

利用自动编码器进行异常检测的潜在矢量扩展

UJuGim公司 , 永亨公园

关键词：自动编码器、异常检测、深度学习

摘要

arXiv
:2201
.0141
6v1[c
s. CV]
2022
年1月
5日
深度学习方法可以将图像、语言和语音等各种非结构化数据分类为输入数据。随着对异常进行分类的任务在现实世界中变得越来越重要，存在各种使用深度学习对现实世界中收集的数据进行分类的方法。随着对异常进行分类的任务在现实世界中变得越来越重要，使用深度学习对现实世界中收集的数据进行分类的方法多种多样。在各种方法中，代表性方法是基于预训练模型的过渡模型提取和学习主要特征的方法，以及仅使用正常数据学习基于自动编码器的结构并通过阈值将其分类为异常的方法。然而，如果数据集不平衡，即使是最先进的模型也无法获得良好的性能。这可以通过将不平衡数据中的正常和异常特征增强为具有强烈区别的特征来解决。我们使用自动编码器的特性从低维到高维训练潜在向量。我们将正常和异常数据训练为在不平衡数据的特征之间具有强烈区别的特征。我们提出了一种潜在的矢量扩展自动编码器模型，该模型可以提高不平衡数据的分类性能。与使用不平衡异常数据集的基本自动编码器相比，所提出的方法显示了性能改进。

编码器从经过训练的自动编码器生成的潜在矢量。为了提取生成的潜在向量的正常和异常分类的强特征值，将低维扩展到高维。这通过强烈划分每个类的决策边界来提高分类性能。通过对不平衡异常数据集的实验，我们显示了比基本自动编码器性能的提高。

2相关工作

基本的自动编码器由编码器和解码器组成。通过通过编码器减小输入值的维数，该值被压缩成代表输入值的特征。之后，将降维潜在向量作为解码器的输入值，并恢复该向量以生成与编码器的输入值类似的值。基本自动编码器的目的是从编码器中的降维潜在向量训练有意义的数据。变分自动编码器在结构上类似于自动编码器，通过潜在向量表达输入数据中的概率分布[6]。之后，通过解码器生成数据。自动编码器和变分自动编码器之间的区别如下。自动编码器通过减少数据的维数来恢复减少的数据。相反，变分自动编码器是一种生成模型，在概率分布中生成相似的数据。我们使用自动编码器的原因是，它仅用于减少维度，而不是用于数据生成。与自动编码器的编码器相反，核心技巧是将数据的特征从低维扩展到高维，以区分每个类的边界确定[7]。支持向量机(SVM)[8]改进了输入数据从低维线性模型到高维模型的分类性能。内核技巧实际上并不扩展数据，而是通过扩展属性计算数据的标量积。我们通过爆炸性地扩展自动编码器的潜在向量的维数来解决分类问题，由于低维特征值的维数降低，难以分类。

1简介

如今，通过在现实世界中收集的数据集进行深度学习，各种非结构化数据中的图像分类[1, 2]和异常情况确定[3, 4]正在进行中。为了对图像进行分类并确定异常情况，收集数据并从收集的数据集中提取有意义的特征值。提取的重要特征值使机器能够识别数据集的输入数据。然而，存在一个问题，即即使在收集的数据中执行数据预处理，机器也无法识别正常和异常之间的差异，并且很难比较类之间的差异。为了克服这一限制，我们训练了一个自动编码器，只需简单改变基本自动编码器的结构即可[5]。正常和异常数据通过

3基于潜在矢量扩展的自动编码器

在本节中，我们提出了基于潜在向量扩展的自动编码器模型，这是本文提出的方法。?? 中的基本自动编码器(BA) ?? 显示基本自动

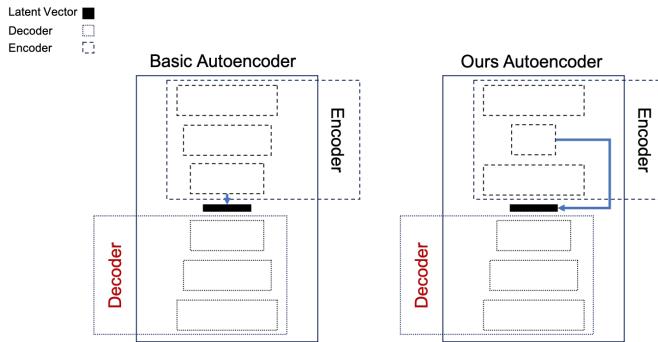


图1. 自动编码器结构比较

编码器和我们的自动编码器，在减小编码器的尺寸后通过解码器恢复。每一段都描述了我们的自动编码器和潜在向量扩展网络。我们展示了不同于BA的自动编码器。首先，我们将第一个线性层添加到自动编码器的编码器中，该编码器指定输入值数据的大小。第二层被设置为线性层，其与第一层的大小成比例地减小，并且输入和输出值相同。将ReLU激活功能添加到第一层和第二层。编码器的第三层将第二层的输出值设置为输入值，并将第一层的输入值设置为输出值。随后，解码器反转编码器的设置层的参数，然后将最后一层的激活函数设置为S形。我们采用了我们的方法，通过实验在第三层输出的基础上扩展了第二层的输出。表1显示了我们的出色性能，与通过BA结构生成的潜在向量相比，在减小每个输入数据的大小后，第三层中的输出值得到了扩展。线性模型的描述将在下一段，潜在向量扩展网络中给出。

表1. 自动编码器与AUROC的比较。
。方法AUROC线性模型w/BA0.87
2线性模型w/Ours0.951

其次，我们构建了一个潜在向量扩展网络，该网络从经过训练的自动编码器的编码器中训练潜在向量。该网络简单地由两个线性层和作为输出的线性模型组成。在将第一层的输入值设置为编码器的输出值之后，输出值将维度扩展到1024。之后，激活函数使用ReLU，并将丢失设置为0.5。此外，线性层被设置为将输出设置为1，用于正常和异常二进制分类，最终值通过logsigmoid输出。我们通过表2展示了1024维的性能。第4章提供了每个表的详细描述。

表2. 与AUROC的膨胀尺寸比较。方法扩展尺寸A
UROC

1280. 9692	560. 9685
0. 9691, 0240.	970

我们的扩展

4实验

在本章中，我们介绍了用于我们提出的基于潜在矢量扩展的自动编码器实验的数据集和预处理。之后，将描述表1、2和3中的每一个中使用的参数设置。实验使用了信用卡数据集，该数据集的主要目的是对欺诈行为进行分类。这是一个不平衡的数据集，在总共284807个数据中有492个异常，仅占约0.17%[9]。我们执行了最小-最大缩放以防止不平衡数据集的过度拟合，并通过K-Fold（交叉验证技术）进行了实验。对于实验中使用的所有模型，历元为20，学习率为0.001，优化器使用Adam，损失使用二进制交叉熵。不同的是，自动编码器使用Epoch50的均方误差和训练期间的损失。首先在表1中，w/BA和w/Ours在学习自动编码器之后将编码器潜在向量设置为线性模型的输入值。表2通过改变潜在向量扩展网络的第一层的扩展维度来进行实验。表3显示，每个模型在没有自动编码器的情况下通过K倍训练数据集的输入值进行实验。潜在向量可拓网络被用作线性模型。w/o展开将线性模型的第一层的展开尺寸更改为10，w/o膨胀将展开尺寸更改成1024，并进行了实验。

4. 1实验结果

在本章中，我们解释了表3和表4之间性能差异的原因。我们在表4中使用K-Fold展示了BA模型和我们的模型性能。与表3相比，表4与线性模型相比性能相对较差，但线性模型的输入值是基本数据，而不降低数据的维数。由于我们的模型是从经过训练的自动编码器的编码器中提取的数据，因此有两个优点。第一个是在学习模型时它可以是轻量级的，第二个是在进行推理时可以比基本数据更快。在表4中的模型比较中，与使用BA时相比，它在所有折叠中表现出优异的性能。因此，我们提出的基于潜在向量扩展的自动编码器和潜在向量扩展方法有助于提高性能。图2显示了2倍和2倍的PCA分析，显示了最佳性能，5倍和7倍显示了不好

表4中两个模型（左边是我们的，右边是图2中的BA）的性能。可以看出，模型甚至使用扩展潜在向量对数据分布不好的数据集进行分类。

表3. 线性模型无膨胀模型和膨胀模型的比较。

	线性模型	线性模型
	无扩展	无扩展
极光	10.9940.	10.99020.
极光	9950.99	9950.99
530.	9980.	99940.
	9350.	92750.
	.964	.97260.
	9860.	98770.
	9900.	99180
	.9700.	.97890.
	9830.	985100.
	9730.	981

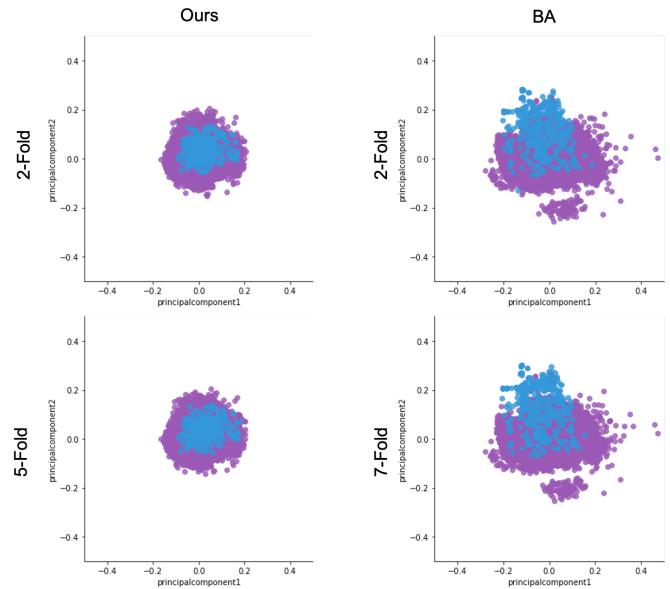


图2. BA模型和我们的模型PCA比较

5 结论

在本文中，我们提出了一种基于潜在向量扩展的自动编码器模型，该模型可以表明我们的方法优于基本的自动编码器结构和异常情况数据编码器。通过实验，所提出的模型表明，通过信用卡数据集，异常情况检测性能优于现有模型。我们将在未来对图像和各种数据集进行实验。

表4. BA模型和我们的模型性能比较。

	BA	我们
	w/ 扩展	w/ 扩展
极光	10.9390.	10.95720.
极光	9940.	9430.
96930.	8840.	93040.
	90150	8510.
	.8640.	89860.
	9190.	94570.
	.7900	92080.
	9230.	95490.
	.8840.	9101
00.	8470.	935

参考文献

[1] Y. LeCun、L. Bottou、Y. Bengio和P. Haffner，“基于梯度的学习应用于文档识别”，《IEEE学报》，第86卷，第11期，第2278–2324页，1998年。

[2] A. Krizhevsky, G. Hinton等人，“从微小图像中学习多层特征”，2009年。

[3] Y. Park、W. S. Park和Y. B. Kim，“使用假设剪枝生成对抗网络的颗粒物传感器异常检测”，《ETRI杂志》，2020年。

[4] W. Sultani、C. Chen和M. Shah，“监控视频中的真实世界异常检测”，《IEEE计算机视觉和模式识别会议论文集》，第6479 – 6488页，2018年。

[5] G. E. Hinton、S. Osindero和Y.-W. Teh，“深度信念网络的快速学习算法”，《神经计算》，第18卷，第7期，第1527 – 1554页，2006年。

[6] D. P. Kingma和M. Welling，“自动编码变分贝叶斯”，arXiv预印本arXiv:1312.6114v13。

[7] B. Scholkopf，“距离的核技巧”，《神经信息处理系统进展》，第301–307页，2001年。

[8] W. S. Noble，“什么是支持向量机？”，《自然生物技术》，第24卷，第12期，第1565–1567页，2006年。

[9] 年。LeBorgne和G. Bontempi，“信用卡欺诈检测实用手册的机器学习”，ACMS IGKDD探索通讯，第6卷，第1期，第1–6页，2004年。