分布规律，为异常检测奠定了坚实基础。

AnoGAN 作为开创性工作，首次展示了 GAN 在异常检测领域的潜力。后续提出的 GANomaly[18]、Efficient-GAN-Anomaly 等改进方法，在保持 GAN 优势的同时，逐步解决了计算效率问题，使基于 GAN 的异常检测方法更具实用价值。

1.4　紧密包裹学习

为了学习更精确的决策边界，杨国为等学者[19] 提出了紧密包裹学习的思想。紧密包裹学习由同类特征集合的紧密包裹集构造算法，以及基于同类特征集合和紧密包裹集的同类特征区域紧密包裹面的求解算法组成，其中正常类的紧密包裹集构造是至关重要的部分。通过紧密包裹学习，能获得同心内、外两个超球面，且内超球面能紧致包含正常类样本集，同时外超球面能把异常类点集和紧密包裹点集支撑到外超球之外，实现正常类与异常类的最大分隔。

2　DSVDD-ATWL 方法

在本节中，提出了基于 DSVDD、对抗学习和紧密包裹学习的双超球间隔最大博弈异常检测单阶段模型。该模型旨在解决传统深度支持向量数据描述方法中存在的超球体坍塌、特征判别能力有限以及决策边界松散等问题。为实现对正常样本分布的紧凑表示并增强对异常样本的判别能力，研究构建了一个端到端的单阶段学习框架。

该框架的核心创新在于设计了双超球体结构和对抗博弈机制。模型采用残差网络 ResNet 作为共享特征提取器，将输入数据映射到特征空间。

2.1　整体框架

本文提出 DSVDD-ATWL 模型，通过双超球间隔最大博弈机制实现异常检测。该模型将 DSVDD 的超球包裹、GAN 的对抗学习和紧密包裹学习有机融合，在统一框架中同步实现三大目标：利用 DSVDD 学习正常样本的紧凑特征表示，通过紧密包裹学习优化分布边界，借助对抗博弈增强特征判别力。模型架构如图 1 所示。

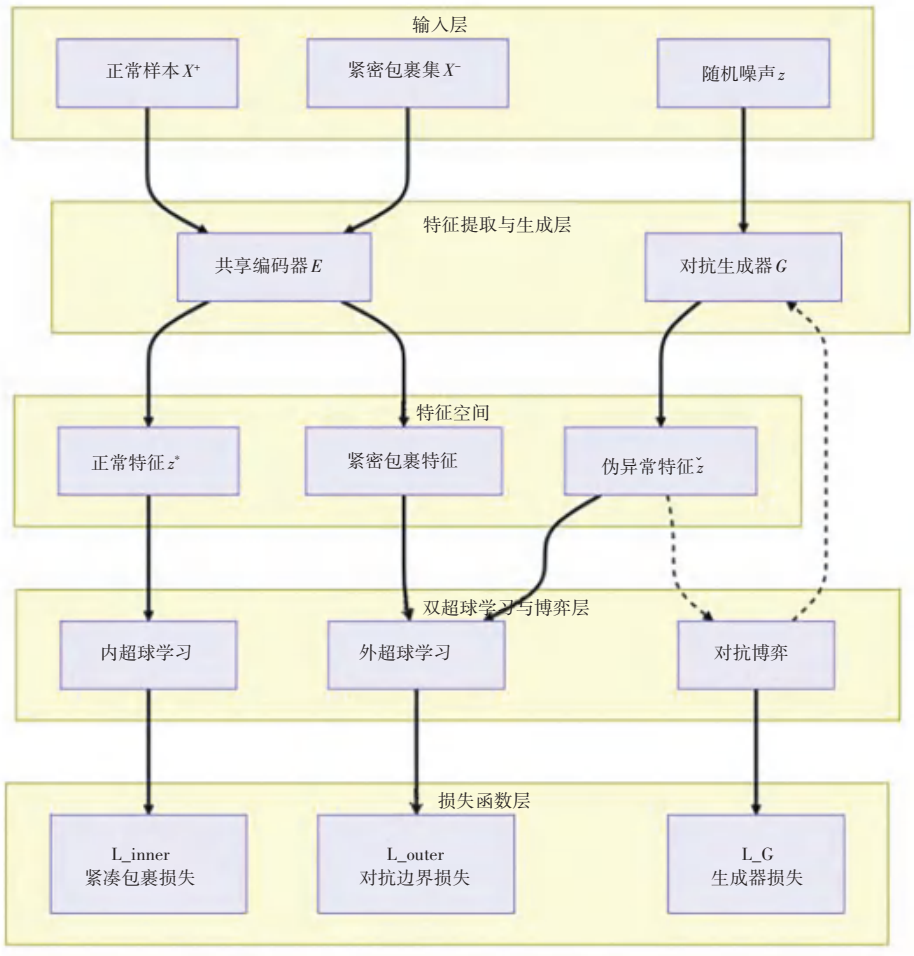


图 1 DSVDD-ATWL 模型图

Fig. 1 Diagram of DSVDD-ATWL model

2.2 目标函数

为实现正常样本紧密聚合、异常样本有效分离和对抗样本稳健防御的协同优化目标,本文将异常检测问题建模为带非线性约束的极小极大博弈问题。

在实际训练中,生成器 G 与异常检测模型构成动态博弈系统。生成器致力于生成能够欺骗检测模型的伪样本,使其误判为正常数据;检测模型则力求准确识别真实正常样本并排除所有异常。

在每一轮训练迭代中,优化过程分为 2 个阶段:

(1)固定异常检测模型参数 $(\boldsymbol{W},c,r,\rho)$,优化生成器 G。旨在生成位于当前超球面边界附近或内部的样本,以最大化地挑战现有决策边界。

(2)固定生成器 G 的参数,优化异常检测模型。旨在准确地将真实正常样本收缩于超球内部,同时将生成样本与真实异常样本(如紧密包裹点集与其他未知类)坚决地排斥于半径为 $(r^2+\rho^2)$ 的决策边界之外。

所有正常样本的特征都需要被内超球包裹,用数学公式表示为:

$$\|\phi(x_i;\boldsymbol{W})-c\|^2 \leqslant r^2, \forall i=1,2,\cdots,n \quad (3)$$

其中,$\phi(\cdot;\boldsymbol{W})$ 表示共享网络的特征映射函数,负责将输入样本转换为低维特征;c 表示双超球的共享中心,在初始阶段,将其设置为正常样本特征的均值,这样能确保初始超球可以覆盖大部分正常样本;x_i 为正常样本。

生成器生成的伪异常样本特征需要被外超球(半径为 $\sqrt{r^2+\rho^2}$)隔离,数学表达式为:

$$\|\phi(G(z_i);\boldsymbol{W})-c\|^2 \geqslant r^2+\rho^2, \forall i=1,2,\cdots,n \quad (4)$$

其中,$G(z_i)$ 表示生成器基于随机噪声 z_i 生成的样本;ρ 表示双超球间隔,控制着正常样本与异常样本的特征分离程度。

为了便于进行优化计算,通过引入惩罚项,将上述的约束问题转化为无约束的极小极大目标函数。该函数融合了双超球约束损失、对抗损失与正则化项,各部分协同工作,实现包裹、隔离与判别的三重

优化逻辑，整体目标函数如下：

$$L_{\text{total}} = \min_{r,\rho,W,c}\max_{G}\Big(r^2 - \rho^2 + \frac{1}{\nu n}\sum_{i=1}^{n}\max\{0, \|\phi(x_i;\boldsymbol{W}) - c\|^2 - r^2\} + \frac{\lambda}{2}\sum_{l=1}^{L}\|\boldsymbol{W}^l\|_F^2 - \frac{1}{\mu m_{k_0}}\sum_{\text{为紧密包裹点集类}}\sum_{j=1}^{n_k}\min\{0, \|\phi(x_i^{k_0};\boldsymbol{W}) - c\|^2 - r^2\} - \rho^2\} - \frac{1}{\mu m_{k_1}}\sum_{\text{为其他未知类},j=1}^{m}\min\{0, \|\phi(x_j^{k_1};\boldsymbol{W}) - c\|^2 - r^2\} - \rho^2\} - \omega_1\sum_{i=1}^{n}\min\{0, \|\phi(G(z_i);\boldsymbol{W}) - c\|^2 - r^2\} - \omega_2\sum_{i=1}^{n}\|\phi(G(z_i);\boldsymbol{W}) - \phi(x_i;\boldsymbol{W})\|^2\Big) \tag{5}$$

其中，第 2 项通过最小化 r^2 并惩罚正常样本偏离球面，使正常样本特征紧聚于中心 c。第 3 项对网络权重进行 Frobenius 范数惩罚，防止过拟合，第 4、5 项通过最大化 ρ^2 并利用负例样本的排斥项将已知异常推离正常球面，从而拓宽决策边界。最后 2 项引入了生成器 G，通过对抗生成样本和特征重构约束，进一步增强特征表示的鲁棒性与判别性。

该模型通过融合深度超球异常检测、间隔最大化紧密包裹学习与对抗性正则化机制，协同优化超球半径 r 与间隔带 ρ，从而实现了对正常类分布的“紧密包裹”与对异常区域的“强硬排斥”，显著增强了模型的判别能力。

2.3　优化策略与训练算法

基于前述联合目标函数，本文采用交替优化策略将复杂的极小极大博弈问题分解为 2 个相对独立的子问题进行迭代求解，以确保训练过程的稳定性和收敛性。

模型训练算法如下：

输入　正常样本集 $\{x_i\}_{i=1}^{n} = 1$，异常样本集（按照紧密包裹集构造算法等方法，建立的紧密包裹点集与其他未知类），初始化参数 $\boldsymbol{W}, c, r = 0, \rho$，$G$，超参数 $\alpha, \beta, \gamma, \delta, \lambda$，学习率 η，最大迭代次数 T

输出　最优参数 $\boldsymbol{W}^*, r^*, c^*, \rho^*, G^*$

步骤 1　初始化。使用 Xavier 方法初始化 $\boldsymbol{W}$；对生成器 G 进行短期预训练；初始化 c 为初始批次特征向量的均值；设置 $r = 0, \rho = 0$

步骤 2　for $t = 1$ to T do

步骤 3　固定生成网络及生成网络参数，优化判别网络特征提取器与中心：固定 G, r, ρ。通过随机梯度下降更新 $\boldsymbol{W}, c$：

$$(\boldsymbol{W}, c) \leftarrow (\boldsymbol{W}, c) - \eta\nabla_{W,c}L_{\text{total}}$$

步骤 4　固定特征提取器与生成器，更新超球面半径与间隔：固定 $\boldsymbol{W}, c, G$。通过投影梯度法更新 r, ρ（确保 $r \geqslant 0$，$\rho \geqslant 0$）

$$(r, \rho) \leftarrow \Pi_{R_+}((\boldsymbol{W}, c) - \eta\nabla_{W,c}L_{\text{total}})$$

步骤 5　固定判别网络，优化生成器：

固定 $\boldsymbol{W}, c, r, \rho$。通过随机梯度上升更新 G：

$$G \leftarrow G + \eta\nabla_{G}L_{\text{total}}$$

步骤 6　判断收敛：若 $\|\Delta\boldsymbol{W}\| < \varepsilon$，$\|\Delta G\| < \varepsilon$，$\|\Delta r\| < \varepsilon$，且 $\|\Delta\rho\| < \varepsilon$，则提前跳出循环

步骤 7　结束循环

步骤 8　返回 $\boldsymbol{W}^*, r^*, c^*, \rho^*, G^*$

3　实验与结果

在本节中，为验证 DSVDD-ATWL 方法的有效性，在多个基准数据集上对所提算法进行了性能评估，并与当前主流方法进行了比较。实验结果表明，该算法在开放集场景中能够实现高性能和高鲁棒性的分类。

3.1　基线方法

为全面评估所提出模型的性能，选取了多种具有代表性的异常检测算法作为基线比较方法。这些方法涵盖了不同的技术路线，包括：经典的深度单类分类算法 DeepSVDD、基于重构的 Autoencoder、OpenGAN[20] 和 PANDA[21]，同时还包含了近期提出的 MSC[22] 算法。

在具体实现上，本文的模型采用预训练的 ResNet（包括 ResNet152 与 ResNet18 两种架构）作为图像特征提取的主干网络。所有实验均严格遵循数据集原有的训练集与测试集划分，确保评估结果的公平性与可比性。

3.2　数据集

在多个标准基准数据集上开展实验，包括 FMNIST、MVTec、CIFAR-10、CIFAR-100 和 DIOR。其中，CIFAR-10 包含 60 000 张 32×32 像素的彩色图像，涵盖 10 个常见物体类别。CIFAR-100 则包含 100 个细粒度类别，图像内容涵盖动植物、家居物品等多种现实场景，具有较好的多样性和真实性。该数据集中图像的风格多变、背景复杂，对算法的泛化能力提出了较高要求，也为图像识别与分析任务带来了显著挑战。

3.3　结果和分析

本研究在多个异常检测基准数据集上对所提方法进行了全面评估，包括 FMNIST、CIFAR-10、CIFAR-100、MVTec 和 DIOR。遵循标准设定，将多

类别数据集转化为异常检测任务:每类依次作为正常类,其余作为异常类,形成多个独立任务。

在小数据集上的异常检测精度见表 1(表 1 中,最好的结果用粗体表示)。本方法在单类别分类基准测试中表现优异,超越了当前领先的自监督学习方法及基于预训练特征的自适应方法。不同网络体系结构下的性能提升见表 2(表 2 中,最好的结果用粗体表示)。表 2 中结果清晰地显示,与 DN2、PANDA 等方法相比,本方法在 VIT 架构上实现了显著性能提升。

由于引入了生成对抗网络和对抗训练机制,DSVDD-ATWL 在所有类别上的 AUC 值均超越原始 DSVDD 模型。

表 1 在小数据集上的异常检测精度(平均 ROC-AUC)

Table 1 Anomaly detection accuracy (average ROC-AUC) on small datasets %

Dataset	DSVDD	MSC	Autoencoder	OpenGAN	本文模型
FMNIST	84.8	92.8	76.1	93.4	**95.4**
MVTEC	77.9	85.1	58.7	85.7	**88.3**
DIOR	70.0	97.5	65.4	97.7	**98.1**
CIFAR-10	64.0	93.1	68.1	97.1	**97.4**
CIFAR-100	64.3	93.8	69.3	97.3	**97.7**

表 2 不同网络体系结构下的性能提高(CIFAR-10,平均 ROC-AUC)

Table 2 Performance improvement under different network architectures (CIFAR-10, average ROC-AUC) %

Method	ResNet	EfficientNet	DenseNet	ViT
DN2	92.5	89.3	85.6	95.7
DSVDD	84.5	82.1	80.3	88.2
PANDA	96.2	95.3	82.4	95.8
MSC	97.2	97.0	95.7	98.6
本文模型	**97.4**	**98.0**	**97.7**	**98.8**

3.4 鲁棒性实验分析

为评估 DSVDD-ATWL 模型的稳健性,在保持其他所有超参数恒定的情况下,系统性地调整了关键参数 ν 的取值。实验设计基于 CIFAR-10 数据集,随机选取了其中 3 个具有代表性的类别(飞机、狗和船)进行详细分析。

实验结果如图 2 所示,展示了 ν 值变化时模型性能的变化趋势。AUC 指标波动幅度维持在 3%~5%之间,这表明 DSVDD-ATWL 对 ν 参数具有良好的鲁棒性。当 ν 值设置在 0.05~0.20 区间时,模型达到最佳性能平衡,此时正常样本的覆盖率和异常样本的排斥率实现最优权衡。

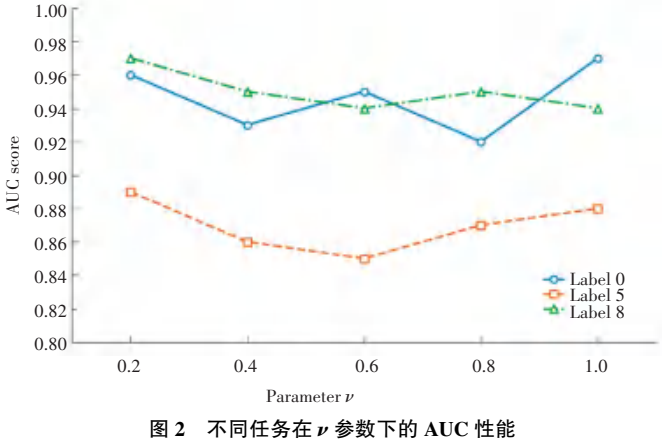


图 2 不同任务在 ν 参数下的 AUC 性能

Fig. 2 AUC performance under the ν parameter for different tasks

4 结束语

基于 DSVDD、对抗学习和紧密包裹学习的异常检测单阶段模型,通过创新的多机制融合与单阶段协同优化架构,在异常检测领域实现了理论方法的重要突破。该模型不仅克服了传统单一方法在处理高维复杂数据时的局限性,更通过双超球间隔最大化机制与对抗博弈策略,显著提升了特征表示的判别性与决策边界的精确性。

参考文献

[1] Aydogdu O, Ekinci M. A data stream-based approach for anomaly detection in surveillance videos [J]. Expert Systems with Applications, 2017, 79: 174-185.

[2] 彭鹏. 入侵检测技术在网络安全中的运用分析[J]. 网络安全技术与应用, 2025(1): 10-12.

[3] Karakose M, Yetis H, Cecen M. A new approach for effective medical deepfake detection in medical images[J]. IEEE Access, 2024, 12: 52205-52214.

[4] Huang K, Sun B, Wu S, et al. Metric learning-based fault diagnosis and anomaly detection for industrial data with intraclass

variance[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(1): 547-558.
[5] Tax D M, Duin R P. Support vector data description[J]. Machine Learning, 2004, 54: 45-66.
[6] Fei S, Yan M, Wang Y. MSFCLDNN: Local and global feature extraction methods for automatic modulation recognition[C]// Proceedings of 2025 International Conference on Communication Networks and Smart Systems Engineering. Piscataway, NJ: IEEE, 2025: 77-80.
[7] Lecun Y, Bengio Y, Hinton G. Deep learning[J]. Nature, 2015, 521(7553): 436-444.
[8] Huang S, Wang L, Wen X, et al. A satellite-terrestrial integrated network architecture based on stateless core network[C]// Proceedings of 2023 9th International Conference on Computer and Communications. Piscataway, NJ: IEEE, 2023: 390-395.
[9] Al-Tammie H K, Al-Anber N J. A comparative dimensionality reduction study in diabetes patients using LDA and PCA[C]// Proceedings of 2022 3rd Information Technology To Enhance E-learning and Other Application. Piscataway, NJ: IEEE, 2022: 170-175.
[10] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets[C]//Proceedings of Advances in Neural Information Processing Systems. Montréal, Canada: NeurIPS, 2014:2672-2680.
[11] 武阳, 刘靖. 面向图像分析领域的黑盒对抗攻击技术综述[J]. 计算机学报, 2024 ,47 (5) : 1138-1178.
[12] Schlegl T, Seeböck P, Waldstein S M, et al. f-AnoGAN: Fast unsupervised anomaly detection with generative adversarial networks[J]. Medical Image Analysis, 2019, 54: 30-44.
[13] Choi S, Choi J W. Noisy-Arcmix: Additive noisy angular margin loss combined with mixup for anomalous sound detection[C]// Proceedings of 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2024). Piscataway, NJ: IEEE, 2024: 516-520.
[14] Mohammed A B, Chaari F L, Fakhrudeen A M. Isolation forest algorithm against UAV's GPS spoofing attack[C]//Proceedings of 2024 IEEE International Conferences on Internet of Things and IEEE Green Computing & Communications and IEEE Cyber, Physical & Social Computing and IEEE Smart Data and IEEE Congress on Cybermatics. Piscataway, NJ: IEEE, 2024: 459-463.
[15] Schlachter P, Liao Y, Yang B. One-class feature learning using intra-class splitting[C]//Proceedings of 2019 27th European Signal Processing Conference. Piscataway, NJ: IEEE, 2019: 1-5.
[16] Jiang J, Kim D, Kim B, et al. GA-VAE: Enhancing local feature representation in VQ-VAE through genetic algorithm-based token optimization[J]. IEEE Access, 2025, 13: 34286-34295.
[17] Ruff L, Vandermeulen R, Goernitz N, et al. Deep one-class classification[C]//Proceedings of International Conference on Machine Learning. San Diego: PMLR, 2018: 4393-4402.
[18] Cao N, Luo Y. Application research of monitoring abnormal behavior analysis and detection method based on GANomaly network[C]//Proceedings of 2022 IEEE 2nd International Conference on Data Science and Computer Application. Piscataway, NJ: IEEE, 2022: 364-369.
[19] 杨国为, 万鸣华, 赖志辉, 等. 具有合适拒识机制的高正确识别率分类器设计[J]. 电子学报, 2021, 49(8): 1569-1576.
[20] Kong S, Ramanan D. OpenGAN: Open-set recognition via open data generation[C]//Proceedings of 2021 IEEE/CVF International Conference on Computer Vision. Piscataway, NJ: IEEE, 2021: 793-802.
[21] Bergmann L, Fauser P, Sattlegger D, et al. PANDA: Pathological image anomaly detection with adversarial learning[C]//Proceedings of the IEEE Winter Conference on Applications of Computer Vision. Piscataway, NJ: IEEE, 2021: 1023-1032.
[22] Reiss T, Hoshein Y. Mean-shifted contrastive loss for anomaly detection[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(2): 2155-2162.