



计算机工程与应用  
*Computer Engineering and Applications*  
ISSN 1002-8331, CN 11-2127/TP

## 《计算机工程与应用》网络首发论文

题目： 机器学习模型在车险欺诈检测的研究进展  
作者： 卢冰洁, 李炜卓, 那崇宁, 牛作尧, 陈奎  
网络首发日期： 2021-11-16  
引用格式： 卢冰洁, 李炜卓, 那崇宁, 牛作尧, 陈奎. 机器学习模型在车险欺诈检测的研究进展[J/OL]. 计算机工程与应用.  
<https://kns.cnki.net/kcms/detail/11.2127.TP.20211115.1252.010.html>



**网络首发：**在编辑部工作流程中，稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定，且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式（包括网络呈现版式）排版后的稿件，可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定；学术研究成果具有创新性、科学性和先进性，符合编辑部对刊文的录用要求，不存在学术不端行为及其他侵权行为；稿件内容应基本符合国家有关书刊编辑、出版的技术标准，正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性，录用定稿一经发布，不得修改论文题目、作者、机构名称和学术内容，只可基于编辑规范进行少量文字的修改。

**出版确认：**纸质期刊编辑部通过与《中国学术期刊（光盘版）》电子杂志社有限公司签约，在《中国学术期刊（网络版）》出版传播平台上创办与纸质期刊内容一致的网络版，以单篇或整期出版形式，在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊（网络版）》是国家新闻出版广电总局批准的网络连续型出版物（ISSN 2096-4188，CN 11-6037/Z），所以签约期刊的网络版上网络首发论文视为正式出版。

# 机器学习模型在车险欺诈检测的研究进展

卢冰洁<sup>1</sup>, 李炜卓<sup>2,4</sup>, 那崇宁<sup>1</sup>, 牛作尧<sup>3</sup>, 陈奎<sup>1</sup>

1. 之江实验室, 杭州 311121

2. 南京邮电大学现代邮政学院, 南京 210003

3. 东南大学苏州联合研究生院, 江苏 苏州 215123

4. 南京大学计算机软件新技术国家重点实验室, 南京 210093

**摘要:** 随着保险行业的蓬勃发展, 保险欺诈问题也显得日趋严重。车险欺诈一直是保险欺诈的“重灾区”, 对保险行业的发展至关重要。因此, 车险欺诈检测技术一直是国内外学者研究的热点问题。鉴于我国在机动车辆保险欺诈检测技术方相对滞后, 而国外的研究成果又较少对我国车险业务数据进行有效建模与分析, 本文首次针对机器学习模型在车险欺诈检测的研究工作进行了文献调研, 对二十多年来的研究工作进行系统化地归纳与总结。通过引入车险欺诈流程的简介, 对专家系统与机器学习模型在车险欺诈检测的流程进行了叙述; 然后依次从国外和国内的角度介绍了机器学习模型应用在车险欺诈检测的具体研究进展, 并进行了宏观的对比; 接着基于国内某车险公司提供近 5 年来高质量的车险数据选取具有代表性的机器学习模型进行建模, 并进行了全面地测试与分析; 最后, 探讨了车险欺诈检测技术未来的研究方向。

**关键词:** 汽车保险欺诈; 机器学习; 深度学习; 数据不均衡; 保险监管

**文献标志码:** A **中图分类号:** TP 391 **doi:** 10.3778/j.issn.1002-8331.2109-0312

## Auto Insurance Fraud Detection with Machine Learning Models: A Survey

LU Bingjie<sup>1</sup>, LI Weizhuo<sup>2,4</sup>, NA Chongning<sup>1</sup>, NIU Zuoyao<sup>3</sup>, CHEN Kui<sup>1</sup>

1. Zhejiang Lab, Hangzhou 311121

2. School of Modern Posts, Nanjing University of Posts and Telecommunications, Nanjing 210003

3. Southeast University - Monash University Joint Graduate School, Southeast University, Suzhou, Jiangsu 215123

4. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093

**Abstract:** With the vigorous development of the insurance industry, the problem of insurance fraud has become increasingly serious. Auto insurance fraud has been the hardest "hit area" of insurance fraud, which is very important for the development of insurance industry. Therefore, auto insurance fraud detection technology has been a hot top for researchers. Considered that the fraud detection techniques of automobiles in China have been lagged, and re-

**基金项目:** 国家自然科学基金青年科学基金项目“基于嵌入学习的不协调本体处理方法的研究”(62006125); 国家自然科学基金联合基金项目“面向大规模多源数据的人物画像和定位分析关键技术”(U1736204); 江苏省双创博士项目“中文移动应用知识库的构建、演化、应用的研究”(JSSCBS20210532); 南京邮电大学引进人才科研启动基金资助“大型生物医学本体修正技术的研究”(NY220171)。

**作者简介:** 卢冰洁(1996-), 女, 硕士, 之江实验室助理研究员, 研究方向: 金融科技、机器学习; 李炜卓(1989-), 男, 博士, 南京邮电大学讲师, CCF 普通会员, 研究方向: 知识图谱、自然语言处理, E-mail: liweizhuo@amss.ac.cn; 那崇宁(1980-), 男, 博士, 之江实验室高级研究员, 研究方向: 金融科技、人工智能; 牛作尧(1998-), 男, 硕士研究生, 研究方向: 知识图谱、自然语言处理; 陈奎(1989-), 男, 博士, 之江实验室副研究员, 研究方向: 金融风险、机器学习。

search results in aboard are not enough to model and analyze China's auto insurance business data, this paper present the first work on the survey of the methods of machine learning applied in auto insurance fraud detection, and systematically summarizes the related works in the two decades. We firstly give a brief introduction to the process of auto insurance fraud detection based on expert systems and machine learning models. Then, we describe the specific research progresses of machine learning models applied in auto insurance fraud detection at home and aboard. Moreover, with the high-quality auto insurance data provided by the insurance company in recent five years, we carry out a detailed comparison based on the representative models from machine learning and give a comprehensive analysis. Finally, the future research direction of auto insurance fraud detection is discussed and outlooked.

**Key words:** Auto insurance fraud; Machine learning; Deep learning; Unbalanced data; Insurance regulation

自改革开放以来,我国保险业取得了长足的发展。据 2021 年 4 月保监会发布的保险业发展报告,我国发展至 2020 年,共计 235 家保险公司,总资产达 23 万亿,保费收入 4.53 万亿元,同比增长 6.12%,成为了全球第二大保险市场。车险作为财产险中的第一大险种占比 69%,对保险行业的发展至关重要。然而,随着保险欺诈案件的频率和损失也逐年上升,保险欺诈的形势也日趋严峻。保守估计,我国车险欺诈渗漏占理赔金额的比例至少达 20%<sup>[1]</sup>。2020 年我国车险理赔支出合计约为 4725.50 亿元,照此推算,保险公司在车险欺诈方面的渗漏损失高达 900 亿元以上<sup>[2]</sup>。车险欺诈增加了保险公司运营成本和经营风险,侵害了保险消费者的合法权益,破坏车险市场秩序,同时也对他人财产及整个社会构成危害。为此,保监会于自 2018 年 2 月专门印发了《反保险欺诈指引》以指导保险公司和保险行业进行反欺诈制度建设。如何有效地识别车险欺诈对促进车险市场良性健康发展具有重要意义。

在我国保险欺诈领域,车险欺诈相比于其他险种的欺诈,存在犯罪手段隐蔽、手法多样,并逐渐呈现出团伙化的作案方式<sup>[2]</sup>。从近几年的数据可以发现,车险共同犯罪的比例存在明显的提升,且作案人员分工明确,这都给车险欺诈检测带来的不小的挑战。近年来,由各个国家监管部门与保险公司对车险欺诈的广泛关注,车险欺诈检测技术的研究取得了很大的进展。由于机器学习模型对原始数据的预处理要求比较低、因子间存在交互效应和非线性关系、具有预测能力较好等优点,目前已在车险损失预测中有了很多应用研究<sup>[3]</sup>。

保险欺诈案件检测问题可以抽象为一个二分类或者多分类问题,国内外均有不少学者将机器学习模型应用在车险欺诈检测技术上,并取得了较好

的研究成果。譬如,在国外, S. Viaene 等人<sup>[4]</sup>、Hanafizadeh 等人<sup>[5]</sup>、Kašćelan 等人<sup>[6]</sup>、Li 等人<sup>[7]</sup>分别探索了贝叶斯模型、聚类模型、数据挖掘、随机森林等技术对车险欺诈检测的效果; He 等人<sup>[8]</sup>、Guo 等人<sup>[9]</sup>、Wang 等人<sup>[10]</sup>等人则进一步探索了深度学习模型在该任务上的应用价值; Subudhi 等人<sup>[11]</sup>、Majhi 等人<sup>[12]</sup>则从混合模型的角度进行切入,对其进行了有效的建模。相应的,国内学者虞国柱等人<sup>[13]</sup>、刘喜华等<sup>[14]</sup>最早开始从车险的理论进行了探究; 桂萍等人<sup>[15]</sup>收集了大量国内外车险道德风险文献,并在此基础上进行归纳梳理。赵桂芹等人<sup>[16]</sup>、汤俊等人<sup>[17]</sup>、王海巍等人<sup>[18]</sup>则对根据国内的车险欺诈的实际情况,应用传统机器学习模型对其进行建模。近些年,闫春等人<sup>[19]</sup>、喻炜等人<sup>[1]</sup>、徐徐等人<sup>[20]</sup>也从开始从深度学习网络、混合模型的角度出发,在车险欺诈检测任务上取得了较大的进展。此外,车险欺诈领域具有其独特的挑战性。比如:车险欺诈的特征空间庞大,特征之间往往有着复杂的依赖关系,而传统机器学习往往需要进行特征选择。针对这个问题, Panigrahi 等人<sup>[21]</sup>采用了三种特征选择算法,提取车险欺诈数据中的重要特征,并利用机器学习算法进行检测,从而挑选出不同机器学习模型的最佳特征选择方法。另一方面,车险欺诈相对于信用卡欺诈等常见形式发生概率更低,因此类别不平衡现象更为明显<sup>[22]</sup>。为此, Hassan 等人<sup>[23]</sup>、Padhi 等人<sup>[24]</sup>分别使用了欠采样、过采样等策略来缓解车险欺诈任务所存在的挑战。

然而,尽管已有上述的诸多车险欺诈检测的研究工作,并且取得了较为显著的进展,但缺乏基于机器学习模型对车险欺诈检测进行系统深入地梳理与总结的工作,特别是近些年深度学习工作方法在车险欺诈检测研究上的进展。一方面,国内在车辆

保险欺诈检测技术方相对滞后,模型实验所采用的车险欺诈数据较为陈旧,且部分来自国外早期开源的数据进行模拟。另一方面,国外的研究成果又较少对我国车险业务数据进行关注,无法适配目前国内车险行业拟定的规范,因此无法较好的进行建模。

为此,本文首次针对机器学习模型在车险欺诈检测的研究工作进行了文献调研。具体地说,本文首先给出车险欺诈流程的简介,对专家系统与机器学习模型在车险欺诈检测的流程进行了简要地叙述。然后对二十多年来的研究工作进行系统化地归纳与总结,依次从国外和国内的角度介绍了机器学习模型在车险欺诈检测的具体研究进展,将其归纳为基于传统机器学习方法、基于神经网络的方法以及基于混合模型的方法,并进行了宏观的对比。接着基于国内某车险公司提供近5年来高质量的车险数据选取最具代表性的机器学习模型进行建模,并进行了全面的测试与分析。最后,对全文进行总结并展望车险欺诈技术未来的研究方向。

## 1 车险欺诈检测流程简介

本节将分别从车险专家系统与智能理赔系统两个角度来介绍车型欺诈检测的流程。

车险专家系统(下称专家系统)是一种基于车险领域知识的推理系统,具体来说,它能够利用车险专家的经验知识进行决策,由此判定案件的性质以达到预警的目的<sup>[25]</sup>。专家系统的特点在于其基于规则和推理,这使得它具备了良好的可解释性。但相对的,一旦规则触发的条件不充足或者得不到满足时,专家系统就很难得出有用的结果。倘若欺诈方对规则有所了解,就可以在犯罪过程中绕过这些规则的触发条件来规避专家系统的检测。因此,专家系统在欺诈检测的精度和准确度上都有所局限。

目前,专家系统在车险欺诈检测中依然有着广泛的应用。通常来说,当车险案件进入核价核损阶段时,案件数据将通过接口传输到专家系统中进行检测。如图1所示,数据进入专家系统后首先根据数据类型进行分类,随后根据数据类别采取相应的计算准则,计算得到案件触发的风险因子集合,接着,将该案件触发的风险因子集合与规则的触发条件进行一一匹配,最终得到案件的反欺诈判别结果和触发的欺诈规则集合,并提示该案件最终的欺诈风险等级。

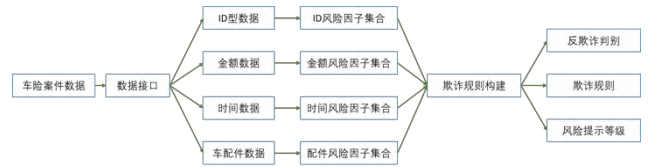


图1 专家系统车险欺诈检测流程图

Fig.1 The diagram of expert system for auto insurance fraud detection

随机人工智能技术的发展,基于大数据的机器学习技术能够突破传统专家系统的局限,通过对被保险人、保险标的、出险情况等各方面数据进行收集和分析,为车险理赔提供了调查的方向。图2展示了构建智能理赔系统地5个步骤,包含数据需求、数据清洗、特征工程、超参调优以及模型训练。

(1) 数据需求:根据车险业务场景提出数据需求,构建原始数据库。通常情况下,原始数据库中应包含报案、查勘、立案、定损、核价核损等多个重要各环节数据;

(2) 数据清洗:处理原始数据中可能存在的数据重复、数据格式不规范以及字段数据大量缺失等问题,并聚合清洗后的数据,将数据汇总至一张表中,形成结构化数据库;

(3) 特征工程:采用手动/自动特征工程的方法处理结构化数据,包含时间类型数据处理、经纬度数据处理、离散型变量处理、特征交叉和选择等等,最终生成统计学特征库;

(4) 超参调优:基于标注好的训练数据,通过手动/自动超参优化方法优化机器学习模型参数,得到模型最优超参数设置;

(5) 模型训练:采用最优超参训练模型,获得最优模型。需要注意的是,为了保证智能理赔系统的性能,在模型上线后,往往需要保持增量训练或定期更新模型。

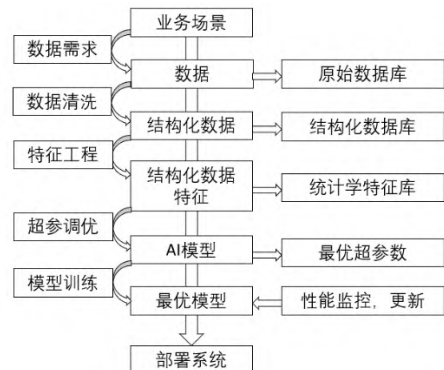


图2 智能理赔系统车险欺诈检测流程图

Fig.2 The diagram of intelligent claim system for auto insurance fraud detection

## 2 机器学习模型在车险欺诈检测的研究进展及评述

### 2.1 国外研究进展

#### 2.1.1 基于传统机器学习的方法

国外早期研究主要采用了一些传统的机器学习方法，目标是在车险欺诈检测数据中筛选出若干数据特征，从而根据这些特征构建车险欺诈检测的分类模型。

**基于贝叶斯模型**的主要思路是利用贝叶斯分类的影响因子独立假设思想来根据保险欺诈的因素来构建分类器，最终推理得到保险欺诈的分类概率。基于该思想，S. Viaene 等人<sup>[4]</sup>探索了具有自动确定相关性 (Automatic Relevance Determination, ARD) 权重正则化项的神经网络分类器的显式能力，并将该网络应用于汽车保险索赔欺诈检测。该方案使用了一种基于贝叶斯学习的证据框架来实现 ARD，从而确定每个输入的相对重要性，并剔除冗余特征。此外，作者通过和流行的 Logistic 和决策树算法得出的输入相对重要性进行了比较，认为不同分类器具有互补的可能性，这符合现代贝叶斯学习在数据量有限时选择模型的方法。Bermúdez 等人<sup>[26]</sup>将非对称链接函数的思想应用到保险欺诈领域，使用了一种有偏连接模型，假设模型参数服从某种先验分布进而通过贝叶斯估计和 Gibbs 采样来拟合。同时，作者在一个西班牙保险数据集上进行了实验，验证了该方法能显著提高了保险欺诈检测的准确率。贝叶斯模型的局限性在于车险欺诈检测的特征通常具有复杂的关系，而无法满足相互独立的假设。此外，贝叶斯模型预测概率不够精确，往往只用于定性分析的特征选择过程。

**基于聚类模型**的主要思路是根据若干风险因素对车险案例进行划分，并得到可疑车险欺诈案例。基于该思想，Hanafizadeh 等人<sup>[5]</sup>基于自组织映射和 K-Means 算法，提出了一种基于新颖的两阶段车险客户细分模型。在第一阶段，作者从文献综述中提取了人口统计学规范、汽车规范、政策规范和驾驶

员记录四类 18 种不同的风险因素。在第二阶段，作者进一步利用专家意见来确定筛选过程。通过实证分析，作者发现保险公司的客户在很多方面都有所不同，而数据分析表明了基于历史数据和专家意见的最终选定因素对于区分客户的重要性。K-Means 算法的性能取决于聚类簇的数量以及划分标准，在特征空间较大的情况下开销较大，因此在车险欺诈领域中应用依赖专家意见和人工筛选特征等过程。

**基于数据挖掘**的主要思路是从大量数据中找出隐藏的信息，主要通过统计学、模式识别等方法来进行有用信息地提炼。基于该思想，Rekha<sup>[27]</sup>分别提出了基于朴素贝叶斯，决策树以及产生式规则的欺诈检测方法，并借助可视化工具从实际车险数据中分析存在道德风险的可能性。同时，作者通过实证分析发现混淆矩阵具有很强的类倾斜性，成为了许多重要的欺诈检测领域的可靠性能指标。Kaščelan 等人<sup>[6]</sup>基于数据挖掘技术挖掘处现存风险和风险因子之间的功能依赖关系，继而帮助保险人评估风险和计算适当的保费。同时，作者通过实例分析验证了数据挖掘技术同样可以准确地预测索赔的规模和发生情况，从而为保费计算和风险分类提供了依据。在实例分析的过程，作者指出数据质量和合适的数据挖掘技术是该方法成功的前提条件。Yan 等人<sup>[28]</sup>研究了数据挖掘技术在反车险欺诈中的应用。将基于规则剪枝的最近离群点检测方法应用于车险欺诈领域，建立了改进的车险欺诈识别模型，利用关联规则挖掘车险欺诈规律。实验结果表明，改进后的车险欺诈识别算法具有时间复杂度低、识别率高、准确率高、对聚类算法 K 值影响小等优点。Mihaela<sup>[29]</sup>通过对投保人年龄变量进行显著性分析，得出高欺诈风险人群特征。具体的，作者基于五个年龄区间构建了保费计算的负二项分布模型。在利用似然比对检验了泊松分布等假设后，试验结果表明负二项分布模型能更好地拟合数据，缓解保险组合中存在的过度分散现象。Nian 等人<sup>[30]</sup>基于异常点检测的方法，提出了一种基于谱排序的异常保险样本检测方法，并发现谱优化问题可以解

释为一个无监督支持向量机问题。作者通过利用拉普拉斯矩阵的非主特征向量来直接推导排序向量，从而找出异常的欺诈样本。同时，作者基于一个真实索赔数据集进行了实证分析。通过将该问题建模为无监督学习，基于海明距离及其核函数来生成该数据集的谱排序，并取得了良好的性能，此外，作者也表明为欺诈检测问题选择适当的相似度的重要性。数据挖掘方法的特点是基于数据进行统计学分析，再利用机器学习模型实现车险欺诈检测的具体任务。因此，数据质量，统计建模以及模型选择等过程都会影响最终的预测结果。

基于 **K 近邻算法** 的主要思路是给定车险欺诈数据的训练集，当新输入样本时分析该样本的最相似的  $K$  个实例，也就是  $K$  近邻的类别，把出现次数最多的类别作为新输入样本的类别。Badriyah 等人<sup>[31]</sup> 采用最近邻法和四分位数法检测车险数据中的欺诈行为。从实验结果来看，使用特征选择会提高检测欺诈的性能。具体的，作者采用基于距离的遗传算法进行特征选择，利用最近邻法进行欺诈检测。 $K$  近邻法应用于车险欺诈检测仍有较大的局限性， $K$  比较小时对噪声数据非常敏感，容易过拟合； $K$  比较大时，由于每个新输入数据作分类时都要遍历整个数据集，会造成巨大开销。

基于**回归模型**的主要思路是利用统计分析方法模拟风险因素的关系，继而得到保险欺诈因素之间的线性关系。Yan 等人<sup>[32]</sup>提出了一种基于人工蜂群算法(ABC, Artificial bee colony)的核岭回归算法(Kernel ridge regression, KRR), KRR-ABC, 用于汽车保险欺诈检测。具体的，作者利用 ABC 算法的全局优化能力和良好的并行性对 KRR 的参数组合进行优化，提高了模型的泛化能力和计算速度。同时作者在 8 个基准数据集上对 KRR-ABC 模型的性能进行了测试，结果表明 KRR-ABC 模型具有更快的运行时间和更好的生成性能。将 KRR-ABC 模型应用于汽车保险欺诈检测，得到了欺诈规则。由于逻辑回归模型只能进行线性拟合，而且对变量相关性敏感，因此无法直接用于真实车险欺诈数据的检测，往往用来进行特征选择。

基于**随机森林模型**的主要思路是利用集成学习泛化性能强的优势来进行分类器之间的组合，以此来提升保险欺诈的判别效果。基于该思想，Xu 等人<sup>[33]</sup>提出了一种基于随机粗糙子空间的神经网络集成方法用于保险欺诈检测。该方法利用粗糙集划分的子集分别基于真实保险数据训练一个神经网络分类器，并利用集成策略将训练好的神经网络分类器进行组合。为了验证该方法的有效性，作者进行了实证分析。实验结果表明，作者提出的集成模型优于单个分类器和其他模型，能够快速准确地发现可疑的保险欺诈行为。Li 等人<sup>[7]</sup>从潜在最近邻的角度分析了随机森林的分类机制，用基于潜在最近邻的投票机制取代了多数投票机制，避免了出袋(out of bag, OOB)样本造成的信息丢失。在此基础上，提出了主成分分析转换方法，将数据转换到主成分分析空间，提高分类器的多样性，从而提高随机森林算法的整体分类精度。虽然随机森林无须进行特征选择也可以获得较强的拟合能力，但是组合分类器给模型建立和预测增加了代价。此外，随机森林的参数较传统机器学习更多，不易调节。

基于 **XGBoost** 的方法同样属于集成学习，但它不同于随机森林的弱分类器之间相对独立的关系，XGBoost 算法以提升树为原理，模型的预测结果受上一次预测结果的影响。因此相比随机森林有较差的并行性。然而，XGBoost 的整体效率高于使用多棵树进行预测的随机森林。此外，XGBoost 可以用于对连续型欺诈数据进行回归分析，而随机森林模型只能用于分类任务。Dhieb 等人<sup>[34]</sup>将 XGBoost 应用于车险欺诈检测的批量学习，该算法不仅具有优越的计算速度和模型性能，还能解决跨学科问题。此外作者利用快速决策树(VFDT)实现在线学习，该策略在新数据进入系统时动态地调整参数，而不需要重新训练整个模型。

基于传统机器学习方法均是先采用特征工程的方式来筛选对保险或者车险欺诈的敏感特征，随后以各类机器学习模型为基础进行有效地改进，从而达到更好的检测结果。然而，上述方法仍会存在数据转换适应性方面的问题。同时，传统方法不易

挖掘出汽车保险数据中隐藏的特征及其关联。

### 2.1.2 基于神经网络的方法

基于神经网络的车险欺诈检测方法主要集中在浅层神经网络、图神经网络以及深度学习。目前,国外相关研究工作主要聚焦在图神经网络与深度学习这两种类型。

**基于图神经网络**的主要思路是利用图结构可以更好的表示车险欺诈中多方主体之间的关系,并发现潜在的组织行为。基于该思想, Liang 等人<sup>[35]</sup>在索赔者之间引入了一个设备共享网络,然后开发了一个基于图学习算法的欺诈检测自动化解决方案,以将诈骗者从常规客户中分离出来,并发现有组织的诈骗者群体。作者介绍了三种类型的图,并展示了它们通过图神经网络区分欺诈和正常行为的优势。经过人类专家调查,与之前部署的基于规则的分类器相比,该解决方案的准确率超过 80%,可疑账户覆盖率增加 44%。此外该模型可以简单有效的推广到其他类型的保险。Liu 等人<sup>[36]</sup>针对欺诈者产生的不一致问题,即上下文不一致、特征不一致和关系不一致,设计了一个新颖的图神经框架 GraphConsis,并分别设计了三种模块来解决不同的不一致性问题。具体来说:1)对于上下文不一致性,将上下文嵌入与节点特征相结合;2)对于特征不一致性,设计了一致性评分来过滤不一致的邻域并产生相应的采样概率;3)对于关系不一致性,学习与抽样节点相关的关系注意权值。实验分析表明,各种模块所针对的不一致性问题在欺诈检测任务中扮演着至关重要的角色。图神经网络适合构建元素之间具有复杂拓扑关系的模型,车险欺诈中往往涉及多方主体,因此引入该方法可以学习到多方主体之间的潜在关系,从而用于预测。然而,图神经网络目前还不能保证收敛点的质量和实际预测效果。

**基于深度学习**的主要思路是利用深度学习的网络深度优势与对深度框架的改了来提高汽车保险欺诈的推理效果。基于此思想, Qu 等人<sup>[37]</sup>提出了一种基于点积的神经网络(PNN),该神经网络通过嵌入层来学习分类数据的分布式表示,然后通过

点积层来捕获域间类别之间的交互模式,进一步利用全连接层来探索高阶特征交互。Cheng 等人<sup>[38]</sup>提出了深浅层学习框架(Wide & deep learning, WDL),通过联合训练浅层线性模型和深度神经网络,将其记忆和泛化功能结合起来用于推荐系统。他们在 Google Play 上制作并评估了这个系统。在线实验结果显示,应用 WDL 比单独的浅层和深度模型显著增加了 APP 应用的购买量。Xiao 等人<sup>[39]</sup>通过区分不同特征交互的重要性来改进 FM。他们提出了一种新的模型,称为注意力因子分解机(AFM),该模型通过神经网络从数据中学习每个特征交互的重要性。在两个真实数据集上的大量实验证明了 AFM 的有效性。Wang 等人<sup>[40]</sup>提出了深度交叉网络(DCN)保留了深度神经网络(DNN)的优点,并引入了一种新颖的交叉网络,在学习某些有界度特征交互时更有效。特别地,DCN 显式地在每一层应用特征交叉,不需要手动进行特征工程,并且增加的复杂度可以忽略不计。实验结果表明,在点击率预测数据集和密集分类数据集上,该算法在模型精度和内存使用方面均优于现有的算法。Guo 等人<sup>[41]</sup>证明了可以推导出一个同时强调低阶和高阶特征交互的端到端学习模型 DeepFM。在新的神经网络架构中,DeepFM 结合了分解机制和深度学习的能力分别用于推荐和特征学习。与深度学习模型 Wide&Deep 相比,DeepFM 有一个共享的输入分别传输到浅层和深层,可以直接利用原始特征不需要特征工程。同时作者在基准数据和商业数据上进行了综合实验,验证了 DeepFM 对点击率预测的有效性。尽管上述模型只是深度学习模型在推荐任务上的应用,但两者关联非常紧密,可以将上述模型根据车险欺诈检测任务进行适配,并得到较为理想的效果(见 4.2 节测试模型与结果分析)。

近年来,由于深度学习模型无须进行繁琐的特征选择,并能够捕获文本中的特征之间隐藏的语义关系,不少学者开始将深度学习应用于车险欺诈检测,通过大量实证分析,深度学习模型往往优于传统机器学习模型。He 等人<sup>[8]</sup>提出了一种用于稀疏预测的神经因子分解机(NFM)模型。NFM 巧妙地结合

了因子分解机(FM)在建模二阶特征交互中的线性和神经网络在建模高阶特征交互中的非线性。具体的说,作者通过添加隐藏层获得比 FM 更强的性能。相较于深度学习方法 Wide&Deep 和 DeepCross 而言, NFM 使用了更浅的结构并保证了其性能,因此在实践中更容易训练和调整。Guo 等人<sup>[9]</sup>提出了一种基于历史注意的交互式 LSTM (HAIInt-LSTM)循环神经网络来学习序列行为表示以进行欺诈检测。作者利用历史自注意模块解释了人类行为的周期性,并通过将源信息编码为一个交互模块,以增强行为序列的学习。通过结合历史自注意模块和交互模块, HAIInt- LSTM 在欺诈检测的序列行为表示学习、序列预测和序列分类等方面都取得了良好的性能。同时,作者在车险欺诈数据集上证明了该方法在欺诈检测任务上的优越性。Wang 等人<sup>[10]</sup>提出了一种结合潜在狄利克雷分布(Latent Dirichlet Allocation, LDA)和深度学习的文本分析模型,并用于车险欺诈检测。该方法首先利用 LDA 提取事故索赔文本描述中隐藏的文本特征,利用深度神经网络训练文本特征和传统的数字特征。实验结果表明,深度神经网络的性能优于随机森林和支持向量机等广泛使用的机器学习模型。

基于神经网络方法更多是利用了神经网络的较大的特征学习能力。不过,目前特征的选取仍是通过聚类、LDA 无监督方式来进行训练筛选,并未涉及到端到端的模式。此外,基于深度学习的方法普遍依赖于大量训练数据,不利于小样本场景下的表示学习问题。特别是在车险欺诈领域,公开的有标签数据难以轻易获得,而标注任务也需要相当的专业知识。最近已经有学者将无监督深度学习用于保险欺诈检测,从而缓解数据对该任务的影响。Gomes 等人<sup>[42]</sup>提出的方法结合无监督深度学习模型变分自编码器(VAE)和自编码器(AE)的能力,通过点击按钮进行周期性模型更新,持续学习用户行为的复杂变化。目前无监督深度学习方法分类精度有限,将更多应用于检测结果的质量评估、相似欺诈案例的推荐等场景。

### 2.1.3 基于混合模型的方法

目前基于混合模型的方法主要集中在将多个模型组合形成的系统框架,国外相关研究工作主要包括基于内在关联属性的方法以及其他的混合模型方法两种类型。

**基于内在关联属性**的主要思路是从实体因素之间的关系来进行建模,继而利用因素之间的网络关联来进行保险欺诈工作。基于该思想, Lovro 等人<sup>[25]</sup>提出了一种车险欺诈群体检测的专家系统,并对该系统进行了详细的描述和评估,同时考虑了检测欺诈的几个技术难点,以使其在实践中适用。与其他方法不同的是,该系统使用网络来表示数据,刻画和分析了实体之间的复杂关系。此外,作者还提出了一种新颖的迭代评估算法 IAA(iterative evaluation algorithm)来发现虚假实体。该算法除了研究实体的内在属性外,还研究了实体之间的关系,并根据真实世界数据进行了严格分析。结果表明,该系统在良好的数据表示的前提下,能够有效地检测出汽车保险欺诈行为。

**其他混合模型算法**的主要思路是将各个方法的优势进行融合。基于此思想, Subudhi 等人<sup>[11]</sup>提出的车险欺诈检测系统为训练和欺诈检测两阶段。在训练阶段,结合遗传算法和模糊 c 聚类方法,在大多数类实例上生成具有最优集群中心的集群,从而识别出异常值和冗余数据点并删除,最终得到一个平衡的数据集,用于进一步的实验。在第二阶段对可疑样本进行验证,分别由四种不同的有监督学习方法 DT、SVM、MLP 和 GMDH 进行验证。作者在一个真实的汽车保险数据集上进行了实验,验证了该系统的有效性。Majhi 等人<sup>[12]</sup>采用模糊 c 均值聚类方法进行聚类,并通过改进的鲸优化算法寻找给定数据集的全局最优解,进而提出了一个基于模糊聚类的保险欺诈检测系统。该方法首先采用模糊聚类方法去除离群点,对大部分样本数据集进行裁剪,然后使用 CATBoost、决策树等先进的分类器对修改后的数据集进行分类。通过测量灵敏度、特异性和准确性等性能参数对分类器进行评价。

总的来说,国外对于保险欺诈检测领域的研究



多采用组合分类器(如: 随机森林),或较为前沿的深度学习模型(如: 长短期记忆网络(LSTM)、图神经网络(GNN)。通过实证分析来进行模型的评价与改善, 往往模型都能够达到较高的准确率与较强的泛化能力。从数据集的角度来看, 这得益于国外的保险索赔数据具有更丰富的评价指标体系, 从而为模型训练特征的选取提供了更多的保障。

## 2.2 国内研究进展

### 2.2.1 基于传统机器学习的方法

随着国内保险事业的兴趣, 国内越来越多的学者也参与到保险欺诈与车险欺诈的研究中来。与国外类型, 国内学者早期仍以回归模型、聚类分析、数据挖掘等技术为主。

**基于回归模型**的主要思路是利用逻辑回归模型模拟风险因素的关系, 继而得到保险欺诈与其他因素之间的关联关系。基于该思想, 赵桂芹等人<sup>[16]</sup>为了探究车险市场中是否存在道德风险, 作者首次采用动态续保数据进行实证研究。通过使用逻辑回归的参数方法和条件相关模型的非参数方法, 从多个方面论证了道德风险存在的范围, 并发现了道德风险在不同投保人群中具有不同显著性的现象。此外, 作者再次验证了信息不对称的广泛性和显著性给道德风险带来的影响。张连增等人<sup>[43]</sup>基于国外保险索赔数据, 通过逻辑回归模型分析了车险索赔的影响因素, 并利用 SAS 软件对实验结果进行统计分析, 得出汽车价值、地区、车型和驾驶员年龄都会影响车险索赔发生概率, 并预测了概率数值。此外作者考虑到风险暴露对车险索赔造成的影响, 通过引入风险暴露因子对模型进行了优化, 从而扩展了逻辑模型在保险业的应用。

**基于聚类模型**的主要思路是根据若干风险因素对车险案例进行划分, 并得到可疑欺诈案例。基于该思想, 王海巍等人<sup>[18]</sup>利用一个保险运营的动态数据流, 通过对投保、承保、理赔等关键环节的数据字段进行聚类分析, 并建立数理模型观测、估计

保险欺诈风险阈值, 探索了保险实务中的道德风险识别问题。同时, 作者基于实证分析提出了建立动态 Hadoop 模型进行风险因子聚类分析的必要性。

**基于数据挖掘**的主要思路是从大量数据中找出隐藏的信息, 主要通过统计学、模式识别、大数据分析等方法对保险数据中特征关联进行提炼。基于该思想, 汤俊等人<sup>[17]</sup>基于支持向量机和 Apriori 算法的数据挖掘技术, 提出了一种新颖的车险欺诈检测规则挖掘方法。具体的说, 作者利用 Apriori 算法挖掘到的规则构造了一个欺诈规律知识库, 用于对支持向量机从历史数据库汇总挖掘出来的可疑案例进行再检验, 从而提高车险欺诈检验的准确性。此外, 作者建议周期性的对知识库中的规则进行维护更新以应对不断变化的车险欺诈行为。袁幕琴等人<sup>[44]</sup>基于我国保险欺诈的现状和主要表现形式, 对保险欺诈的原因和危害进行了定性的分析研究工作, 并结合大数据等现代信息技术提出了高效防范保险欺诈的对策建议, 包括建设智能反欺诈模型、大数据分析优化承保、理赔规程等。卢文龙等人<sup>[45]</sup>基于保险欺诈案件的风险因子和大数据技术, 提出了一个闭环式的保险欺诈循环处理系统, 通过提炼出的风险因子建立数理识别模型, 再将识别结果反馈来更新风险因子, 从而构建出一个越来越完善的反欺诈模型。张澄等人<sup>[46]</sup>结合保险业个性化、定制化的发展趋势, 使用大数据分析和“互联网+”技术实现风险管理的精细化和产品服务的定制化。具体的说, 作者从位置大数据应用的角度出发, 对手机定位的车辆位置信息在车险管理的应用问题进行探讨, 并提出了一种新颖的地理区域网格化方法用于风险划分和计算。同时, 作者针对生产应用中的承包端和理赔端分别给出模型实施路径和使用建议。

### 2.2.2 基于神经网络的方法

相比于国外学者集中在浅层神经网络、图神经网络以及深度学习领域, 国内相关研究工作主要集中在浅层神经网络。

**基于浅层神经网络**的主要思路是利用前馈神

神经网络来学习各个欺诈因素的权重,以此来提高保险欺诈的推理效果。基于此思想,叶明华<sup>[47]</sup>以保险欺诈行为中的车险索赔为例,对基于反向传播神经网络(BP 神经网络)用于保证欺诈识别的有效性进行验证。作者将欺诈识别分为统计回归混合人工智能两个阶段,利用逻辑回归分析选出显著性指标作为精炼变量来进行训练的 BP 神经网络模型。通过实验验证了 BP 神经网络和统计回归方法融合的效果。通过实验结果验证了经过融合后方法的识别准确率要高于单独使用 BP 神经网络识别的结果,从而证明了统计回归与 BP 神经网络具有互补性和相互交错性的理论。因此,作者指出提高神经网络识别效果的前提是完善索赔指标体系。为了克服 BP 神经网络容易陷入局部最优、收敛速度慢而且依赖样本等局限性,闫春等人<sup>[48]</sup>利用改进的遗传算法来优化基于 BP 神经网络的车险欺诈识别模型。首先通过主成分分析将某保险公司的欺诈索赔数据进行指标的提炼,将提炼后的指标用于模型欺诈预测。改进的遗传算法通过自适应调节交叉概率与变异概率,进一步提高了遗传算法的寻优能力,防止算法陷入局部最优。作者在实证分析中发现,改进的遗传算法和经典遗传算法 GA 和 IAGA 算法相比,取得了收敛速度、精准度等评价指标的性能提升。

近年来,少数学者开始尝试利用深度学习技术构建车险欺诈检测模型,相比浅层神经网络方法在效果上有明显改善。徐徐等人<sup>[20]</sup>基于深度学习构建了一个车险欺诈识别模型。具体的说,作者基于采样思想来转换生产不平衡数据集,同时采用主成分分析算法对车险数据进行降维处理并消除变量之间的相关性。通过实证分析,作者验证了深度学习模型相比传统机器学习模型在欺诈识别领域取得更好的效果。

### 2.2.3 基于混合模型的方法

基于混合模型目前主要集中在将多个模型组合形成的系统框架,国内相关研究工作体现在基于内在关联属性以及其他的混合模型两种类型。

基于内在关联属性的主要思路是从实体因素

之间的关系来进行建模,继而利用因素之间的网络关联来进行保险欺诈工作。基于该思想,赵长利等人<sup>[49]</sup>基于变分不等式理论和变步长投影算法,探索了投保人、保险人和保险监管者三方主体在车险行为中的最优均衡模式。不同于常规模型在探究此类问题上的局限性,本文构建的风险控制闭环模型能够以定量的方式分析各方主体的决策行为和利益关系。通过数据分析,作者发现了汽车网络利润不均衡的特点,进而提出给予各方参与者一定的利润空间以实现各方利润最大化和风险控制。喻炜等人<sup>[1]</sup>针对车险欺诈检测问题,首次在该领域引入了团伙微观建模的概念,利用矩阵运算识别出可疑的车险欺诈团伙行为。同时,将可疑欺诈团伙的碰撞网络矩阵映射为人的网络关系,从而识别出人为规避行为。相比传统方法,矩阵数值运算省略了样本预处理、模型训练等步骤,极大提高了计算效率。

其他混合模型算法的主要思路是将各个方法的优势进行融合。基于此思想,闫春等人<sup>[19]</sup>提出了一种基于蚁群算法和随机森林模型的组合分类器来提取出用于车险欺诈识别的一组特征。作者用平衡随机森林算法可来改善车险索赔数据的不平衡性,然后将特征在随机森林中的重要性得分与数据的统计分数传递给蚁群算法实现信息素实时更新,从而准确地提取出车险欺诈特征。和传统算法相比,该方法提高了车险欺诈识别的准确性与鲁棒性。

总的来说,国内的车险欺诈检测方法更倾向于使用传统机器学习模型,如逻辑回归、BP 神经网络,并利用数据挖掘等技术建立统计模型,在深度学习与集成学习方面的研究并不突出。这可能是因为国内的风险评价体系尚未健全,很多学者利用爬虫技术自行收集的数据量级比较小,且数据中含有大量的噪音,导致数据质量不高,因此无法满足在一定程度满足深度学习训练条件,这大大制约了国内保险欺诈识别的性能和应用场景。

## 2.3 模型评述

在这一小节中,将常用的机器学习模型及其特

点总结,如表 1 所示,其中贝叶斯分类中的  $C$  表示类别,  $x$  表示样本特征。逻辑回归模型中的  $w$  表示样本权重,  $b$  表示偏置。决策树模型通过计算信息增益  $Info(D)$  依次选择分类效果最好的属性,其中的  $i$  表示类别,  $D$  表示样本集合,  $P_i$  表示  $D$  中任意一个样本属于  $i$  的概率。 $K$  近邻中的函数  $I()$  根据括号中的参数是否相等返回 1 或 0。另外,公式中出现的  $sign(.)$  函数的作用是根据参数和阈值的大小关系返回相应类别,  $\sigma(.)$  函数称为激活函数,和  $sign(.)$  函数的作用类似,区别是  $sign(.)$  函数的取值是离散的,而激活函数  $\sigma(.)$  的取值是连续值。集成学习中的  $h(x)$  表示弱分类器预测结果,  $H(x)$  综合这些结果得到强分类器的结果。除此以外,公式表中相同的符号有着相同或相似的含义。

贝叶斯分类器是以贝叶斯定理为基础的分类算法的总称,是基于样本分布已知的假设来选择最有可能的类别。与其他方法相比,贝叶斯分类器支持增量训练并实时调整概率值。此外由于假设特征之间相互独立而无须考虑特征组合,大大提高了大规模训练集的计算效率。然而,贝叶斯分类器对特征组合较为受限。逻辑回归模型实际上是用于二分类问题的分类模型,选择与实际输出值误差最小的类别作为预测标签。这种方法实现简单,易于理解,并且能够方便的根据新的数据更新模型,因而得到了广泛的应用。然而,当数据量或特征空间比较大导致线性不可分时,该模型也会因为过于简单而无法对数据进行较好地学习,从而体现出欠拟合、异常值敏感等问题。支持向量机通过核函数可以较好地解决非线性问题,能够提高模型的泛化性能,解

决高维度数据的问题,但是方法本质受限于算法的复杂度(特别是核方法)无法处理大规模数据。决策树也是一种易于理解的白盒模型,它甚至不限制使用非数值型数据。但是决策树完全依赖数据,存在过拟合的风险。集成学习的思想是利用多个弱分类器组合成强分类器,从而提高预测精度,并且一些集成学习方法如随机森林实现了数据的并行化处理,提高了效率,但是组合学习器相比单学习器势必会增加来更多的计算成本。神经网络通过前向传播来拟合数据,通过反向传播来更新参数,是一种自主学习器,但是浅层的神经网络往往因为有限的样本数量和参数数量而无法拟合复杂函数。与之相比,深度学习通过增加网络的参数数量和数据的需求量来实现更复杂的功能,但是这也使硬件成本和数据标注成本大大提升。无论是浅层神经网络还是深度学习方法都是一个完全的黑箱模型,因为人类无法得知模型输入特征多对应的相对权重,因此较难给出对输出的结果进行合理的解释。从本文收集的各种机器学习模型的文献数量和发表时间来看,传统机器学习模型应用较早,但是研究成果不多,这反映出传统机器学习可能在特征选择、模型拟合等环节存在较大局限性;而近年来基于神经网络,特别是基于深度学习的方法以强大的表示能力和数据拟合能力开始广泛应用于车险欺诈检测。

总之,没有一种机器学习技术能在所有数据集上所有任务中优于其他技术,它们都有各自的模型特点与局限性。为此,在车险欺诈研究的过程中,诸多学者提出了相应的改进思路。

表 1 车险欺诈检测中机器学习模型的总结

Table 1 Summary of machine learning models for auto fraud detection

模型名称	核心公式	模型特点	局限性	文献数量	改进思路
贝叶斯分类	$f(x) = \operatorname{argmax}_{c \in C} P(c x)$	支持增量训练, 假设特征独立	无法处理特征组合问题	3	正则化, 分类器互补(S. Viaene et al.,2005[4]) Gibbs 采样(Bermúdez et al.,2008[26])

逻辑回归模型	$f(x) = \text{sign}(\sum_i \omega_i x_i + b)$	易于建模, 支持增量式训练	异常值敏感	4	条件相关模型(赵桂芹等, 2010[16]) 风险暴露因子(张连增等, 2012[43])
支持向量机	$f(x) = \omega^T x + b$ s.t. $yf(x) \geq 1$	鲁棒性强, 可以非线性映射	大规模训练难以实施	2	基于 Apriori 的数据挖掘(汤俊等, 2013[17]) 谱排序(Nian et al., 2016[30])
决策树	$\text{Info}(D) = -\sum_i p_i \log(p_i)$	规则清晰, 可处理异常值	依赖数据, 容易过拟合	3	数据挖掘(Kašćelan et al., 2014[6]) 模糊 c 均值聚类(Majhi et al., 2019[12])
K 近邻	$f(x) = \underset{i=1,2,\dots,N; j=1,2,\dots,k}{\text{argmax}} I(y_i = c_j)$	支持增量训练, 对缺失值、参数独立性和噪声鲁棒	分类速度慢 大规模计算代价过高	1	基于遗传算法的特征选择(Badriyah et al., 2018[31])
集成学习	$H(x) = \text{sign}(\sum_i h_i(x))$	鲁棒性强, 精度较高	增加计算成本, 部分算法并行性差	3	粗糙集(Xu et al., 2011[33]) 基于潜在最近邻的投票机制(Li et al., 2018[7]) 快速决策树(Dhieib et al., 2020[34])
神经网络	$f(x) = \sigma(\sum_i \omega_i x_i + b_i)$	自主学习, 可以非线性拟合	无法拟合复杂函数, 可解释性差	4	logit 回归分析(叶明华, 2011[47]) 图学习算法(Liang et al., 2019[35]) 解决不一致性问题(Liu et al., 2020[36])
深度学习	$f(x) = \sigma(\sum_i \omega_i x_i + b_i)$	学习能力强, 精度很高	计算和标注成本高, 部分超参数需凭经验确定	8	添加隐藏层(He et al., 2017[8]) 行为序列交互, 注意力机制(Guo et al., 2018[9])

### 3 模型结果分析

#### 3.1 测试数据集与评估标准

数据集选取真实生产环境下某车险保险公司降采样数据<sup>1</sup>共 11350 条, 采集时间为 2014.03—

<sup>1</sup>由于正常保险公司欺诈概率在 1%左右, 我们收集的标注数据欺诈概率在接近 20%, 实际上降低了正常数据的样本, 因此称之为降采样。

2019.08, 采集案件主要集中在 2019 年。其中, 非欺诈数据 8792 条占数据总量的 77.46%, 欺诈数据 2558 条占数据总量的 22.54%。经数据清洗后, 可用字段合计 900 项, 包含类别型字段 31 项、数值型字段 868 项以及欺诈标签字段 1 项。

由于车险数据是一种有偏的样本数据, 因此在数据划分时需维持原样本的标签分布。在本此模型测试过程中, 训练集、测试集分别占数据总量的 80% 和 20%。其中, 训练集数据共 9080 条, 含非欺诈数据 7036 条、欺诈数据 2044 条; 测试集数据共 2270

条, 含非欺诈数据 1756 条、欺诈数据 514 条。需要注意的是, 对于深度学习模型, 我们将从训练集中额外划分出 20% 的数据作为验证集以用于调整模型的超参数。

对于二分类问题, 根据样本真实类别和对应模型预测结果的组合分为真正例 (True Positive, TP), 真负例 (True Negative, TN), 假正例 (False Positive, FP), 假负例 (False Negative, FN), 如表 2 所示。

表 2 分类样本混淆矩阵

Table 2 The confusion matrix of classified sample

预测结果 真实类别	正例	负例
正例	TP	FN
负例	FP	TN

评估指标主要从精确率、召回率、F1-值、精度、AUC 面积大小、逻辑损失 5 种评估指标来进行度量, 以下分别对这 5 种指标来进行描述

**Precision:** 又被称为精确率、查准率, 是二分类任务中常用于评估模型预测结果是否精确的性能指标。精确率定义为真正例占所有预测结果为正例样本的比值, 对应的公式为

$$P = \frac{TP}{TP + FP} \quad (1)$$

**Recall:** 又被称为召回率、查全率, 是二分类任务中常用于评估模型预测结果是否完备的性能指标。召回率定义为真正例占所有真实类别为正例样本的比值, 对应的公式为

$$R = \frac{TP}{TP + FN} \quad (2)$$

**F1-score:** 又被称为 F1 度量, 它是在精确率和召回率的基础上取调和平均数得到的, 对应的公式为

$$F1 = \frac{2PR}{P + R} \quad (3)$$

**Accuracy:** 又被称为精度, 定义为分类正确的样本占样本总数的比值, 对应的公式为

$$acc = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

**AUC (Area Under ROC Curve):** AUC 是二分类任务中用于评估模型泛化性能的指标, 它的定义是 ROC (Receiver Operating Characteristic) 曲线下的区域面积。ROC 曲线按照模型的预测结果逐个对样本进行排序, 并分别以真正例率和假正例率为纵轴和横轴绘制在二维坐标系上形成一条曲线。其中真正例率 (True Positive Rate, TPR) 和假正例率 (False Positive Rate, FPR) 公式为

$$TPR = \frac{TP}{TP + FN} \quad (5)$$

$$FPR = \frac{FP}{TN + FP} \quad (6)$$

通常使用曲线下区域面积 AUC 来进行比较, 如下图 3 所示。该性能指标可以在数据不平衡的数据集上进行客观的评估。

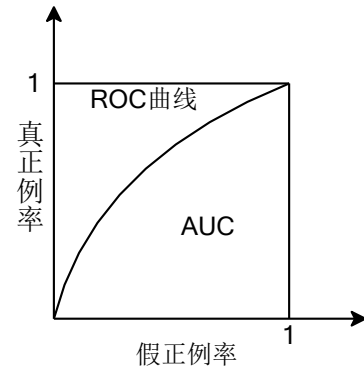


图 3 AUC 示意图

Fig.3 The diagram of AUC

此外, 为了分析欺诈模型在多分类上的效果, 我们进一步将数据的标签细分为 9 个标签<sup>2</sup>, 并保持实验的训练测试比例不变。具体的细分标签为: 非欺诈标签(8892), 人工标记欺诈(1302), 倒签单(7), 痕迹不符(928), 酒驾(131), 虚假报案(9), 隐瞒事故真相(60), 重复索赔(12), 准驾异常(5); 相应的, 实验采用了多分类的评价指标, 分别

<sup>2</sup>为了保证多分类模型的训练效果, 在欺诈标签类型细分时, 会将少量原因不明欺诈数据视为正常数据处理。

使用了 Precision, Recall, F1-score 对应的微平均 (Micro), 宏平均 (Macro) 和带权平均 (Weighted) 的评估方式。

**Micro:** Micro 形式的评价指标不关注样本类别, 直接评估全体样本的分类效果。以 precision 为例, 将所有类的 TP 加和, 再除以所有类的 TP 和 FN 的加和。Micro 形式下的 precision, recall, accuracy 相等。

$$precision_{micro} = \frac{\sum_{k \in C} TP_k}{\sum_{k \in C} TP_k + FP_k} \quad (7)$$

$$recall_{micro} = \frac{\sum_{k \in C} TP_k}{\sum_{k \in C} TP_k + FN_k} \quad (8)$$

$$f1 - score_{micro} = \frac{2 * precision_{micro} * recall_{micro}}{precision_{micro} + recall_{micro}} \quad (9)$$

**Macro:** Macro 形式的评价指标首先分别求出每个类的对应值, 再求算术平均。

$$precision_k = \frac{TP_k}{TP_k + FP_k} \quad (10)$$

$$recall_k = \frac{TP_k}{TP_k + FN_k} \quad (11)$$

$$f1 - score_k = \frac{2 * precision_k * recall_k}{precision_k + recall_k} \quad (12)$$

$$f1 - score_{macro} = \frac{1}{n} \sum_{k=0}^n f1_k \quad (13)$$

**Weighted:** Weighted 形式是在 Macro 形式上的改进, 对各类的结果值不再取算术平均, 而是乘以

该类在总样本数中的占比作为权重。

$$f1 - score_{weighted} = \sum_{k=0}^n w_k * f1_k \quad (14)$$

## 3.2 测试模型与结果分析

我们在 Linux 操作系统上 (16 核的 Inter Xeon 2.99GHz CPU, 内存 16G) 进行了仿真实验, 采用编程语言为 Python 3.7, 并基于 sklearn 库、xgboost 库和 deepCTR-torch 库实例化测试模型。深度学习模型均选择自适应梯度算法 (Adaptive Gradient Algorithm) 作为优化函数, 设定学习率为 0.01、批量采样的大小 batch\_size 为 32, 周期 epochs 选择对验证集梯度最小的参数值。需要注意的是, 在未说明的情况下, 输入数据中类别型数据默认采用标签编码 (Label Encoding) 的方式处理。

为了评估全面的评估现有机器学习模型的效果, 我们一共选择了 7 类传统机器学习模型 (含变种) 以及 6 种深度学习模型进行测试和分析, 具体列出如下:

**贝叶斯网络:** 为经典的机器学习模型, 基于特征间强独立假设和贝叶斯定理, 车险数据特征大多离散分布, 适用于二分类或者多分类任务建模, 其中模型的先验平滑因子 alpha=1.0。

**逻辑回归:** 为经典的机器学习模型, 基于概率论, 通过极大似然模型求解参数以实现未知数据的欺诈检测, 其中模型的惩罚参数 penalty='l2', 最大迭代次数 max\_iter=100。

**SVM (线性):** 为经典的机器学习模型, 基于几何间隔最大化原理, 以找出最大几何间隔的分类面为优化目标, 其中模型的正则化参数 penalty='l2', 模型的损失函数为平方合页损失 (squared\_hinge)。

**SVM (非线性):** 为 SVM 的核方法, 适用于数据线性不可分的情况, 通过核函数将数据映射到高维空间直到线性可分, 其中模型选取的核为径向基函数 (RBF)

**随机森林:**属于机器学习中集成学习范畴,是一个由多个决策树构成的组合分类器,决策树之间无依赖关系,其中基评估器的数量为100个。

**Xgboost:**属于机器学习中集成学习范畴,是一个由多个分类回归树构成的组合分类器,分类回归树之间存在强依赖关系,其中目标函数分别采用 binary:logistic(二分类)和 multi:softprob(多分类)。

**Xgboost (one-hot):**为Xgboost的变种,主要是对输入数据中类别型数据采用 one-hot encoding 处理,其中目标函数同样采用 binary:logistic(二分类)和 multi:softprob(多分类)。

**PNN:**为基于点积的神经网络,属于深度学习模型。相较于传统的MLP模型,PNN通过嵌入层来学习分类数据的分布式表示,然后通过点积层来捕获域间类别之间的交互模式,进一步利用全连接层来探索高阶特征交互,其中隐藏层层数为2层,神经元数量均为128个,激活函数为relu,核的类型为mat。

**WDL:**为深浅层学习框架,属于深度学习模型。WDL通过结合线性模型和深度模型,保证了记忆与泛化的优点,同时采用联合训练(joint training)的方法进行优化。其中隐藏层层数为2层,神经元数量分别为256和128个,激活函数为relu。

**DeepFM:**为深度的因子分解机,属于深度学习模型。DeepFM结合了分解机制和深度学习的能力分别用于推荐和特征学习,它改进了WDL模型的Wide部分,将LR替换FM(因子分解机),以实现自动构造二阶特征,其中隐藏层层数为2层,神经元数量分别为256和128个,激活函数为relu。

**DCN:**为深度交叉网络,属于深度学习模型。它改进了WDL模型的Wide部分,DCN能够显式地在每一层应用特征交叉,自动构造有限高阶的交叉特征并学习对应权重,其中隐藏层层数为2层,

神经元数量均为128个,激活函数为relu。

**NFM:**为神经因子分解机,属于深度学习模型。改进了WDL模型的Deep部分,NFM将FM的二阶交叉项作为Deep模型的输入,通过添加隐藏层获更强的性能,其中隐藏层层数为2层,神经元数量均为128个,激活函数为relu。

**AFM:**为注意力因子分解机,属于深度学习模型。改进了WDL模型的Deep部分,加入注意力机制区分不同交叉特征的重要性,其中激活函数为relu,attention network的隐藏层大小设置为8层。

表3列出了上述机器学习模型在车险欺诈中的整体实验结果。可以发现基于集成学习Xgboost及其变种Xgboost(one-hot)模型与基于深度学习的模型效果较好,特别在F1-score、Accuracy、AUC均超过传统的机器学习模型。Xgboost及其变种Xgboost(one-hot)在F1值与AUC上取得了最佳的效果,我们认为主要是受益于数据特征的提炼以及集成学习自身较强的泛化能力。相对的,在深度学习模型中,DCN的效果最佳,得益于它在改进部分深度学习模型(如:WDL)对于深度模块的建模方式。由于深度学习模型受限于现有数据规模,无法进一步从海量的特征中进行隐形特征的学习,因此效果较Xgboost略差。此外,我们发现贝叶斯网络和SVM-核方法分别在Recall和Precision取的了最佳效果。从侧面可以发现,这两类模型在车险欺诈检测任务中表现的较为极端。贝叶斯网络尽管可以发现更多的车险欺诈案例,但对应的也会误判部分正常的车险理赔案件,因为其正确率较低,这将会给公司校对人员带来更大的现场勘测成本。而SVM-核方法则过于保守,尽管不会将正常的车险理赔案件误判,但也很难对真实的车险欺诈案件进行有效检测,因此难以达到实现车险欺诈检测的目的。

表3 车险欺诈检测整体的实验结果

Table 3 The whole experiment result of auto fraud detection

方法	Precision	Recall	F1-score	Accuracy	AUC
贝叶斯网络	0.3247	<b>0.7529</b>	0.4537	0.5894	0.7086
逻辑回归	0.9057	0.3735	0.5289	0.8493	0.8072

SVM-线性	0.9126	0.3658	0.5222	0.8485	0.7923
SVM-核方法	<b>0.9350</b>	0.3638	0.5238	0.8502	0.7306
随机森林	0.7532	0.3444	0.4726	0.826	0.7874
Xgboost	0.7973	0.4514	0.5764	0.8498	0.8328
Xgboost-one-hot	0.8114	0.4689	<b>0.5943</b>	<b>0.8551</b>	<b>0.8351</b>
PNN	0.8719	0.4105	0.5582	0.8529	0.8131
WDL	0.8182	0.4202	0.5553	0.8476	0.8086
deepFM	0.8689	0.4125	0.5594	0.8529	0.8137
DCN	0.8549	0.4241	0.567	0.8533	0.817
NFM	0.8353	0.4047	0.5452	0.8471	0.8132
AFM	0.894	0.3774	0.5308	0.8489	0.7981

考虑到车险欺诈数据在真实场景中存在客观的不均衡性,因此,我们进一步检测了不同幅度下数据不均衡对各模型的影响。具体来说,我们将训练集中标注为“欺诈”的训练样例进行随机移除,同时保证正常的车险理赔案件数量不变,由此对训练数据集中的不均衡性进行调整。数据不均衡对各类机器学习模型的影响如表4所示。可以发现,大部分模型的性能都出现了不同程度的下降趋势。整体而言,Xgboost及其变种Xgboost(one-hot)依然能在各种数据不均衡的车险欺诈检测任务中获得最佳的效果。受益于one-hot的建模效果,

Xgboost(one-hot)在比例减少时,性能上甚至存在着一定程度的反弹。我们分析认为,可能在于该批移除的车险欺诈的数据存在部分噪声,使得模型学习剩余数据的效果反而得到了提升。整体来说,随着数据不均衡的加剧,Xgboost(one-hot)仍会出现性能下降的趋势。此外,大部分深度学习模型在车险欺诈任务的性能上也会有不同程度的下降。尽管如此,在性能的损失方面,除了NFM与DCN之外,其他的深度模型下降的幅度只有1.5%左右,这在一定程度凸显出了这些模型能较好地学习到数据的隐性特征。

表4 数据不均衡对各模型的影响

Table 4. The whole experiment result of auto fraud detection

正反样例比	0.77: 0.23		0.82: 0.18		0.86: 0.14		0.91: 0.09	
方法	F1-score	AUC	F1-score	AUC	F1-score	AUC	F1-score	AUC
Xgboost	0.5764	0.8328	0.5603	0.8239	0.5512	0.8089	0.5113	0.7991
Xgboost-one-hot	<b>0.5943</b>	<b>0.8351</b>	<b>0.8578</b>	<b>0.9508</b>	<b>0.7747</b>	<b>0.9239</b>	<b>0.702</b>	<b>0.8825</b>
PNN	0.5582	0.8131	0.537	0.8086	0.5203	0.7905	0.5132	0.7835
WDL	0.5553	0.8086	0.5269	0.8081	0.5154	0.7951	0.4675	0.7863
deepFM	0.5594	0.8137	0.5311	0.8102	0.5112	0.7916	0.4651	0.7772
DCN	0.567	0.817	0.535	0.8106	0.5201	0.7974	0.495	0.7849
NFM	0.54	0.8122	0.538	0.7949	0.4915	0.787	0.5382	0.8112
AFM	0.5308	0.7981	0.5222	0.7937	0.5203	0.7858	0.521	0.7834

为了进一步验证训练数据规模对各模型的影响,我

们对整体的训练集进行了等比例的缩放,并保证测



试集不变。表 5 列出了不同百分比数据集对模型性能的影响。可以发现，即便在整体训练规模只有原训练集的 50% 时，Xgboost 及其变种 Xgboost(one-hot) 依然能在车险欺诈检测任务上获得最佳的效果，综合 F1-score 和 AUC 的评分情况，可以发现 Xgboost 及其变种 Xgboost(one-hot) 在性能上均处于前 2 名。从图 4 中，我们可以观察到其在取值上整体高出了

深度学习模型 1.5%-2.0%。相对的，大部分深度学习模型在车险欺诈任务的性能都有不同程度的下降。此外，在性能损失方面，即便只有 50% 的训练数据，Xgboost 及其变种 Xgboost(one-hot) 在 F1-score 与 AUC 的评分上只有 2% 左右的下降，在一定程度上凸显出了它们的泛化能力。

表 5 训练百分比对各模型的影响

Table 5 Influence of training percentage on each model

训练百分比	50%		60%		70%		80%		90%		100%	
	F1	AUC	F1	AUC	F1	AUC	F1	AUC	F1	AUC	F1	AUC
Xgboost	0.5475	0.8075	<b>0.5599</b>	0.8122	0.5598	<b>0.8272</b>	<b>0.5625</b>	0.8278	0.5732	0.8315	0.5764	0.8328
Xgboost-one-hot	<b>0.5528</b>	<b>0.8134</b>	0.5569	<b>0.8266</b>	<b>0.5609</b>	0.8266	0.5606	<b>0.8352</b>	<b>0.5833</b>	<b>0.8369</b>	<b>0.5943</b>	<b>0.8351</b>
PNN	0.5337	0.7811	0.5319	0.7854	0.5319	0.7938	0.533	0.8026	0.5342	0.8041	0.5718	0.8147
WDL	0.5288	0.7865	0.5398	0.7957	0.5368	0.8107	0.5515	0.8068	0.5469	0.8132	0.5553	0.8087
deepFM	0.5279	0.789	0.5415	0.7944	0.5238	0.8074	0.5304	0.8044	0.5306	0.806	0.5667	0.8108
DCN	0.5335	0.7977	0.5423	0.7901	0.5417	0.8089	0.5481	0.8083	0.5598	0.8146	0.5658	0.8149
NFM	0.5209	0.7853	0.5457	0.7938	0.5427	0.8098	0.5469	0.8075	0.5526	0.8086	0.5509	0.8132
AFM	0.5222	0.7807	0.5315	0.7903	0.5284	0.7964	0.5315	0.7988	0.5284	0.7986	0.5333	0.799

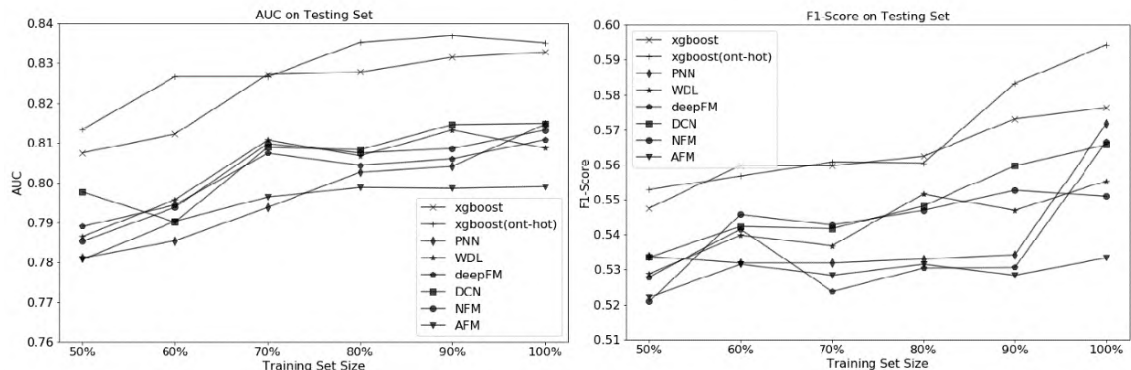


图 4 不同训练百分比数据集中模型性能的趋势图

Fig.4 Trend graph of model performance in data sets with different training percentage

表 6 给出的是机器学习模型在多分类任务中评估的结果。整体上,我们可以看到在三项评估中,Xgboost-one-hot 依然在 Micro 形式与 Weighted 形式上较传统的机器学习方法与深度学习方法有着更加出色的效果。贝叶斯网络与 Xgboost 分别在 Macro 形式的 Recall 与 Weighted 形式的 Precision 上获得了最佳的效果。而深度学习模型整体表现非常一般,其效果甚至只能与逻辑回归模型的结果相当。经过对数据集的分析,我们发现深度学习模型主要还是受限于数据规模的影响。此外,在 Macro

评估方式中,我们可以发现所有的模型在 Precision、Recall、F1-Score 的表现都不如人意,特别是在虚假报案、隐瞒事故真相、重复索赔、准驾异常、倒签单这些样本不足 100 的分类标签上。通过表 7 中的实验结果,我们进一步证实了,绝大多数的模型是无法对一些稀疏样本的欺诈数据进行学习与区分的。因此,以算术平均为基础的 Macro 评估则会给出一个整体较差的结果。相对来说,传统的机器学习模型在这些少样本的分类任务上能取得的效果比深度学习模型的效果略好一些。

表 6 机器学习模型在多分类任务中的评估结果

Table 6 Evaluation results of ML models in multi-classification tasks

正反样例比	Micro Evaluation			Macro Evaluation			Weighted Evaluation		
	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score
贝叶斯网络	0.3286	0.3286	0.3286	0.1512	<b>0.2527</b>	0.1201	0.7633	0.3286	0.3756
逻辑回归	0.8595	0.8595	0.8595	0.1963	0.1898	0.1912	0.7747	0.8595	0.8117
SVM-线性	0.8599	0.8599	0.8599	0.1958	0.1437	0.1495	0.7451	0.8163	0.7533
SVM-核方法	0.8163	0.8163	0.8163	0.1958	0.1437	0.1495	0.7451	0.8163	0.7533
随机森林	0.8396	0.8396	0.8396	0.2585	0.1822	0.1986	0.8107	0.8396	0.8039
Xgboost	0.8656	0.8656	0.8656	0.2682	0.2040	0.2171	<b>0.8656</b>	0.8351	0.8331
Xgboost-one-hot	<b>0.8661</b>	<b>0.8661</b>	<b>0.8661</b>	<b>0.3267</b>	0.2094	<b>0.2261</b>	0.8434	<b>0.8661</b>	<b>0.8346</b>
PNN	0.8595	0.8595	0.8595	0.1971	0.1887	0.1907	0.7748	0.8595	0.8113
WDL	0.8617	0.8617	0.8617	0.1979	0.1905	0.1922	0.7768	0.8617	0.8137
deepFM	0.8595	0.8595	0.8595	0.1971	0.1887	0.1907	0.7748	0.8595	0.8113
DCN	0.8595	0.8595	0.8595	0.1971	0.1887	0.1907	0.7748	0.8595	0.8113
NFM	0.8595	0.8595	0.8595	0.1971	0.1887	0.1907	0.7748	0.8595	0.8113
AFM	0.8595	0.8595	0.8595	0.1971	0.1887	0.1907	0.7748	0.8595	0.8113

表 7 机器学习在不同类别中 F1 的实验结果

Table 7 Experimental results of F1 of ML models in different categories.

方法	正常	人工欺 诈标记	倒签单	痕迹 不符	酒驾	虚假 报案	隐瞒事 故真相	重复 索赔	准驾 异常
贝叶斯网络	0.4033	0.3570	0.0000	0.2103	0.1101	0.0000	0.0000	0.0000	0.0000
逻辑回归	0.9181	0.8026	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
SVM-线性	0.9189	0.8052	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
SVM-核方法	0.8951	0.4503	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
随机森林	0.9065	0.6458	0.0000	0.2348	0.0000	0.0000	0.0000	0.0000	0.0000
Xgboost	0.9207	<b>0.8131</b>	0.0000	0.2203	0.0000	0.0000	0.0000	0.0000	0.0000
Xgboost -one-hot	<b>0.9211</b>	0.8043	0.0000	<b>0.2379</b>	<b>0.0715</b>	0.0000	0.0000	0.0000	0.0000
PNN	0.9182	0.7983	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
WDL	0.9194	0.8103	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
deepFM	0.9182	0.7983	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
DCN	0.9182	0.7983	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
NFM	0.9182	0.7983	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
AFM	0.9182	0.7983	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

根据目前车险公司提供的数据表明，在车险欺诈检测任务中，集成学习的效果与深度学习效果较传统机器学习模型效果更好。一方面，集成学习和传统的机器学习模型对硬件要求较低，而深度学习对硬件普遍具有较高的要求。另一方面，深度学习在保险欺诈检测任务中具备较好的效果，基于深度学习的思想可以学到潜在的特征表示，且标注数据规模越大而越有效。相对的，传统的机器学习模型与集成学习模型对数据的特征提取存在较高的要求。

#### 4 总结与展望

本文重点对机器学习模型在车险欺诈检测的研究进展进行全面细致的归纳与总结，基于车险公司真实的数据对各类机器学习模型进行全面测试

与分析。实验结果表明，在车险欺诈的任务中，集成学习与深度学习模型较传统机器学习模型效果更好。相对的，集成学习需要对数据特征的提取存在较高的要求，而深度学习则对模型实现的硬件环境与数据集规模具有较大的需求。

经过对国内现有保险数据进行综合分析，我们认为将来车险欺诈检测的研究可以从以下五方面进行展开：

(1)基于小样本学习的欺诈检测技术:目前机器学习的模型在常规的二分类任务上表现较为满意。然而，对于多分类任务，可以发现当下的机器学习模型无法胜任这些欺诈类别中样本极度稀疏的分类工作。为此，可以将小样本学习( few-shotlearning )<sup>[50][51]</sup>的前沿技术进行引入到车险欺诈的多分类任务中，以此来提高多种车险欺诈类型的检测性能。

(2)基于图谱的团伙检测技术:目前车型欺诈团

伙犯罪的趋势较为明显,未来车险欺诈检测可以从团伙车险欺诈检测<sup>[52]</sup>入手,结合知识图谱<sup>[53]</sup>与事件图谱<sup>[54]</sup>等方法中实体关联,利用知识图谱或事件图谱表示学习中连续、稠密的向量表示来预测对案件因子之间内在的关联与案件之间的因果联系,从而将案件相关信息和相似案件信息进行深度结合,以此来提高欺诈检测的效果。

**(3)基于表示学习的案因回溯检测技术:**目前机器学习模型尽管能表现效果较好,但仍存在解释匮乏的问题。而专家系统中的规则表达方式可以较好的弥补这一点。为此,可以对专家系统中的触发因子与机器学习和深度学习的向量表示进行关联,利用机器学习中各因子所在模型中所对应的权重以及深度学习所学习得到的向量表示来评估触发的规则的概率,即便专家系统中的触发规则并未触发,但仍可以通过规则中相应的触发因子以及因子权重来获得最可能的规则推送给专家,继而利用案因回溯的思想<sup>[55]</sup>·<sup>[56]</sup>给保险公司现场勘测人员提供有效的线索,提升勘测人员去现场确认的成功率。

**(4)融合文本、图像的多模态检测技术:**目前的机器学习模型更多的围绕车型欺诈拟定的指标体系从数据集库数据中抽取与提炼核心的特征,但对于文本(勘测记录的文字描述)以及图像数据(如:现场勘测拍摄的图片)的信息利用并不成熟。利用多模态技术<sup>[57]</sup>·<sup>[58]</sup>从来提高车厢欺诈的检测精度将是未来的一个重要的研究方向。一方面,可以利用自然语言处理中的关系抽取技术、事件抽取技术可以从勘测记录中得到更多有用的结构化信息;另一方面,利用图像中的场景识别技术与匹配技术,可以有效地辨识是案件中是否存在车险欺诈常用的场景,继而提高车险欺诈检测整体的效果。

**(5)基于车险体系的联邦学习技术:**由于目前车险欺诈领域高质量的标注数据存在不平衡现象,细粒度的欺诈标注数据集十分稀缺。为此,我们可以通过各保险公司协商,基于知识对齐技术<sup>[59]</sup>形成一套统一的车险规范体系<sup>[60]</sup>,再进一步利用联邦学习技术<sup>[61]</sup>·<sup>[62]</sup>将保险公司中高质量的标注数据进行数据加密共享,最终,借助引入外部的高质量数据来

提升模型学习的效果,继而提高车型欺诈检测的性能。

## 参考文献

- [1] 喻炜,冯根福,张文珺.机动车辆保险欺诈检测系统及团伙识别研究[J].保险研究,2017(2):63-73.  
Yu W, Feng G F, Zhang W J. Research on fraud detection system and gang identification of motor vehicle insurance [J]. Insurance Research, 2017(2):63-73.
- [2] 车险反欺诈联合课题组.车险欺诈与反欺诈问题研究及监管建议[J].保险研究,2021(6):3-10.  
Auto Insurance Anti-fraud Joint Research Group. Research on Auto Insurance Fraud and Antifraud and Supervision Suggestions[J]. Insurance Research, 2021(6):3-10.
- [3] 张碧怡,肖宇谷,曾宇哲.车险定价中风险因子重要性测度的比较研究——基于集成学习方法和广义线性回归模型[J].保险研究,2019(10):73-83.  
Zhang B Y, Xiao Y G, Zeng Y Z. Comparative study on the importance measurement of risk factors in auto insurance pricing-based on ensemble learning method and generalized linear regression model[J]. Insurance Research, 2019(10):73-83.
- [4] Viaene S, Dedene G, Derrig R A. Auto claim fraud detection using Bayesian learning neural networks[J]. Expert Systems with Applications, 2005, 29(3): 653-666.
- [5] Payam Hanafizadeh, Neda Rastkhiz Paydar. A Data Mining Model for Risk Assessment and Customer Segmentation in the Insurance Industry[J]. International Journal of Strategic Decision Sciences (IJSDS), 2013, 4(1).
- [6] Kaščelan L, Kaščelan V, Novović-Burić M. A Data Mining Approach for Risk Assessment in Car Insurance: Evidence from Montenegro[J]. International Journal of Business Intelligence Research (IJBIR), 2014, 5(3): 11-28.
- [7] Li Y, Yan C, Liu W, et al. A principle component analysis-based random forest with the potential nearest neighbor method for automobile insurance fraud identification[J]. Applied Soft Computing, 2018, 70: 1000-1009.
- [8] He X, Chua T S. Neural factorization machines for sparse predictive analytics[C]//Proceedings of the 40th International ACM SIGIR conference on Research and Development in Information Retrieval. 2017: 355-364.
- [9] Guo J, Liu G, Zuo Y, et al. Learning sequential behavior representations for fraud detection[C]//2018 IEEE international conference on data mining (ICDM). IEEE, 2018: 127-136.
- [10] Wang R, Fu B, Fu G, et al. Deep & cross network for ad click predictions[M]//Proceedings of the ADKDD'17.

- 2017: 1-7.
- [11] Subudhi S, Panigrahi S. Use of optimized Fuzzy C-Means clustering and supervised classifiers for automobile insurance fraud detection[J]. *Journal of King Saud University-Computer and Information Sciences*, 2020, 32(5): 568-575.
- [12] Majhi S K. Fuzzy clustering algorithm based on modified whale optimization algorithm for automobile insurance fraud detection[J]. *Evolutionary intelligence*, 2021, 14(1): 35-46.
- [13] 鹿国柱,段家喜.保险欺诈的博弈分析[J].*首都经济贸易大学学报*,1999(3):51-54.
- Guo G Z, Duan J X. Game analysis of insurance fraud [J]. *Journal of capital university of economics and business*, 1999(3):51-54.
- [14] 刘喜华,金加林.保险欺诈博弈与基于最优博弈策略的保险契约[J].*系统工程理论与实践*,2004(2):19-24.
- Liu X H, Jin J L. Insurance fraud game and insurance contract based on optimal game strategy [J]. *System Engineering Theory and Practice*, 2004(2):19-24.
- [15] 桂萍,胡庆为.国内外车险道德风险文献综述[J].*保险研究*,2011(6):121-127.
- Gui P,Hu Q. literature review on moral hazard of auto insurance at home and abroad[J]. *insurance research*, 2011(6):121-127.
- [16] 赵桂芹,吴洪.汽车保险市场中存在道德风险吗?——来自动态续保数据的分析[J].*金融研究*,2010(6):175-188.
- Zhao G Q, Wu H. Is there moral hazard in the automobile insurance market? —— Analysis from dynamic renewal data [J]. *Financial Research*, 2010(6):175-188.
- [17] 汤俊,莫依雯.基于数据挖掘技术的车险反欺诈系统构建[J].*上海保险*,2013(11):39-42+63.
- Tang J, Mo Y W. Construction of auto insurance anti-fraud system based on data mining technology [J]. *Shanghai Insurance*, 2013(11):39-42+63.
- [18] 王海巍.我国险企运营中道德风险甄别问题研究——以大数据 Hadoop 聚类分析技术为视角[J].*保险研究*,2016(2):59-67.
- Wang H W. Research on moral hazard screening in the operation of insurance enterprises in China-from the perspective of big data Hadoop cluster analysis technology [J]. *Insurance Research*, 2016(2):59-67.
- [19] 闫春,李亚琪,孙海棠.基于蚁群算法优化随机森林模型的汽车保险欺诈识别研究 [J]. *保险研究*,2017(6):114-127.
- Yan C, Li Y Q, Sun H T. Auto insurance fraud identification based on ant colony algorithm optimizing stochastic forest model [J]. *insurance research*, 2017(6):114-127.
- [20] 徐徐,王正祥,王牧群.基于深度学习技术的机动车辆保险欺诈识别模型与实证研究 [J]. *上海保险*,2019(8):53-58.
- Xu X, Wang Z X, Wang M Q. The model and empirical study of motor vehicle insurance fraud identification based on deep learning technology [J]. *Shanghai Insurance*, 2019(8):53-58.
- [21] Panigrahi S, Palkar B. Comparative analysis on classification algorithms of auto-insurance fraud detection based on feature selection algorithms[J]. *Int. J. Comput. Sci. Eng*, 2018, 6(9): 72-77.
- [22] Błaszczyszki J, de Almeida Filho A T, Matuszyk A, et al. Auto loan fraud detection using dominance-based rough set approach versus machine learning methods[J]. *Expert Systems with Applications*, 2021, 163: 113740.
- [23] Hassan A K I, Abraham A. Modeling insurance fraud detection using imbalanced data classification[M]//*Advances in nature and biologically inspired computing*. Springer, Cham, 2016: 117-127.
- [24] Padhi S, Panigrahi S. Decision Templates based Ensemble Classifiers for Automobile Insurance Fraud Detection[C]//2019 Global Conference for Advancement in Technology (GCAT). IEEE, 2019: 1-5.
- [25] Šubelj L, Furlan Š, Bajec M. An expert system for detecting automobile insurance fraud using social network analysis[J]. *Expert Systems with Applications*, 2011, 38(1): 1039-1052.
- [26] Bermúdez L, Pérez J M, Ayuso M, et al. A Bayesian dichotomous model with asymmetric link for fraud in insurance[J]. *Insurance: Mathematics and Economics*, 2008, 42(2): 779-786.
- [27] Bhowmik R. Detecting auto insurance fraud by data mining techniques[J]. *Journal of Emerging Trends in Computing and Information Sciences*, 2011, 2(4): 156-162.
- [28] Yan C, Li Y. The identification algorithm and model construction of automobile insurance fraud based on data mining[C]//2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC). IEEE, 2015: 1922-1928.
- [29] David Mihaela, Jemna DănușVasile. Modeling the Frequency of Auto Insurance Claims by Means of Poisson and Negative Binomial Models[J]. *Annals of the Alexandru Ioan Cuza University - Economics*,2015,62(2).
- [30] Nian K, Zhang H, Tayal A, et al. Auto insurance fraud detection using unsupervised spectral ranking for anomaly[J]. *The Journal of Finance and Data Science*, 2016, 2(1): 58-75.
- [31] Badriyah T, Rahmaniah L, Syarif I. Nearest neighbour

- and statistics method based for detecting fraud in auto insurance[C]//2018 International Conference on Applied Engineering (ICAIE). IEEE, 2018: 1-5.
- [32] Yan C, Li Y, Liu W, et al. An artificial bee colony-based kernel ridge regression for automobile insurance fraud identification[J]. *Neurocomputing*, 2020, 393: 115-125.
- [33] Xu W, Wang S, Zhang D, et al. Random rough subspace based neural network ensemble for insurance fraud detection[C]//2011 Fourth International Joint Conference on Computational Sciences and Optimization. IEEE, 2011: 1276-1280.
- [34] Dhieb N, Ghazzai H, Besbes H, et al. A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement[J]. *IEEE Access*, 2020, 8: 58546-58558.
- [35] Liang C, Liu Z, Liu B, et al. Uncovering insurance fraud conspiracy with network learning[C]//Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval. 2019: 1181-1184.
- [36] Liu Z, Dou Y, Yu P S, et al. Alleviating the inconsistency problem of applying graph neural network to fraud detection[C]//Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. 2020: 1569-1572.
- [37] Qu Y, Cai H, Ren K, et al. Product-based neural networks for user response prediction[C]//2016 IEEE 16th International Conference on Data Mining (ICDM). IEEE, 2016: 1149-1154.
- [38] Cheng H T, Koc L, Harmsen J, et al. Wide & deep learning for recommender systems[C]//Proceedings of the 1st workshop on deep learning for recommender systems. 2016: 7-10.
- [39] Xiao J, Ye H, He X, et al. Attentional factorization machines: learning the weight of feature interactions via attention networks[C]//Proceedings of the 26th International Joint Conference on Artificial Intelligence, 2017: 3119-3125.
- [40] Wang Y, Xu W. Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud[J]. *Decision Support Systems*, 2018, 105: 87-95.
- [41] Guo H, Tang R, Ye Y, et al. DeepFM: a factorization-machine based neural network for CTR prediction[C]//Proceedings of the 26th International Joint Conference on Artificial Intelligence. 2017: 1725-1731.
- [42] Gomes C, Jin Z, Yang H. Insurance fraud detection with unsupervised deep learning[J]. *Journal of Risk and Insurance*, 2021, 88(3): 591-624.
- [43] 张连增,孙维伟.车险索赔概率影响因素的 Logistic 模型分析[J].*保险研究*,2012(7):16-25.
- Zhang L Z, Sun W W. Logistic model analysis of influencing factors of auto insurance claim probability [J]. *insurance research*, 2012(7):16-25.
- [44] 袁幕琴.保险欺诈与大数据时代下的防范对策[J].*金融与经济*,2015(7):77-80.
- Yuan M Q. Insurance fraud and countermeasures in the era of big data [J]. *finance and economy*, 2015(7):77-80.
- [45] 卢文龙.大数据与车险反欺诈模型构建[J].*上海保险*,2015(1):27-30.
- Lu W L. Big data and auto insurance anti-fraud model construction [J]. *Shanghai Insurance*, 2015(1):27-30.
- [46] 张澄,赵晨.位置大数据在车辆保险风险管理中的应用[J].*大数据*,2016,2(5):79-87.
- Zhang C, Zhao C. application of location big data in vehicle insurance risk management[J]. *big data*, 2016,2(5):79-87.
- [47] 叶明华.基于 BP 神经网络的保险欺诈识别研究——以中国机动车保险索赔为例[J].*保险研究*,2011(3):79-86.
- Ye M H. Research on insurance fraud identification based on BP neural network-taking China's motor vehicle insurance claims as an example [J]. *insurance research*, 2011(3):79-86.
- [48] 闫春,厉美璇,周潇.基于改进的遗传算法优化 BP 神经网络的车险欺诈识别模型[J].*山东科技大学学报(自然科学版)*,2019,38(5):72-80.
- Yan C, Li M X, Zhou X. Auto insurance fraud identification model based on improved genetic algorithm and BP neural network [J]. *journal of Shandong university of science and technology (natural science edition)*, 2019,38(5):72-80.
- [49] 赵长利,李方媛.汽车保险网络风险闭环控制优化模型及算法[J].*系统工程*,2016,34(3):69-73.
- Zhao C L, Li F Y. Optimization model and algorithm for closed-loop control of automobile insurance network risk [J]. *System Engineering*, 2016,34(3):69-73.
- [50] Chen W Y, Liu Y C, Kira Z, et al. A closer look at few-shot classification[J]. *arXiv preprint arXiv:1904.04232*, 2019.
- [51] Bendre N, Marin H T, Najafirad P. Learning from few samples: A survey[J]. *arXiv preprint arXiv:2007.15484*, 2020.
- [52] 杨烁. 基于图的车险欺诈可视化分析系统的设计与实现[D].北京邮电大学,2019.
- Yang S. Design and implementation of visual analysis system of auto insurance fraud based on graph [D]. *Bei-jing University of Posts and Telecommunications*, 2019.

- [53] 漆桂林,高桓,吴天星.知识图谱研究进展[J].情报工程,2017,3(1):4-25.  
Qi G L, Gao H, Wu T X. Research progress of knowledge map [J]. Information Engineering, 2017,3(1):4-25.
- [54] 胡志磊,靳小龙,陈剑赟,黄冠利.事件图谱的构建、推理与应用[J].大数据,2021,7(3):80-96.  
Hu Z L, Jin X L, Chen J Y, Huang G L. Construction, reasoning and application of event map [J]. Big Data, 2021,7(3):80-96.
- [55] Frankendal J M, Ghanbarisaied S. Enabling innovation through an ecosystem: an exploratory case study[D]. , 2020.
- [56] 曾春艳,严康,王志锋,余琰,纪纯妹.深度学习模型可解释性研究综述[J].计算机工程与应用,2021,57(8):1-9.  
Zeng C Y, Yan K, Wang Z F, Yu Y, Ji C M. The deep learning model can be summarized by interpretive approach[J]. Computer Engineering and Application, 2021,57(8):1-9.
- [57] 孙影影,贾振堂,朱昊宇.多模态深度学习综述[J].计算机工程与应用,2020,56(21):1-10.  
Sun Y Y, Jia Z T, Zhu H Y. Summary of multimodal deep learning[J]. Computer Engineering and Applications, 2020,56(21):1-10.
- [58] 杨杨,詹德川,姜远,熊辉.可靠多模态学习综述[J].软件学报,2021,32(4):1067-1081.  
Yang Y, Zhan D C, Jiang Y, Xiong H. Review of reliable multimodal learning [J]. Journal of Software Engineering, 2021,32(4):1067-1081.
- [59] 王雪鹏,刘康,何世柱,刘树林,张元哲,赵军.基于网络语义标签的多源知识库实体对齐算法[J].计算机学报,2017,40(3):701-711.  
Wang X P, Liu K, He S Z, Liu S L, Zhang Y Z, Zhao J. Multi-Source Knowledge Base Entity Alignment by Leveraging Semantic Tags. [J]. Computer Engineering and Applications, 2017,40(3):701-711.
- [60] 陈焕新,李爱萍.基于Fabric的快速公平合同签署协议[J].计算机工程与应用:1-10[2021-09-17].  
Chen X X, Li A P, Zhu H Y. Fast and Fair Contract Signing Protocol for Fabric[J]. Computer Engineering and Applications, [2021-09-17].:1-10
- [61] 王健宗,孔令炜,黄章成,陈霖捷,刘懿,何安珣,肖京.联邦学习算法综述[J].大数据,2020,6(6):64-82.  
Wang J Z, Kong L W, Huang Z C, Chen L J, Liu Y, He A X, Xiao J. Summary of federated learning algorithms[J]. big data, 2020,6(6):64-82.
- [62] 刘俊旭,孟小峰.机器学习的隐私保护研究综述[J].计算机研究与发展,2020,57(2):346-362.  
Liu J X, Meng X F. Review of privacy protection in machine learning[J]. Computer Research and Development, 2020,57(2):346-362.