



ELSEVIER

Contents lists available at ScienceDirect

Engineering

journal homepage: [www.elsevier.com/locate/eng](http://www.elsevier.com/locate/eng)



Research  
Artificial Intelligence—Review

## 基于数据挖掘技术的税务风险检测方法评述

郑庆华<sup>a,b</sup>, 徐一明<sup>a,b</sup>, 刘慧祥<sup>a,b</sup>, 师斌<sup>a,b,\*</sup>, 王嘉祥<sup>a,b</sup>, 董博<sup>b,c</sup>

<sup>a</sup> School of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China

<sup>b</sup> Shaanxi Provincial Key Laboratory of Big Data Knowledge Engineering, Xi'an Jiaotong University, Xi'an 710049, China

<sup>c</sup> School of Distance Education, Xi'an Jiaotong University, Xi'an 710049, China

### ARTICLE INFO

#### Article history:

Received 26 December 2022

Revised 27 April 2023

Accepted 17 July 2023

Available online 25 September 2023

#### 关键词

税务风险检测

数据挖掘

知识指南

信息化

智能化

### 摘要

税务风险行为造成财政收入严重损失, 损害国家公共基础设施, 扰乱公平竞争的市场经济秩序。近年来, 受数据挖掘和人工智能等信息技术的推动, 税务风险检测受到了广泛的关注。为促进税务风险检测方法的高质量发展, 本文首次对全球现有的税务风险检测方法进行了全面的概述和总结。具体而言, 首先讨论了税务风险行为的成因及其负面影响, 以及税务风险检测的发展历程。随后, 重点分析了全球范围内基于数据挖掘的税务风险检测方法。根据算法所采用的不同原理, 现有的风险检测方法可分为基于关系的和非基于关系的两类, 共 14 种风险检测方法, 并对每种方法进行了深入的探讨和分析。最后, 本文分析和讨论了当前数据驱动的税务风险检测方法面临的四个主要技术瓶颈, 包括整合和利用财政和税收碎片化知识的困难、检测结果的不可解释性、风险检测算法的高成本以及现有算法对标记信息的依赖。通过对这些问题的研究, 得出知识导向和数据驱动的大数据知识工程将是未来税务风险领域的发展趋势, 即税务风险检测从信息化向智能化转型。

© 2023 THE AUTHORS. Published by Elsevier LTD on behalf of Chinese Academy of Engineering and Higher Education Press Limited Company. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## 1. 引言

税收是国家最重要的收入来源。据中国税务机关统计, 2021 年税收收入 (扣除出口退税) 占全国一般公共预算收入的 76.3% [1]。然而, 全球各国在税收治理方面面临的最大挑战仍然是逃税、欺诈和其他税务风险等问题。逃税和欺诈等税务风险行为不仅导致严重的税收损失, 侵蚀税基, 损害国家税收安全, 同时也扰乱了公平竞争的市场经济秩序, 造成不正当竞争。从 2011 年到 2013 年, 美国每年的平均税收总收入损失估计为 4410 亿

美元[2]。在欧盟, 根据 2015 年提供的数据, 税收损失的平均份额为 18.3%; 在瑞士这个份额最低的国家, 税收损失仍然相当于国内生产总值 (GDP) 的 6.9% [3]。据世界银行估计, 在 135 个发展中国家中, 有 54% 的公司没有向税务机关申报所有的所得税[4]。因此, 打击和整治税务风险行为对于规范市场秩序、维护公平公正至关重要, 也是提高国家治理能力的重要措施。

精准的税务风险检测是打击和整治税务风险行为的关键[5]。但是, 这项任务极其复杂且困难, 原因如下:

(1) 数据复杂、高维且规模庞大。税务场景包含来自

\* Corresponding author.

E-mail address: [shibin@xjtu.edu.cn](mailto:shibin@xjtu.edu.cn) (B. Shi).

不同来源（如工商、税收、社保、海关等）的数万亿数据以及多种类型的数据（如法规和政策、报表、发票、合同、交易文件等）。

**(2) 隐蔽的逃税模式。**在税务稽查员与逃税者之间不断博弈的过程中，逃税欺诈行为向团伙化、专业化、隐蔽化发展。例如，注册或购买空壳公司、层层掩盖、拉长犯罪时间链以及肆意跨地区、跨行业乃至跨境实施犯罪，以逃避监管和打击。

鉴于上述问题，传统的税务风险检测方法，如人工选案、举报选案、基于规则的选案等，由于高度依赖人力和财税专家的知识，存在很大的局限性。因此，隐藏的和复杂的与税务相关的犯罪难以识别。如何有效地从大量的多源异质税务相关数据中挖掘隐藏的税务风险线索，已成为税务当局和科研人员亟待解决的问题。

近年来，基于人工智能和数据挖掘的税务风险检测方法引起了许多国家和地区的广泛关注，并涌现出许多先进的方法。这类方法能够从海量的结构化和非结构化数据中挖掘出数据内部关系和规律，从而为解决上述瓶颈问题提供有效方案，并为税务风险检测提供新的范式。这些方法能够更深入地从税务交易网络包含的复杂结构信息和丰富语义信息中挖掘出更深层次的知识，从而提高税务风险检测的准确性。

本文回顾了现有的税务风险检测方法，旨在介绍税务风险检测的相关背景知识和发展过程，全面梳理现有方法，总结当前税务风险检测中遇到的主要问题，并探讨该领域的未来研究方向，以促进税务风险检测研究，助力更有效的税务风险治理。本研究的主要贡献可以总结如下：

(1) 据我们所知，本文是首篇系统性回顾全球税务风险检测的研究进展和发展趋势的综述。希望推动探索更强大的税务风险检测方法，从而减少国家税收损失。

(2) 介绍了有关税务风险检测的相关背景知识，包括税务风险行为的原因和负面影响以及税务风险检测的发展历程。此外，形式化定义了税务风险检测并详细介绍了输入数据的细节。

(3) 根据相关性和重要性筛选了来自世界各地的89篇税务风险检测研究文献，对税务风险检测的研究进行了综合整理，并将现有的方法划分为基于关系的风险检测方法和非基于关系的风险检测方法两大类，列出并介绍了14种典型方法。此外，还总结了每种方法的优缺点，这对实际应用至关重要。

(4) 总结了当前税务风险检测实践中面临的主要问题，并提出了今后推进税务风险检测从信息化走向智能化过程中亟待开展的未来研究方向。

本文的结构安排如下：第2节介绍了与税务风险检测相关的背景，并对现有的税务风险检测算法进行了分类，同时对税务风险检测问题进行了形式化定义。第3节和第4节全面回顾了现有的税务风险检测方法。第5节探讨了税务风险检测领域的未来研究方向。最后，第6节对全文进行了总结。

## 2. 背景

本节首先介绍有关税务风险检测的相关背景知识，包括税务风险行为的原因和负面影响。接下来，讨论在税务场景中的输入数据的性质。然后，提出了开发过程和税务风险检测的类型，以提供该领域的清晰概述。最后，提出了税务风险检测的具体问题的定义。

### 2.1. 税务风险行为的原因及负面影响

税务风险行为本质上是一种由利润驱动的非活动。纳税人可以通过欺诈或故意逃避真实的纳税义务来获得高额利润。税务风险行为不仅严重侵蚀了税基，而且间接影响了守法诚信纳税人的竞争力，从而扰乱了公平竞争的市场经济秩序。

### 2.2. 税务数据的性质

税务风险检测中最重要的部分是税务相关数据。风险检测模型从海量数据中挖掘风险信息，以实现风险管理。由于应纳税额的数量与公司的整个生产经营有关，税务相关数据自然包括纳税人及其经营信息。根据税务数据的性质，用于税务风险检测的输入数据可以分为上下文属性和行为属性。

#### 2.2.1. 上下文属性

上下文属性用于确定实体对象的上下文和固有属性。本研究选择了一些与税务风险检测相关的重要上下文属性，如表1所示。这些上下文属性包括三类：注册信息、财务报表和业务信息。因此，属性类型可以分为三类：数字、枚举和文本。

#### 2.2.2. 行为属性

行为属性定义了实体对象的非上下文特征，并描述了这些实体对象之间的各种类型的关系，如上/下游信息和交易金额。本研究选择了一些与税务风险检测相关的重要行为属性，如表2所示。行为属性可分为两类：统计信息和上下游信息。

表1 上下文属性

Category	Attributes	Type
Registration information	Registration type	Enum
	Taxpayer current status	Enum
	Industry code	Enum
	Registration address	Text
	Business scope	Text
	Registration capital	Number
Financial statements	Total investment	Number
	Annual sales	Number
	Profit margin	Number
	Total investment	Number
Business information	Number of employees	Number
	Age of legal person	Number
	Corporate credit rating	Enum
	Business items	Text

表2 行为属性

Category	Attributes	Type
Statistical information	Average transaction value	Number
	Transaction value variance	Number
	Total transaction value	Number
	Median transaction value	Number
	Minimum transaction value	Number
	Maximum transaction value	Number
	Average tax rate	Number
Up-/down-stream information	Proportion of upstream invoices	Number
	Proportion of downstream invoices	Number

2.3. 税务风险检测技术的发展

税务风险检测是有效处理税务风险的实践，是国家税收治理水平的集中体现。税务风险检测经历了两个主要的演变阶段：传统的选案和基于数据挖掘的选案。

(1) 传统选案。早期，税务风险检测主要采用传统的选案方法，该方法可进一步细分为基于报告的选案方法、基于人工的选案方法和基于规则的选案方法。基于报告的选案方法主要依赖于报告信息，具有很强的偶然性。基于人工的选案方法主要依靠财税专家的人力资源。值得注意的是，随着经济的快速发展，财税数据的总量呈爆炸式增长，不可能再通过人工检查对所有企业进行充分的风险检测。基于规则的选案方法通常采用专家经验来定义规则，然后建立一个基于规则的推理系统来识别财政和税务数据中的风险点。这种基于规则的选案方法依赖于税务专家在审计工作中的经验和知识，往往存在主观性强和滞后性（即规则不能及时更新）等问题，难以发现新的税务风险行为。

(2) 基于数据挖掘的选案。为了减轻传统选案方法的局限性，基于数据挖掘的选案方法在国内外得到了广泛的研究。该方法通过对历史数据的不断学习来指导税务审计工作。由于基于数据挖掘的税务风险检测方法与传统选案方法相比具有更多优势，前者取得了优越的性能，因此受到了广泛的关注。自1999年以来，国内外每年发表的关于基于数据挖掘的税务风险检测方法的论文数量见图1。从图中可以看出，基于数据挖掘的税务风险检测的研究越来越受到研究人员的关注，过去20年发表的关于这一主题的论文数量总体上呈增长趋势。

根据输入数据的使用情况，基于人工智能和数据挖掘的税务风险检测方法可分为两类：非基于关系的税务风险检测和基于关系的税务风险检测。一般来说，非基于关系的方法只使用纳税人的上下文属性（参见第2.2.1节）来识别风险，而不考虑纳税人之间的相互作用。但实际上，在一个税务场景中，不同的实体对象之间存在着各种类型

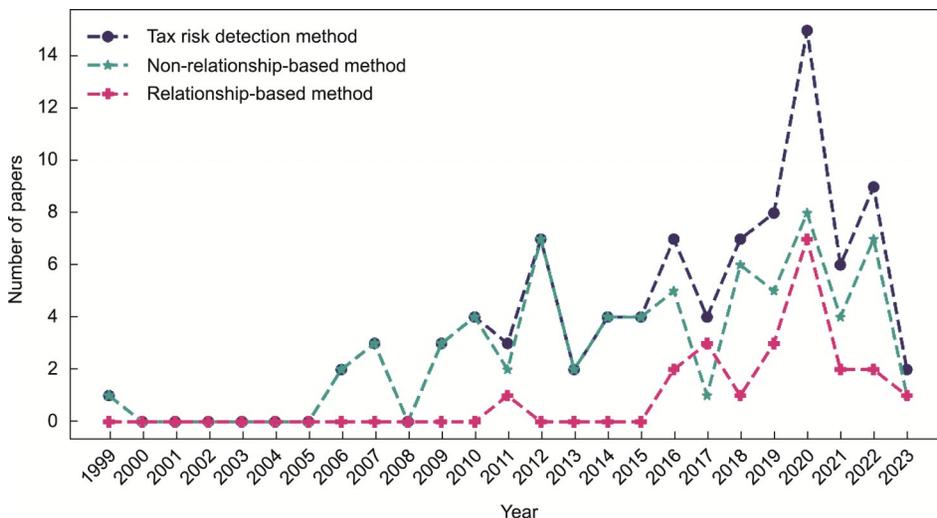


图1. 税务风险检测的研发趋势。

的关系。为了充分利用税务场景中实体之间丰富的行为属性（见第2.2.2节），产生了基于关系的风险检测方法。现有的税务风险检测方法可进一步分为14种类型，如图2所示。这14种方法将在第3节和第4节中进行更详细的讨论。

### 2.3.1. 非基于关系的税务风险检测

为识别风险个体，非基于关系的税务风险检测方法首先提取风险个体的相关特征，然后对分类器进行训练，最后进行风险检测。如图3所示，这些方法只使用风险个体的上下文属性（参见第2.2.1节），不考虑他们之间丰富的交互信息，即行为属性。

### 2.3.2. 基于关系的税务风险检测

如上所述，税务场景包含不同类型的实体上下文以及

它们之间丰富的交互信息。但是，非基于关系的方法未深入挖掘描述纳税人之间相互作用的行为属性。为充分利用实体之间丰富的交互信息，基于关系的风险检测方法将风险个体的特征与它们在税务交易网络中的关系和结构特征整合在一起，以便从风险群体的角度来识别风险。如图3所示，这些方法既使用了纳税人的上下文属性，也使用了他们之间共享的行为属性（见第2.2.2节）。

非基于关系的数据挖掘方法比基于关系的方法发展得更早，并且非基于关系的方法相关的研究工作也更多。如图1所示，自2006年以来，许多学者都采用了非基于关系的数据挖掘方法来识别税务风险。这些方法仅利用税务相关实体的上下文属性（见第2.2节），通常采用特征工程等方法对纳税企业的数据进行分析，然后选择一套能够反映纳税企业风险的特征（如个人特征、业务特征、税务特

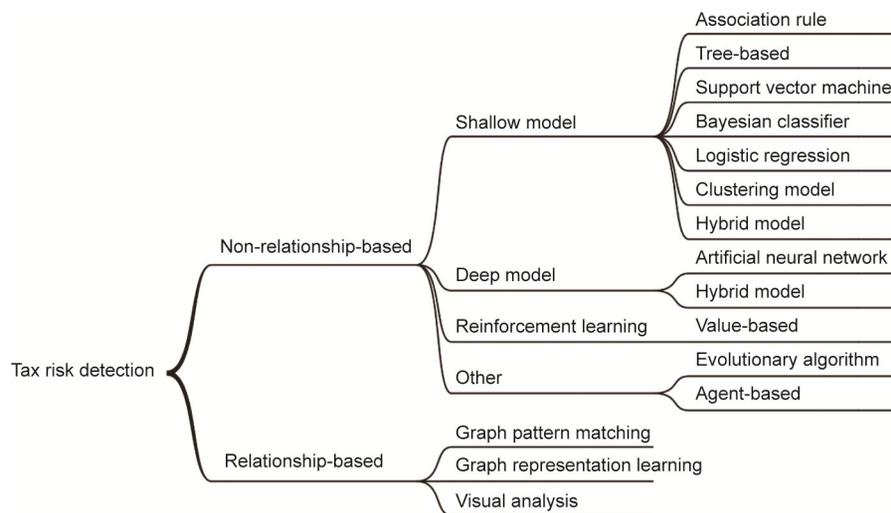


图2. 税务风险检测方法的分类。

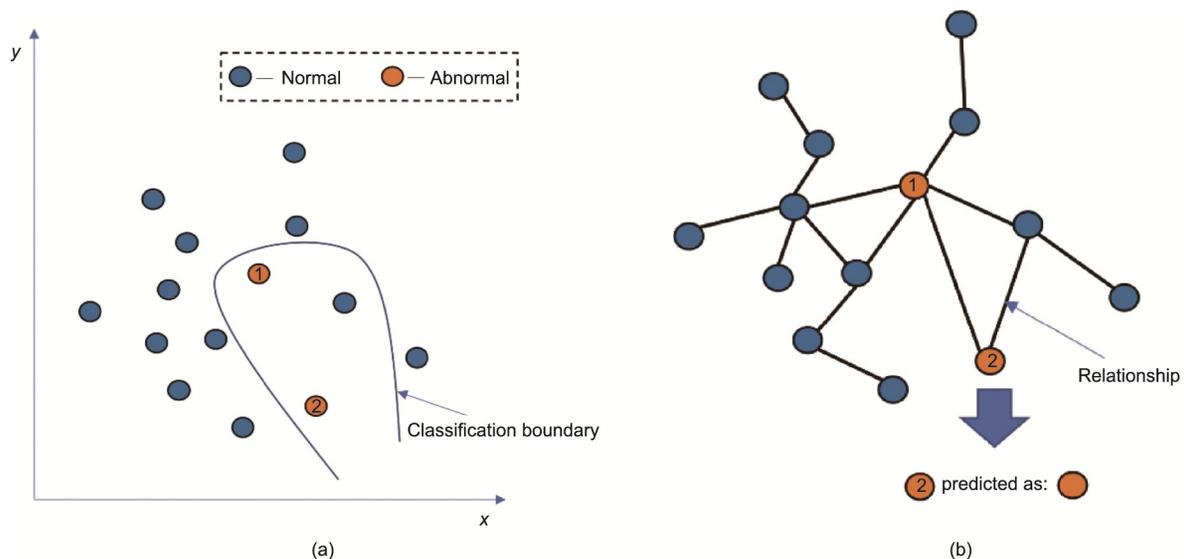


图3. 非基于关系的税务风险检测和基于关系的税务风险检测的差异。(a) 非基于关系的税务风险检测；(b) 基于关系的税务风险检测。

征、账单特征等), 根据所选特征[通过支持向量机(SVM)、聚类模型等]训练分类器。随后, 为充分利用税务场景中各实体之间的交互关系, 开发了基于关系的数据挖掘选案方法。2016年以后, 学者们逐渐开始利用税务网络中的复杂关系来识别风险。由于同时使用上下文属性和行为属性(见第2.2节), 基于关系的方法可以更容易地从税务网络中包含的复杂结构信息和丰富的语义信息中挖掘更深层次的知识, 从而提高风险检测的准确性。税务风险检测技术的趋势是, 模型在税务场景中关注尽可能多的信息, 而不是仅仅探索公司的上下文特征。

## 2.4. 税务风险检测的问题定义

在税务风险检测问题中, 各种对象及其交互可以被建模为  $G(V, E)$ , 其中  $V$  是税务场景中的实体集, 包括多个实体(如纳税人), 而  $E$  是实体之间的关系集。  $N$  是  $G$  中所有实体的数量,  $F$  是上下文特征的维度数, 所有实体的上下文特征被定义为  $X \in \mathbb{R}^{N \times F}$ 。  $E \in \mathbb{R}^{N \times N \times P}$  表示  $G$  中行为特征的矩阵,  $P$  是行为特征的维度,  $\mathbb{R}$  是实数空间,  $E_{ij} \in \mathbb{R}^P$  表示税务实体  $i$  和税务实体  $j$  之间的行为特征。税务风险检测模型的目标是学习一个映射函数  $f$ , 它可以基于上下文特征、行为拓扑信息和行为特征来发现纳税人的风险行为。形式表示如下:

$$Y = f(V, E, X, E) \quad (1)$$

其中,  $Y$  为所有纳税人的风险得分向量, 得分越高, 意味着风险水平越高。

## 3. 非基于关系的税务风险检测方法

### 3.1. 非基于关系的浅层模型

#### 3.1.1. 关联规则

关联规则是一种基于规则的机器学习方法, 是数据挖掘领域中最重要技术之一。它用于发现大量数据[6-7]中某些属性之间的相关性和模式。

Wu等[8]使用增值税数据库的关联规则来发现增值税逃税报表中属性之间的模式和关系。研究人员根据增值税逃税报告中出现的具体模式或规则开发了一个筛选框架, 然后筛选与增值税报告不匹配的案例进行进一步审计。该模型有助于税务审计人员更有效地进行逃税检查, 并在筛选逃税案件时提高命中率。

Matos等[9]对巴西国内的逃税行为进行了调查。研究人员应用关联规则来识别税务欺诈模式, 并应用降维方法(即主成分分析和奇异值分解), 根据纳税人从事欺诈行为

的可能性, 对其进行欺诈规模排名。研究表明, 该模型的识别准确率为80%。

关联规则算法操作简单, 其结果易于理解。然而, 随着数据量的增加, 由于候选集[10]数量的增加, 计算复杂度也显著增加。

#### 3.1.2. 基于树的模型

基于树的模型, 也被称为决策树, 是最著名的机器学习算法之一, 通常用于涉及统计和数据挖掘的任务[11-12]。基于树的模型通常包含一个根节点、几个内部节点和几个叶节点。叶节点表示决策结果, 其他节点表示对属性的判断, 每个分支表示一个判断的输出。

Bonchi等[13]使用了案例研究来说明如何使用基于决策树的分类技术来协助设计审计策略。这类研究需要在最大化审计收益和最小化成本之间进行权衡。研究人员认为, 演绎推理(如逻辑数据库支持的推理)和归纳推理(如决策树支持的推理)的适当整合可以为许多问题提供有效的解决方案。在评价阶段, 联合使用这两种推理方法尤其有效。

Mittal等[14]应用了一种基于随机森林的分类器来识别德里增值税系统中的欺诈企业。该分类器使用来自税务官员的税务数据和报告作为训练集, 来预测企业欺诈的可能性。实验表明, 税务管理部门可以通过这种方法追回因欺诈而造成的数千万美元的损失。此外, 研究人员认为, 每个税收管辖区都有其独特的特点, 这意味着这项工作需要与政策高度相关。

Yao等[15]提出了一种检测金融欺诈的混合方法。研究人员结合了特征选择和分类算法来优化他们的模型。计算并分析了影响欺诈行为的因素, 考虑了变量数量对模型的影响, 并通过实验比较了五种机器学习算法的性能。结果表明, 该随机森林算法性能良好, 适用于高维数据的分析和处理, 可以有效地避免过拟合问题。

Wu和Luo[16]提出了一种基于随机森林的逃税检测方法。该研究以汽车销售行业为对象, 以经营数据、纳税人属性和经营特征为输入, 采用随机森林模型识别有逃税行为的纳税人。在构建随机森林的过程中, 采用  $k$  倍交叉验证的方法选择最优的决策树数量。该实验还将随机森林与AdaBoost、逻辑回归(LR)及其他算法进行了比较。结果表明, 随机森林在该任务中具有最高的准确性, 能够精确地检测逃税行为。

An和Suh[17]提出了一种构建分类模型的方法, 在识别财务报表欺诈的任务方面取得了优异的性能。他们进一步提供了可用于解释分类结果的决策规则。该模型是对随

机森林算法的一大改进，具有较好的分类性能，同时能够提取分类规则。本研究解决了类别不平衡的问题：研究人员将不平衡数据集划分为多个平衡子数据集，在每个子数据集中随机选择特征，并训练适当数量的分类和回归树决策树。最后，利用测试数据筛选出精度最高的模型；该最优模型被称为修正随机森林（MRF）模型。然后使用MRF模型来检测财务报表欺诈行为。

考虑到专家经验与机器学习相结合是一种可行的控制税务风险的方法，Ji和Wang [18]选择某些商业企业作为实验案例，构建随机森林算法，建立检测模型，以评估非法开具虚假发票的风险。实验结果分析表明，该模型具有较高的准确性，可作为税务稽查员的参考。Andrade等 [19]提出了一种基于机器学习的系统，通过对公司的财务数据进行分类，来检测巴西圣埃斯皮里托州的税务欺诈行为。对四种不同的分类器—— $k$ -最近邻、随机森林、SVM和神经网络——进行了训练和测试，其中随机森林获得了在宏平均 $F_1$ 分数上表现最佳，达到了92.98%。该系统可以减少81%的人工工作量，减少了15%的欺诈性公司。未来的工作包括整合新的特性、解决数据不平衡的问题以及跨地理区域转移学习。

Xavier等 [20]提出了一种利用开放和公开数据识别逃税公司的解决方案，通过随机森林模型实现了超过98%的准确率。研究人员强调了使用公共数据来解决逃税问题的可行性，并展示了使用神经网络来处理异构图和关系图的潜力。报道的系统已经被税务稽查员和税务代理使用，表明其实际应用价值。总之，本文提供了一种利用开放数据和人工智能进行逃税识别的很有前景的方法。

总的来说，基于树的模型表现良好，可以处理缺失属性的高维样本，并产生易于理解和解释的结果。但是，基于树的模型也容易发生过拟合，尽管随机森林和树剪枝技术可以缓解过拟合 [21]。最后，树形模型很难支持在线学习，而且在这些情况下，通常需要重新构建决策树。

### 3.1.3. SVM

SVM是一种分类模型——更具体地说，是在特征空间 [22–23] 上定义最大间隔的二值线性分类器。其学习策略是最大化分类间隔，可以形式化为一个凸二次优化问题。除了处理线性分类任务外，SVM还可以使用内核技巧隐式地将输入映射到高维空间中，有效地执行非线性分类。

Wang和Li [24]介绍了在税务欺诈检测中使用SVM。该研究将这项任务看作是一个具有“可信”和“不可信”类别的二元类别问题。本实验对青岛市61家零售企业的

增值税支付情况进行了测试，并采用SVM来确定企业的类别。最终的准确率达到了87.10%。

Liu等 [25]结合粗糙集理论和SVM的优势，提出了一种新的税务评估模型。首先建立税务评价指标体系，然后利用粗糙集理论对评价指标的属性进行简化。然后将简化后的指数作为SVM的输入，从而形成了模型的整体框架。值得注意的是，本研究中SVM的核函数采用了径向基函数核函数。实验结果表明，该模型性能良好；此外，结合粗糙集理论比单独使用SVM具有更高的精度和更短的训练时间。

Xia和Li [26]提出了一种将SVM与自组织地图（SOM）相结合的税务检测方法。首先，使用SVM对纳税人进行分类。在SVM训练过程中，还引入了一种遗传算法来利用其优良的搜索特性。然后将分类的纳税人信息作为输入，并使用SOM对纳税人进行集群分析，以便于审计人员进行进一步检查。

Junqué de Fortuny等 [27]采用结构化和细粒度的发票数据进行欺诈检测，构建了一种具有高效、易于使用的税务欺诈检测方法。他们关注的是在比利时的外国公司之间的交易发票数据。分析结果表明，输入数据具有高维性、高稀疏性的特点。因此，可以使用两种不同的方法来分析输入数据：一种是SVM或朴素贝叶斯，另一种是在图表示上的关系学习。在考虑了性能和可解释性之间的权衡后，最终选择了线性SVM模型。

Rad和Shahbahrani [28]分析、设计并实现了一个预测高风险纳税人的系统，用于预测纳税人的行为并帮助税务稽查员解决在税务审计过程中遇到的问题，以防止逃税。该方法将回归与SVM相结合，并在选择数据时优先考虑高收入纳税人。

Zhang [29]提出了一种基于SVM的企业增值税发票误发检测模型。研究人员设置了一个风险系数，并将企业划分为不同的层次，以表明其开具虚假发票的可能性。

SVM背后的想法很简单。它对小规模数据的分类效果好，泛化能力强。然而，它也具有较高的计算复杂度，并且在处理大规模数据时对缺失的数据很敏感。此外，SVM通常难以在不平衡比率非常大的数据集上表现良好。

### 3.1.4. 贝叶斯分类器

贝叶斯分类器是基于贝叶斯定理 [31–32] 的统计推理过程；它利用有关参数的先验信息和由现有数据的统计模型计算出的似然概率来获得一个未知参数的后验概率。贝叶斯分类器是统计学中的一种重要技术，特别是对序列数据的动态分析尤为重要，广泛应用于科学、工程、医学等

领域。

Kirkos 等[33]比较了三种数据挖掘技术,即决策树、神经网络和贝叶斯信念网络,来检测财务报表数据中的欺诈行为。通过实验验证,确定贝叶斯信念网络模型的性能最好,准确率为90.3%。这项研究可以帮助当局发现财务报表欺诈行为。

Kang 和 Yu [34]构建了一种基于贝叶斯分类模型的税务评估方法,并对真实数据进行了实证分析。结果表明,贝叶斯分类税评估模型具有广泛的应用前景。Zhang 等[35]提出了一种基于贝叶斯分类器的纳税申报欺诈检测方法,该方法可以确定一个企业的纳税申报金额是否异常。Lenz [36]还研究了贝叶斯方法在税务欺诈检测中的应用,并在德国的案例中验证了该方法。

贝叶斯分类器具有相对坚实的理论基础[37],更稳定,对缺失数据的敏感性较低。缺点是假设样本属性相互独立;因此,当样本属性不满足独立性假设时,效果是有限的。需要注意的是,在税务情景中,所选属性之间往往存在一定的相关性。

### 3.1.5. LR

LR 是多变量分析[38]的一种形式,是计算机科学、计量经济学、生物统计学和其他学科中常用的方法。简言之,LR 是一种解决二元分类问题的机器学习方法,用于估计某事发生的可能性。

Qi [40]建立了一个基于实际情况的索引体系。研究人员使用 LR 模型来区分税务案例,提高了准确性和效率。Wang 等[41]选择了9个财务指标来进行税务案例的选择,将税务审计视为两类问题,并采用 LR 模型来预测案例的类型。Su [42]以广州的一些批发企业为样本,建立了批发行业税务审查的 LR 模型。研究结果表明,为了合理解释税务合规行为,有必要使用具有显著特征的指标。利用这种方法,可以为不同的地区和行业构建不同的税务审查模型,以取得最佳的效果。Yuan [43]总结了纳税人常用的五种逃税方法,并利用 LR 模型构建了一个识别特定城市的企业逃税行为的税务审查模型。该模型的准确率达到79.5%。

LR 是一种简单高效、时间短、空间复杂度低的算法。但是,LR 本质上也是一个线性分类器;因此,在高维特征空间中很难发现特征之间的相关性,容易出现欠拟合[44]。

### 3.1.6. 聚类模型

大多数现有的使用人工智能进行税务风险检测的工作

都是基于有监督或半有监督的机器学习技术。然而,对纳税企业的审计过程通常需要富有经验的专家进行深入分析,耗时较长。因此,可用的历史逃税信息数量有限,特别是标记数据,这严重阻碍了某些有监督的机器学习模型在税务风险检测中的使用。这促使一些研究人员使用聚类模型[45–46]这种无监督的方法来识别税务风险。

Denny 等[47]提出了一种基于 SOM 的可视化方法在澳大利亚税务局的客户数据集中挖掘异常热点集群。SOM 将高维数据映射到二维空间,其中相似的实体在一起往往更接近。SOM 还提供了各种可视化功能,使非技术用户能够探索数据集,并帮助分析人员制定策略。

Liu 等[48]在税务审计案例的选择中使用了分层聚类的方法,对30家企业的指标数据进行了层次聚类分析,并将分析结果与已知的逃税案件进行比较,有助于选择案例,提高税务审计的效率和效果。Liu 等[49]提出了一种基于聚类的数据挖掘算法来挖掘税务行业中的离群值问题。该方法可以在大量的税务数据中发现异常情况,不仅可以过滤关键数据源,还可以用于检测纳税人的异常经营行为。该方法甚至可以确定纳税人是否涉嫌逃税和税务欺诈,使其能够快速准确地识别出进行税务审计的候选人。

Assylbekov 等[50]提出了一种基于 Kohonen SOM 的无监督方法来检测哈萨克斯坦法人实体之间的增值税逃税行为。结果表明,该方法优于哈萨克斯坦共和国国家税务委员会目前采用的评分模型。De Roux 等[51]提出了一种新的基于无监督聚类的方法来检测纳税人之间潜在的欺诈行为。对哥伦比亚1367份纳税申报单的实验结果表明,可以在不需要历史标记数据的情况下提高税务监督程序的操作效率。Xia 等[52]提出了一种改进的  $k$  均值聚类算法。该方法采用无监督学习模型,对房地产企业股权转让过程中的税务风险进行了分析和评估。实验结果验证了该方法的有效性。

该聚类算法简单,易于实现,不需要标签信息,非常适合用于税务场景,因此引起了广泛的研究关注。然而,聚类算法往往对噪声和异常值[53–54]很敏感,而且它们在大规模数据集上的收敛速度非常慢。

## 3.2. 非基于关系的深度模型

### 3.2.1. 神经网络

神经网络属于机器学习和认知科学领域,是模拟生物神经网络[55]的结构和功能的数学模型。一个典型的神经网络有三个元素:结构、激活功能和学习规则。近年来,随着计算能力和理论基础完整性的提高,神经网络的深度

限制得到了缓解，新提出的深度学习方法重新点燃了学术界和工业界对神经网络的关注。目前，神经网络被广泛应用于计算机视觉[56]、数据挖掘[57]、机器翻译[58]及其他领域[59]。

Li和Xiao [60]将模糊逻辑理论与神经网络相结合，充分发挥了这两种算法的优势，包括模糊逻辑理论对特定问题的调整能力和神经网络的非线性逼近能力。研究人员首先构建了税务抵免评价指标体系，然后建立了基于模糊神经网络的税务评价模型。最后，通过仿真分析得到了仿真结果，结果表明，该模型非常适合于纳税企业的信用评价任务。

Lin等[61]结合了专家问卷和数据挖掘技术，对财务报表中欺诈因素的重要性进行排序，然后对报表欺诈进行分类和识别。该研究中使用的数据挖掘技术包括人工神经网络、LR模型和决策树。实验结果表明，人工神经网络的分类效果优于决策树模型或LR模型，前者的分类准确率为92.8%。研究人员认为，基于神经网络的识别方法可以有效地帮助审计人员完成工作。

Ioana-Florina和Mare [62]通过对财政行为建模，利用人工神经网络检测纳税人行为中的税务欺诈风险。Pérez López等[63]使用神经网络来计算纳税人之间逃税的概率。研究人员根据西班牙的税务数据验证了该模型，发现其准确率达到84.3%。Zhang等[64]提出了一种基于机器学习的工具，以帮助税务机关检测社交媒体平台上基于交易的逃税行为。更具体地说，采用多模态深度神经网络自动检测平台上的可疑行为，能够大规模识别基于电子商务的逃税行为。Chen等[65]提出了一种基于人工神经网络的税务评估方法，同时考虑到该神经网络的特点使其能够有效地适应非线性税务数据。

Zhang等[66]开发了一种Regtech工具，可以自动检测社交电子商务中基于交易的逃税活动。收集了一个数据集，并手动标注了与销售和逃税活动相关的多个标签。开发了一个多模态深度神经网络模型，自动检测基于交易的逃税活动。实验结果表明，该模型的性能优于任何单一模态模型。

Murorunkwere等[67]使用人工神经网络来检测卢旺达国内的所得税欺诈行为。该模型获得了较高的准确性、精确度和召回率评分，该研究提供的证据可以帮助审计人员减少审计时间和成本，并恢复损失的收入。Mojahedi等[68]采用了一种改进的粒子群优化（IPSO）算法来优化多层感知器（MLP）神经网络和SVM分类器。采用IPSO算法的IPSO-MLP模型和IPSO-SVM模型作为逃税检测的新模型。该系统根据从伊朗西阿塞拜疆省税务事务总局收集

的数据集进行了评估，该数据集有1500个样本。实验结果表明，IPSO-MLP模型的表现优于其他模型，准确率为93.68%。

Alsadhan等[69]提出了一种异常检测技术，用于识别税务欺诈，而不需要带有历史标记的数据。该技术使用堆叠的自动编码器（SAE）来比较纳税申报表上每个字段的可疑值的概率分布。结果表明，该方法对识别现行欺诈方案是有效的。讨论了潜在的限制和未来的扩展，如增加额外的财务比率与增长相关的特征以及在计算异常评分时纳入税务专家的意见等。研究人员提出了一种结合监督和无监督检测方法的监督审计策略，以获得最优的审计策略。

神经网络在许多领域都取得了优异的性能，其强大的性能是第三波人工智能兴起的重要原因。但是，人工神经网络仍然存在一些问题，包括需要大量的标记训练样本来训练模型，以及模型的可解释性[70–71]较差。遗憾的是，在税务场景[72]中，数据标签特别难以获得，因为在这种情况下，标签需要大量的专家知识。此外，模型的可解释性在税务领域尤为重要，因为它可以为审计人员提供线索。

### 3.2.2. 混合模型

一些研究使用集成学习或将任务分为多个阶段，来集成风险检测模型。混合模型是一种结合两种或两种以上不同的模型，利用各自的优势弥补不足，以获得良好的识别结果[73]的方法。Ravisankar等[74]采用多种数据挖掘技术（如多层前馈神经网络、SVM、遗传规划、数据处理的群组方法、LR和概率神经网络）对202家拥有35个财务项目的中国公司的财务报表欺诈行为进行了分析。结果表明，概率神经网络和遗传规划取得了特别好的性能。

Zheng [75]应用决策树和回归建模方法构建了纳税人规避风险评级的回归模型，利用聚类分析、离群值分析和关联规则建立行业交易规则库。González和Velásquez [76]使用了诸如SOM的聚类算法来识别具有类似行为的纳税人群体。随后，使用决策树、神经网络和贝叶斯网络来识别与欺诈或非欺诈行为相关的变量，并检测相关行为的模式，从而生成知识，帮助智利税务当局识别欺诈行为并相应地检测税务犯罪。

Song等[77]提出了一种将机器学习方法与基于规则的系统结合起来以评估财务报表欺诈风险的混合方法。该机器学习模型采用了由LR、神经网络、决策树和SVM四种模型组成的集成学习模型。当应用于2008—2012年期间的550家公司的数据时，该方法在评估财务报表欺诈风险

方面优于机器学习方法。Rahimikia等[78]研究了一种混合智能系统，该系统将MLP、SVM和LR分类模型与和声搜索优化算法相结合，以检测伊朗国家税务总局获得的数据中企业逃税的有效性。在食品和纺织行业，准确率分别达到90.07%和82.45%。Wu等[79]提出的基于正样本和无标签（PU）学习的逃税检测方法（TEDM-PU）利用有限的标记数据和大量的未标记数据来检测逃税行为。该方法采用随机森林模型对税务数据进行预处理，然后基于PU学习对未标记样本进行伪标签分配，最后使用LightGBM进行逃税检测。

Javadian等[80]提出了一种改进的ID3决策树模型，并通过遗传算法优化的多层感知器神经网络相结合，以提高其性能和精度。他们对在德黑兰证券交易所上市的公司财务报表进行的研究，验证了所提出的模型的有效性。Rahman等[81]在2005—2015年在马来西亚证券交易所上市的3365家公司的真实数据集上测试了五种机器学习算法（LR、最近邻算法、朴素贝叶斯、决策树和随机森林）。Mekonnen [82]利用数据挖掘来检测和预测埃塞俄比亚首都亚的斯亚贝巴的纳税人的逃税行为。根据Cios模型，研究人员开发了一个使用K-means算法的聚类模型和基于多层感知机算法结合部分关联规则（PART）的分类模型。该模型获得了较高的准确性并识别出了重要的变量，如税收、负债和支出。Savić等[83]提出了一种混合的无监督异常检测方法，该方法结合了K-means和自动编码器来进行鲁棒离群值检测，并使用决策树为检测到的离群值获得一个可解释的代理模型。该方法在来自塞尔维亚税务管理局的两个数据集上进行了评估，结果显示，它可以识别出90%~98%的内部验证的异常值，这取决于所使用的聚类配置和正则化机制。

Baghdasaryan等[84]探索了机器学习工具的使用（更具体地说，是梯度提升），为亚美尼亚企业纳税人开发了一个欺诈预测模型。梯度提升机按顺序建立模型，每个后续模型（即决策树）的目的是减少之前模型的误差。每个节点在不同的子集中获取特征，从数据中寻找不同的信号。该模型成功地从纳税申报单中获得了重要特征，包括历史欺诈和审计、行政成本分担和外部经济活动。研究人员证明，即使是适度精确的模型也可以提高现有的基于规则的方法的准确性，纳税人的供应商和买方网络中包含的信息可以用作欺诈的预测因素，这对新成立的公司尤其有用。

由于混合模型[85]是由多个模型组成的，因此可以结合每个模型的优点，以获得更好的识别结果，同时提高模型的鲁棒性和可靠性。但是混合模型也存在一些缺点，如

需要更多的计算资源和更复杂的参数调优过程。此外，混合模型需要更多的数据来进行训练和测试，以获得更好的性能，这使得它们在资源匮乏的情况下不太理想，例如在税务情况下，获取数据标签被证明更具挑战性。

值得注意的是，由税务专家对大量数据贴上标签是一个漫长而昂贵的过程。此外，不同地区的经济政策和模式的差异导致了数据分布的不同特征。现有的模型通常不考虑跨区域的使用。因此，出现了一些基于迁移学习思想的混合模型。

Zhu等[86]提出了一种基于迁移学习的区域间逃税检测方法。该方法通过结合基于特征和基于实例的迁移学习，可以获得源区域的补充知识和足够的训练数据，然后将其应用于具有稀疏标签的目标区域，以便在存在区域差异的情况下增加训练数据。Wei等[87]提出了通用的无监督条件对抗网络（UCAN）架构，并将其应用于跨区域逃税检测。该体系结构使用其他审计任务的标记数据来帮助使用稀疏标记的目标审计任务，并减少类内分布差异。无监督特征转移的端到端学习是通过结合分布适配器和标签预测器来实现的。Zhang等[88]提出了一种基于PU学习的可转移逃税检测方法。该方法将PU学习与深度迁移学习相结合，解决迁移过程中边际概率分布和条件概率分布的迁移问题。迁移学习非常适合于税务等低资源场景，可以有效地利用数据[89]。但是，该方法仍然存在一些问题：首先，由于源域和目标域可能不同，算法难以收敛；其次，目标域中的算法可能会继承源域[90]的缺陷。

### 3.3. 非基于关系的强化学习模型

强化学习[91–93]强调通过学习策略与环境的互动，来最大化预期的利益。但是，很难设计出奖励函数并保证强化学习算法的收敛性。关于基于强化学习的风险检测的研究相对较少。

Abe等[94]提出了一种新的基于约束马尔可夫决策过程的强化学习框架，该框架紧密结合了数据建模和优化技术。研究人员在纽约州税收和财政部部署了这个系统。Goumagias等[95]结合了深度强化学习和Q学习，以确定纳税人之间的预期逃税风险行为。研究人员将希腊的税收体系作为一个具体的案例研究，并报告了有关公司的预期行为、利润报告的激励措施、风险规避和政策影响等问题的相关性。

综上所述，强化学习[96–97]具有优化性能和长时间维持变化的优势。然而，强化学习也存在状态过载的风险，可能会对结果产生负面影响。此外，只有在拥有足够的计算能力和数据的情况下，强化学习才能展示其在解决

通过其他方式难以解决的复杂问题方面的独特优势，而这在税务场景中往往难以实现。

### 3.4. 其他非基于关系的模型

#### 3.4.1. 进化算法

进化算法[98-99]是进化计算领域的一个分支。进化算法的机制受到生物进化的启发，通过模拟生物进化的过程，在解空间中寻找最优解。Alden 等人[100]采用遗传算法和分布估计算法，训练基于模糊规则的分类器进行金融欺诈模式检测。结果表明，遗传算法和分布估计算法比传统的 LR 模型更有效地进行企业看不见数据的分类，能够有效地检测财务欺诈。通过 10 倍交叉验证，两种算法的分类准确率分别达到 75.47% 和 74.26%。Warner 等[101]提出了一种原型进化算法，以资产类型、税务实体和实体之间的交易规则集作为输入。该算法为审计人员提供了有关逃税行为的方案信息。这些方案使用“适应度函数”进行排名，最佳的方案将获得最高的税收减免和最低的惩罚。

Hemberg 等[102]认为，逃税计划和审计程序是一种竞争关系。这种相互的影响与进化的本质非常吻合。研究人员提出了一种共同进化模型，用来模拟纳税人网络和审查制度的交易序列。该模型有助于税务机构模拟税法或审查制度的变化如何导致逃税方案的演变。此外，第二年，Hemberg 等[103]提出了通过启发式来模拟逃税和法律的方法，旨在通过模拟逃税方案与审查制度的共同进化来预测逃税。研究人员探讨了为应对审计程序的变化而出现的税收方案。最后，实验验证了使用该方法检测逃税行为的可行性。

进化算法的灵感来自于生物进化，这很容易理解。但是这些方法也有许多参数，而且参数的选择往往依赖于经验。不适当的参数导致收敛速度较慢，并对结果产生严重的负面影响[104-106]。

#### 3.4.2. 基于代理的模型

基于代理的模型[107-109]，也被称为多智能体系统，是用于模拟具有自我意识的独立个体的行为和互动的计算模型。目的是评估个人在系统中的角色。基于代理的模型通常用于计算机科学、经济学、社会科学、生物学和其他领域。这样的模型可以模拟复杂的现象，尽管它们需要预设许多参数。

Antunes 等[110]使用基于代理的模型来探讨逃税的原因。研究人员认为，基于代理的模型在探索税收合规问题方面是有效的，因为它可以为基于个人动机的决策提供实证解释。此外，基于代理的模型还可以探索个体心理、智

能体互动和社会机制。这种强大的解释力可以用来预测社会制度的未来，进而可以用来设计一个减少逃税的税收监管制度。实验研究表明，基于代理的个性化模型可以帮助审计人员更有效地检查逃税问题。

Lima 等[111]采用了一种基于代理的蒙特卡罗模拟方法，并在 Zaklan 模型中加入了一种有噪声的多数投票方法，然后将该方法应用于阿波罗网络上的逃税检测。本研究的目的是测试 Zaklan 模型在阿波罗网络上的稳健性，并验证以往基于该方法的逃税检测结果。实验结果表明，本研究提出的基于多数投票的 Zaklan 模型具有高度的鲁棒性，可以为逃税审计提供有效的帮助。此外，研究人员认为，被审查打击的可能性越高，惩罚也越强，那么发生的逃税行为就越少。

Llacer 等[112]提出了一种新的基于代理的模型，用来模拟税收规则和逃税行为。本研究从三个不同的方面进行了探讨：理论上，研究了支持逃税的因素（效用最大化、公平性、社会影响）之间的相互关系；系统上，基于代理的方法构建的模型更具真实性（如通过赋予个体独特的特征）；政治上，那些被证明有效的模型更有可能成为评估现有税收政策和发现逃税行为的有用工具。该模型被应用于西班牙的实际案例。结果与理论预期基本一致，支持了模型的可靠性。

Noguera 等[113]认为，在税收行为分析领域，基于代理的模型在测试理论和假设方面非常有效。本文提出了一种基于代理的税收规则模拟模型，该模型将理性选择与社会影响规则相结合，生成了税收行为的聚合模型。实验验证了该模型的潜力。

Andrei 等[114]认为，基于代理的模型不仅灵活，而且具有很强的分析能力，在应用于税收规则和逃税机制等复杂问题时取得了良好的效果。研究表明，网络结构对税收规则的动态有重大影响，这表明，靠近网络中心的纳税人更愿意申报他们的所有收入，特别是在面临巨大的罚款时。这项工作还揭示了，在建模税收规则时，网络结构应该被认为是一个重要的因素，因为不同的拓扑结构可能会导致不同的结果。值得注意的是，本研究中提出的模型比现实世界中的逃税更具程式化和抽象性。研究人员计划通过结合特定案例的社会经济和政治背景来优化模型的表现。

Bloomquist [115]比较了三种基于多代理的个人所得税逃税检测模型。研究人员讨论了这些模型之间的异同以及基于多代理的模型在该领域的优势。相似之处在于这些模型的同质性、实例化的代理数量等等，而差异在于用于验证模型的外部数据、评估审计效果的能力、代理的特

点、具体的实现等等。通过比较分析, 研究人员得出结论, 从他们的研究中得到的最重要的启示是, 在开发政策分析的计算模型时, 过程有效性非常重要。他们进一步强调了在进行研究时避免使用黑箱技术的重要性; 尽管这种技术很流行, 但可能会让从实际角度研究情况的专家感到困惑。

基于代理的模型[116–117]具有几个优点, 如对异构种群建模、用最小编码对复杂系统建模的能力以及模拟具有自我意识的独立个体的行为和交互的能力。但是基于代理的模型也存在一些缺点, 如计算要求高、对参数值的敏感性高以及难以验证结果等。然而, 在模拟税收等复杂现象时, 这种模型需要预先设置许多参数。基于代理的模型的动态特性取决于代理规则和属性的参数设定, 不同的设置可能导致完全不同的行为模式和系统属性。找到一个合理而稳定的参数化可能是一项艰巨的任务。此外, 由于它们是基于规则的模拟, 因此确定它们是否产生与现实世界相匹配的紧急行为和属性也具有挑战性。

### 3.5. 总结

上文总结了现有的非基于关系的风险检测方法。每种技术的优缺点和具体文献分析列于表3 [8–9,13–20,24–29,33–36,40–43,47–52,60–69,74–84,86–88,94–95,100–103,110–115]。

表3 非基于关系的风险检测方法总结

Method	Advantages	Weakness	References
Association rule	Simple; results are easy to understand	As the amount of data increases, the amount of computation increases rapidly	[8–9]
Tree-based	Easy to understand and interpret; ability to handle missing attribute samples	Prone to overfitting; difficult to support online learning	[13–20]
Support vector machine	High classification accuracy and generalization ability in small-sample cases	Large-scale training data is computationally intensive and sensitive to missing data	[24–29]
Bayesian classifier	Strong mathematical theoretical foundation and robustness	Reduced performance when sample attributes do not satisfy independent and identically distributed assumptions	[33–36]
Logistic regression	Simple and efficient, with low computational complexity and a low storage footprint	Prone to underfitting	[40–43]
Clustering model	No label information is required; the algorithm is easy to implement	Slow convergence of large datasets; sensitive to noise and isolated points	[47–52]
Artificial neural network	High accuracy and easy parallel processing	Large training sample requirement and limited interpretability	[60–69]
Hybrid model	Strong robustness and leverages the benefits of multiple models	Difficult training process; difficulties with convergence; requires more data.	[74–84, 86–88]
Reinforcement learning	Modeling of sequential decision problems and consideration of long-term rewards	Reward function design is difficult; convergence is unstable; risks state overload; requires more data and computational resources	[94–95]
Evolutionary algorithm	Robustness and parallelism	Too many control variables; slow convergence	[100–103]
Agent-based	Simulation of complex phenomena is possible	Many parameters need to be preset; high computational requirements; difficulty in validating results	[110–115]

## 4. 基于关系的税务风险检测方法

上述非基于关系的风险检测方法从纳税人个人出发, 往往需要根据税务专家的经验进行手工选择、设计和构建不同的特征。然后使用这些特征以及不同的训练模式来训练一个非关系性风险检测模型, 并最终应用于税务风险检测。值得注意的是, 非基于关系的风险检测方法可能会导致大量交互信息的丢失。然而, 税务场景可以自然地构建为一个复杂的网络, 其中包含一系列的实体对象, 如税务企业、法人、商品和税收法律法规。不同实体之间也存在着各种类型的关系, 如税务企业之间的交易关系、税务企业与法人之间的投资持有关系、企业商品买卖关系等。逃税行为往往表现出“类似帮派”的特征, 如通过关联交易逃税。识别这类风险行为需要更多地考虑关系的重要性, 并从具有更丰富语义信息的网络中挖掘逃税线索。

### 4.1. 图模式匹配

图模式匹配[118–119]是研究图的重要研究途径之一, 因此在数据挖掘和数据库等领域引起了广泛的研究关注。在税务场景中, 研究人员通常使用图模式匹配算法来挖掘整个税务交易网络中的逃税群体。

Tian 等[120]提出了一个基于彩色网络的模型来表征纳税人之间的经济行为、社会关系和利益相关交易，并据此生成一个纳税人的利益交互网络。通过构建模式树和匹配组件模式，可以发现利益交互网络中的可疑群体。Wei 等[121]提出了一种新的基于图的联锁可疑群体逃税检测方法 GSG2I，该方法包括一种图投影算法，设计用于识别满足控制器联锁模式的关系和基于组件的模式匹配。该算法基于控制器的联锁来查找可疑的逃税群体。对中国某省份 7 年税务数据进行的实验测试结果表明，GSG2I 方法可以大大提高检测效率。

Liu [122]设计了一种虚假的增值税发票行为检测系统，并提出了一种基于深度优先的有向图循环搜索算法，该算法可以检测基金交易流图中的基金循环，并可以查询循环相关账户的细节，以节省审计成本。Ruan 等[123]提出了一种基于税率差异检测、拓扑模式匹配和税务异常检测的混合方法来识别基于关联交易的逃税行为。

循环交易是由逃税者通过在没有任何增值且没有任何实际货物供应的团伙间开具销售发票来实施的，有助于实施多种金融犯罪。Mathews 等[124]为印度泰伦加纳州政府的商业税收部门开发了一种循环贸易模型，涉及三家经销商。该模型可以预测两个经销商之间是否会形成未来的联系，从而产生一个准确率为 80% 的三重环。

Rocha-Salazar 等[125]提出了一种利用法人属性和动态社交网络来检测金融系统中的空壳公司的创新方法。该模型在平衡精度、真阳性率和假阳性率等方面均优于传统的规则方法。该技术已在一家墨西哥金融公司成功实施，并可被其他金融机构用于识别空壳公司和减少避税和洗钱行为。本研究的局限性包括没有定期拥有已确认的空壳公司，也没有考虑与其他金融机构的客户建立联系。未来的研究应侧重于对可疑的内部联系以及内部法人与外部法人之间的联系进行建模。

Chen 和 Tsourakakis [126]提出了一种新的 AntiBenford 子图框架，用于金融网络中的无监督异常检测。该框架基于统计原理，可以有效地在近线性时间内找到异常子图。该框架在真实数据和合成数据上进行了评估，与最先进的基于图的异常检测方法相比，它表现出了优越的性能。所提出的 AntiBenford 子图显示非法交易的特征，并可以为金融交易数据提供新的见解。最后，本文提出了未来的研究方向，包括设计重叠异常子图的算法以及在实验设置中引入其他统计偏差的度量。

图模式匹配的结果易于理解，经常采用可视化分析的方法对模式匹配的结果进行进一步的分析。但当数据规模较大时，子图匹配问题计算量太大。此外，匹配的图模式

往往需要手动定义，并且在税务审计博弈过程中存在主观性和滞后性，可能导致许多重要的图模式被忽视。

#### 4.2. 图表示学习

图模式匹配方法严重依赖税务专家的经验来总结和提取逃税模式；当新的模式出现时，需要通过硬编码记录。同时，纳税企业的基本特征也没有得到充分的考虑。为了解决这一问题，研究者已经开始使用图表示学习[130–131]来研究逃税检测问题。

Matos 等[132]引入了一种新的基于复杂网络技术的特征选择算法，该方法可以捕获关键的欺诈指标。还提出了一种基于上述算法的精确税务欺诈检测分类器。在巴西财政部获得的真实数据集上验证了该算法的有效性。

Wu 等[133]提出了一种基于融合交易网络表征的逃税检测框架 (TED-TNR)。该方法将交易网络的拓扑信息和纳税人的基本属性联合嵌入到一个低维向量空间中，然后利用纳税人的低维向量进行逃税检测。结果表明，TED-TNR 方法比现有方法能更准确地检测逃税者。

Mi 等[134]提出了一种基于具有网络嵌入特征的 PU 学习的逃税检测方法。首先，利用网络嵌入技术提取交易网络特征。其次，在 PU 学习过程中，根据类先验和排序排名为每个样本分配个体权重。最后，在最小化经验风险的基础上训练一个加权样本分类器。

An 等[135]提出了一种基于上游和下游网络嵌入的税务风险识别方法。该方法设计了优化函数，分别捕获局部和全局静态和动态网络结构。对一个省级税收数据集的实证结果证实了该模型的有效性。

Wang 等[136]提出了时间边缘增强图注意网络方法。在该方法中，使用边缘增强的图注意网络来学习复杂的拓扑，从而捕获空间依赖性，而使用循环加权平均单位来学习交易数据的动态，以捕获时间依赖性。对税务数据的实验测试表明，该方法在检测逃税者方面优于现有方法。

Gao 等[137]提出了一个多阶段的逃税检测框架 FBNE-PU。该框架通过从交易网络中提取有效特征，利用少量的正样本和大量的未标记样本，显著提高了逃税检测性能。Shi 等[138]提出了一种新的图神经网络模型 Eagle，用于使用异构图模型进行逃税检测。基于设计的元路径的指导，Eagle 可以通过分层次注意机制，将纳税人的特征及其关系充分聚合，从而提取更全面的特征。在真实世界的税务数据集上进行的大量实验表明，Eagle 在分类和异常检测场景下都优于最先进的逃税检测方法。

图表示学习利用了大量的结构信息和关系信息，往往

能获得更好的风险检测性能。但当图的规模增加时，会出现可解释性差和计算复杂度增加的问题，迫切需要解决[139]。

#### 4.3. 视觉分析

视觉分析是基于交互式视觉界面的可视化表示，它可以帮助研究人员理解和进一步实施分析和推理方法[140–142]。在税务风险审计领域，大多数现有的数据挖掘方法都缺乏可解释性，因此难以提供逃税的直接证据。仅凭算法的分类结果，税务稽查员很难理解和追踪发现的来源。可视化分析方法构建了一个复杂的实体网络，如纳税人及其交易和利益。由于分析结果易于理解，可视化分析已成为税务审计中不可或缺的技术。

Didimo 等[143]设计了一个名为 VISFAN 的金融活动网络可视化分析系统，将社交网络分析和金融交易网络的聚类分析相结合，目的是检测洗钱和欺诈等金融犯罪。Tselykh 等[144]使用聚类和规则归纳技术来识别属性图中潜在的欺诈性转移定价风险行为。他们使用网络分析和可视化方法来筛选出在转让定价审计中需要特别注意的实体。

意大利税务局开发了 TaxNet，这是一个基于视觉分析的逃税检测决策支持系统[145]。该系统允许用户直观地定义和提取纳税人网络中的可疑模式。该系统目前在托斯卡纳地区的税务局使用，并已证明其在实际工作环境中的有效性。Zheng 等[146]设计了 ATTENet，这是一个可视化分析系统，用于检测和解释可疑的基于交易的逃税群体。通过网络嵌入方法 Structure2Vec [147]和随机森林算法对逃税群体的可疑值进行检测，然后对检测结果进行了可视化解释。

Yu 等[148]设计了 TaxVis，这是一个针对税务稽查员的可视化检测系统。该系统采用两阶段的方法进行逃税群组检测。在第一阶段，采用网络嵌入方法 node2vec [149]从企业关联网络中学习嵌入企业的表示，并使用 LightGBM 计算每个公司的可疑分数。在第二阶段，系统采用桑基图等可视化方法，对可疑公司的上下游异常交易进行分析。

Didimo 等[150]提出了一种名为 MALDIVE 的新方法，通过图模式匹配、社会网络分析和机器学习来检测纳税人之间的税收风险行为。使用信息扩散策略来扩大可能存在风险的纳税人的范围，使用网络可视化系统将结果输出给税务稽查员。

Zha [151]利用分层卷积网络，在构建的税务审计网络中计算纳税人的风险得分。设计了可视化分析系统 TaxAA，允许税务稽查员定制可疑指标，并最终以“车轮”图的形式观察纳税人之间的可疑关系。Lin 等[152]提出了一个名为 TaxThemis 的交互式可视化分析系统，通过分析异质税务数据，帮助税务官员挖掘和探索涉嫌逃税的群组。提出了一种新的编码方案，以在日历热图中可视化通过关联方交易进行的收入转移的证据。

视觉分析具有视觉表现能力，易于理解，具有可解释性高的优点。但是，视觉信息往往是由数据科学家根据自己的经验设计的；因此，所呈现的数据往往是主观的和有偏见的[153–155]，这可能导致重要的线索被忽视，做出不正确的风险检测判断。

#### 4.4. 总结

前面几节讨论了现有的基于关系的税务风险检测技术。每种税务风险检测方法都有其独特的优缺点。分析了每种技术的优缺点，并在表4中列出了相关文献[120–126, 132–138, 143–146, 148, 150–152]。这些发现能够帮助税务数据科学家选择合适的税务风险检测技术。

### 5. 开放的问题和未来的研究方向

税收是一个国家的基础。由于税收的重要性，税务风险检测一直是一个重要的研究课题。近年来，国内外的相关工作取得了很大的进展，出现了许多优秀的税务风险检测方法。然而，现有的方法仍然是数据驱动的并受某些限制的影响，包括知识的碎片化（使知识的集成和利用变得复杂）、税务风险检测结果难以解释、税务风险检测算法计算昂贵以及算法依赖税务专家手动提供的标签信息。仅依靠数据驱动的方法很难解决上述理论和技术问

表4 基于关系的风险检测方法总结

Method	Advantage	Weakness	References
Graph pattern matching	Results are easy to understand	Computationally intensive; relies on manually designed tax evasion group patterns	[120–126]
Graph representation learning	High accuracy and strong generalization ability	Poorly interpretable and computationally intensive when graph scale increases	[132–138]
Visual analysis	Easy to understand and highly interpretable	Subjective and biased	[143–146, 148, 150–152]

题。利用知识导向和数据驱动的大数据知识工程[156–158]将成为税务风险检测领域未来的发展趋势，是从信息化到智能化的唯一路径。本节将特别讨论上述现有工作中的四个局限性，并展望未来基于大数据知识工程的税务风险检测方法。

### 5.1. 研究方向1：基于大数据知识工程的碎片化知识融合

现有的税务风险检测方法往往从纳税人提供的登记和发票信息开始，构建风险检测的特征。然而，现实税务环境中的知识是多来源、多领域、多模式的；此外，一些数据仍未得到充分利用，如国家税务总局和税务部门发布的文件、相关法律、法规、政策、第三方信息（如与纳税人有关的现有案例描述和公共安全信息）。因此，探索如何在税务场景中通过碎片化知识融合将多源异构和碎片化数据转换为机器可表示和可计算的结构化知识库是一项挑战，但未来必须进行必要的工作。碎片化知识融合还满足多重知识表示框架[159]，通过聚合来自多个来源的信息，增强了模型的鲁棒性和可解释性，从而实现了更智能的应用，如应税税务计算[160]等。

针对上述问题，有必要从以下两个方面开展工作：①在财政和税务领域的半结构化和非结构化数据（如税收政策和法规）中，需要研究知识提取、实体提取、关系提取和属性事件提取，以将这些数据转换为结构化知识；②在知识融合的背景下，需要研究共引用消除歧义和实体链接。同时，消除多源异构数据中域间差异大和数据分布多变等问题，将是实现碎片化知识融合的关键。

### 5.2. 研究方向2：基于大数据知识工程的可解释性认知推理

现有的税务风险检测方法大多是所谓的黑箱模型，可解释性较差；这种模型只能知道“如何”，而不知道“为什么”，因此不能直接提供相关证据用于揭露逃税企业。基于视觉分析的方法可以通过机器学习算法挖掘和探索涉嫌逃税的个人或群体，并使用易于理解的可视化界面来帮助税务官员选择合适的案例。虽然这种方法显著提高了可解释性，但它仍然使用了黑箱模型。此外，受数据科学家的解释的影响，视觉分析显示的数据很可能是有偏见和主观的，这将导致重要的线索被忽视。未来该领域的研究重点为如何在利用碎片化知识融合获得的税收知识库中进行高级认知推理，使用认知推理生成可解释的和完整的证据链，并帮助税务稽查员追踪疑点来源。

为了解决上述问题，推荐以下研究方向：①探索基于变压器的方法的可解释认知推理，因为基于变压器的模型

具有更强的表达能力，而基于自我注意的机制在呈现实体之间的风险关系方面具有更好的可解释性，使得这个方向极具吸引力和意义；②使用不同的范式（如转换学习、归纳学习和演绎推理）来扩展和发展现有知识；③将象征主义和连接主义的互补信息相结合，利用现有知识指导数据推理，生成与逃税和欺诈相关的证据链，从而协助税务稽查员追踪数据来源。

### 5.3. 研究方向3：大规模税务情景下的风险检测方法

现有的税务风险检测技术倾向于关注风险检测的准确性，并经常通过使用集成学习和构建更大、更复杂的模型来提高这种准确性。然而，中国每年有数亿纳税人开具数百亿张发票。此外，税务场景还需与第三方数据（如工商、海关、公安等）相结合。在现实世界的税务场景中，有必要处理非常大规模的数据，这可能会导致许多无法直接使用的复杂风险检测模型的失败。设计一种通用的逃税和欺诈检测方法，可以在不失去有效性和稳定性的情况下实现分钟级甚至毫秒级的响应速度，这仍然是一个具有挑战性的命题。

为了解决上述问题，必须在以下两个方面开展工作：①继续研究分布式机器学习和使用技术方法（如计算并行模式、数据并行模式和模型并行模式），以充分利用现有的大数据和大模型；②构建轻量级网络。通过知识蒸馏、剪枝和其他模型压缩技术，可以使模型轻量化和定制化，从而便于设计更快的风险检测算法。

### 5.4. 研究方向4：低资源情景下的风险检测方法

目前，深度学习在许多领域的成功是由于大规模标记数据集的支持。大多数现有的模型也采用了有监督的或半有监督的学习范式。然而，很难获得在税务场景下的标记数据。即使不考虑与税务数据相关的隐私和安全问题，也不可能通过众包和其他方法给公司贴上税务风险行为的标签，因为这将需要丰富的与税务相关的专业知识和经验。因此，构建包含大量标签信息的税务数据集是非常昂贵的。针对低资源场景设计一种认知推理风险检测方法存在以下挑战：①首先，在低资源场景中可用的标记数据有限，使得模型的训练和性能评估变得困难；②其次，在税务情况下，只有极少数的企业被标记为有高风险，而大量的企业则处于未标记状态；③第三，初创企业的交易信息很少，很难准确评估新企业的风险。

鉴于上述问题，在未来的工作中需要关注以下四个方面：①使用主动学习，主动选择最有价值的样本进行标记，从而以最小的开销最大化模型效益；②使用无监督学

习方法（如比较学习、生成模型和聚类方法）为低资源税务场景设计模型；③对PU学习等半监督方法进行研究，以充分利用未标记样本；④研究元学习、数据增强和迁移学习等技术，以更准确地评估新企业的风险。

## 6. 结论

为加快人工智能在税务风险检测领域的高质量发展，更好地协助国家税务机关进行税务风险检测和决策，本研究首次对国内外税务风险检测的研究进展进行了全面回顾，并总结了每种方法的优缺点。分析了当前税务风险检测方法的局限性，总结了四个研究问题——分散的财税知识难以整合和利用、风险检测结果难以解释、风险检测算法的高成本以及现有算法对标签信息的依赖，并描绘了税务风险检测从信息化到智能化的未来发展方向。

## 致谢

本研究由陕西省重点研发项目(2023GXLH-024)和国家自然科学基金项目(62250009、62002282、62037001、62192781)资助。

## Compliance with ethics guidelines

Qinghua Zheng, Yiming Xu, Huixiang Liu, Bin Shi, Jiayang Wang, and Bo Dong declare that they have no conflict of interest or financial conflicts to disclose.

## References

- [1] Wang D, Huang Y, Cai Z. The State Council Information Office held a press conference on tax and fee reduction to boost confidence in the development [Internet]. Beijing: The State Council Information Office of the People's Republic of China; 2022 Jan 26 [cited 2022 Nov 1]. Available from: <http://www.scio.gov.cn/xwfbh/xwfbh/wqfbh/47673/47802/index.htm>. Chinese.
- [2] The tax gap-tax gap estimates for tax years 2014-2016 [Internet]. Washington, DC: Internal Revenue Service; 2022 Oct 28 [cited 2022 Nov 1]. Available from: <https://www.irs.gov/newsroom/the-tax-gap>.
- [3] Andronicăanu A, Gherghina R, Ciobănașu M. The interdependence between fiscal public policies and tax evasion. *Adm Si Manag Public* 2019;32:32-41.
- [4] López JJ. A quantitative theory of tax evasion. *J Macroecon* 2017;53:107-26.
- [5] Allingham MG, Sandmo A. Income tax evasion: a theoretical analysis. *J Public Econ* 1972;1(3-4):323-38.
- [6] Zhao Q, Bhowmick SS. Association rule mining: a survey. Report. Singapore: Nanyang Technological University; 2003.
- [7] Hipp J, Güntzer U, Nakhaeizadeh G. Algorithms for association rule mining—a general survey and comparison. *SIGKDD Explor* 2000;2(1):58-64.
- [8] Wu RS, Ou CS, Lin H, Chang SI, Yen DC. Using data mining technique to enhance tax evasion detection performance. *Expert Syst Appl* 2012;39(10):8769-77.
- [9] Matos T, de Macedo JAF, Monteiro JM. An empirical method for discovering tax fraudsters: a real case study of Brazilian fiscal evasion. In: *Proceedings of the 19th International Database Engineering & Applications Symposium*; 2015 Jul 13-15; Yokohama, Japan. New York City: Association for Computing Machinery (ACM); 2015. p. 41-8.
- [10] Zhao Z, Jian Z, Gaba GS, Alrooba R, Masud M, Rubaiee S. An improved association rule mining algorithm for large data. *J Intell Syst* 2021;30(1):750-62.
- [11] Safavian SR, Landgrebe D. A survey of decision tree classifier methodology. *IEEE Trans Syst Man Cybern* 1991;21(3):660-74.
- [12] Clark LA, Pregibon D. Tree-based models. In: Hastie TJ, editor. *Statistical models in S*. New York City: Taylor & Francis Group; 2017.
- [13] Bonchi F, Giannotti F, Mainetto G, Pedreschi D. Using data mining techniques in fiscal fraud detection. In: *Proceedings of the 1st International Conference on Data Warehousing and Knowledge Discovery*; 1999 Aug 30-Sep 1; Florence, Italy. Berlin: Springer; 1999. p. 369-76.
- [14] Mittal S, Reich O, Mahajan A. Who is bogus? Using one-sided labels to identify fraudulent firms from tax returns. In: *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*; 2018 Jun 20-22; Menlo Park and San Jose, CA, USA. New York City: Association for Computing Machinery (ACM); 2018. p. 1-11.
- [15] Yao J, Zhang J, Wang L. A financial statement fraud detection model based on hybrid data mining methods. In: *Proceedings of the 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*; 2018 May 26-28; Chengdu, China. New York City: IEEE; 2018. p. 57-61.
- [16] Wu C, Luo J. Automatic recognition of tax evasion behavior based on random forest. *Software Guide* 2018;017(008):13-6.
- [17] An B, Suh Y. Identifying financial statement fraud with decision rules obtained from modified random forest. *Data Technol Appl* 2020;54(2):235-55.
- [18] Ji YL, Wang WQ. The stock of research on accurate identification of tax risk under the background of big data technology—based on machine learning. *Public Finance Res* 2020;451(09):121-31. Chinese.
- [19] Andrade JPA, Paulucio LS, Paixao TM, Paixao TM, Berriel RF, Carneiro TCJ, et al. A machine learning-based system for financial fraud detection. In: *Proceedings of the 18th National Meeting on Artificial and Computational Intelligence (ENIAC 2021)*; 2021 Nov 29-Dec 3; online. São Leopoldo: Sociedade Brasileira de Computação (SBC); 2021. p. 165-76.
- [20] Xavier OC, Pires SR, Marques TC, Soares AS. Tax evasion identification using open data and artificial intelligence. *Rev Adm Pública* 2022;56(3):426-40.
- [21] Agarwala, TanYS, RonenO, SinghC, YuB. Hierarchical Shrinkage: improving the accuracy and interpretability of tree-based models. In: *Proceedings of the 39th International Conference on Machine Learning*; 2022 Jul 17-23; Baltimore, MD, USA. New York City: ML Research Press; 2022. p. 111-35.
- [22] Noble WS. What is a support vector machine? *Nat Biotechnol* 2006;24(12):1565-7.
- [23] Pisner DA, Schnyer DM. Support vector machine. In: Mechelli A, Vieira S, editors. *Machine learning*. Cambridge: Academic Press; 2020. p. 101-21.
- [24] Wang S, Li A. Fraud detection in tax declaration based on SVM. *Comput Eng* 2006;.
- [25] Liu H, Yu X, Wan W, Ma X. A tax assessment model based on rough set theory and SVM algorithms. *Comput Simu* 2009;26(12):253-6. Chinese.
- [26] Xia H, Li R. Cases-choice in tax declaration model based on SVM and SOM. *Sci Technol Eng* 2009;009(014):4027-31. Chinese.
- [27] Junqué de Fortuny E, Stankova M, Moeyersoms J, Minnaert B, Provost FJ, Martens D. Corporate residence fraud detection. In: *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*; 2014 Aug 24-27; New York City, NY, USA. New York City: Association for Computing Machinery (ACM); 2014. p. 1650-9.
- [28] Rad MS, Shahbahrani A. Detecting high risk taxpayers using data mining techniques. In: *Proceedings of the 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS 2016)*; 2016 Dec 14-15; Tehran, Iran. New York City: IEEE; 2016. p. 1-5.
- [29] Zhang X. Early warning and investigation countermeasures of crime of issuing false invoice [dissertation]. Beijing: People's Public Security University of China; 2020. Chinese.
- [30] Cervantes J, Garcia-Lamont F, Rodriguez L, López A, Castilla JR, Trueba A. PSO-based method for SVM classification on skewed data sets. *Neurocomputing* 2017;228:187-97.
- [31] Rish I. An empirical study of the Naive Bayes classifier. In: *Proceedings of the IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence*; 2001 Aug 4-6; Washington, DC, USA. Berlin: Springer; 2001. p. 41-6.

- [32] Leung KM. Naive Bayesian classifier. Hong Kong: Polytechnic University Department of Computer Science/Finance and Risk Engineering; 2007.
- [33] Kirkos E, Spathis C, Manolopoulos Y. Data mining techniques for the detection of fraudulent financial statements. *Expert Syst Appl* 2007;32(4):995–1003.
- [34] Kang Z, Yu Y. Study on tax evaluation model based Bayesian classification. *Econ Probl* 2009;6:124–6. Chinese.
- [35] Zhang K, Wu D, Li A, Song BW. Fraud detection in tax declaration based on Bayesian classifier. *Comput Simu* 2010;27(009):306–10. Chinese.
- [36] Lenz HJ. Tax fraud and investigation procedures-everybody, every where, every time. In: *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*; 2016 Feb 19–21; Rome, Italy. Trier: The DBLP Computer Science Bibliography; 2016. p. 3–13.
- [37] Zaidi NA, Cerquides J, Carman MJ, Webb GI. Alleviating Naive Bayes attribute independence assumption by attribute weighting. *J Mach Learn Res* 2013;14(60):1947–88.
- [38] Kleinbaum DG, Klein M. Logistic regression: a self-learning text. 2nd ed. New York City: Springer-Verlag; 2002.
- [39] Hosmer Jr DW, Lemeshow S, Sturdivant RX. Applied logistic regression. Hoboken: John Wiley & Sons; 2013.
- [40] Qi X. The research on the tax inspection methods about identifying tax evasion [dissertation]. Changchun: Jilin University; 2010. Chinese.
- [41] Wang Y, Li Q, Qi X. Research on the tax inspection selection scheme model based on the logistic regression. *Econ Res Guide* 2012;35(2):96–7. Chinese.
- [42] Su Y. Research on tax inspection case selection based on logistic regression model [dissertation]. Guangzhou: Sun Yat-sen University; 2011. Chinese.
- [43] Yuan Y. Research on the model of tax inspection and case selection in H city based on logistic regression to identify enterprise tax evasion [dissertation]. Hohhot: Inner Mongolia University; 2019. Chinese.
- [44] Lever J, Krzywinski M, Altman N. Points of significance: model selection and overfitting. *Nat Methods* 2016;13(9):703–5.
- [45] Fraides I, Matthiesen R. Overview on techniques in cluster analysis. In: Matthiesen R, editor. *Bioinformatics methods in clinical research*. Totowa: Humana Press; 2010.
- [46] Duran BS, Odell PL. Cluster analysis: a survey. Berlin: Springer Science & Business Media; 2013.
- [47] Denny, Williams GJ, Christen P. Exploratory multilevel hot spot analysis: Australian taxation office case study. In: *Proceedings of the 6th Australasian Conference on Data Mining and Analytics-Volume 70*; 2007 Dec 3–4; Queensland, QLD, Australia. New York City: Association for Computing Machinery (ACM); 2007. p. 77–84.
- [48] Liu X, Pan D, Chen S. Application of hierarchical clustering in tax inspection case-selecting. In: *Proceedings of the 2010 International Conference on Computational Intelligence and Software Engineering*; 2010 Dec 10–12; Wuhan, China. New York City: IEEE; 2010. p. 1–4.
- [49] Liu B, Xu G, Xu Q, Zhang N. Outlier detection data mining of tax based on cluster. *Phys Procedia* 2012;33:1689–94.
- [50] Assylbekov Z, Melnykov I, Bekishev R, Baltabayeva A, Bissengaliyeva D, Mamlin E. Detecting value-added tax evasion by business entities of Kazakhstan. In: CzarnowskiI, CaballeroA, HowlettR, JainL, editors. *Proceedings of the International Conference on Intelligent Decision Technologies*; 2016 Jun 15–17; Puerto de la Cruz, Spain. Berlin: Springer, Cham; 2016. p. 37–49.
- [51] De Roux D, Perez B, Moreno A, del Pilar VM, Figueroa C. Tax fraud detection for under-reporting declarations using an unsupervised machine learning approach. In: *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*; 2018 Aug 19–23; London, UK. New York City: Association for Computing Machinery (ACM); 2018. p. 215–22.
- [52] Xia H, Cheng P, Zhang L. Tax risk identification based on improved K-means clustering algorithm under big data. *Fin Accou Mon* 2019;21:143–6. Chinese.
- [53] Ben-David S, Haghtalab N. Clustering in the presence of background noise. In: *Proceedings of the International Conference on Machine Learning*; 2014 Jun 21–26; Beijing, China. New York City: ML Research Press; 2014. p. 280–8.
- [54] Guo X, Li S. Distributed k-clustering for data with heavy noise. In: *Proceedings of the 32nd International Conference on Neural Information Processing Systems*; 2018 Dec 3–8; Montréal, QC, Canada. New York City: Association for Computing Machinery (ACM); 2018. p. 7849–57.
- [55] Bishop CM. Neural networks and their applications. *Rev Sci Instrum* 1994; 65(6):1803–32.
- [56] Khan S, Rahmani H, Shah SAA, Bennamoun M. A guide to convolutional neural networks for computer vision. Berlin: Springer; 2018.
- [57] Sinkov A, Asyaev G, Mursalimov A, Nikolskaya K. Neural networks in data mining. In: *Proceedings of the 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*; 2016 May 19–20; Chelyabinsk, Russia. New York City: IEEE; 2016. p. 1–5.
- [58] Zhang J, Zong C. Deep neural networks in machine translation: an overview. *IEEE Intell Syst* 2015;30(5):16–25.
- [59] Abiodun OI, Jantan A, Omolara AE, Dada KV, Mohamed NA, Arshad H. State-of-the-art in artificial neural network applications: a survey. *Heliyon* 2018; 4(11):e00938.
- [60] Li S, Xiao X. Application of tax payment evaluation based on fuzzy neural network. *Comput Simu* 2012;29(01):352–5. Chinese.
- [61] Lin CC, Chiu AA, Huang SY, Yen DC. Detecting the financial statement fraud: the analysis of the differences between data mining techniques and experts’ judgments. *Knowl Base Syst* 2015;89:459–70.
- [62] Ioana-Florina C, Mare C. The utility of neural model in predicting tax avoidance behavior. In: Czarnowski I, Howlett RJ, Jain LC, editors. *Intelligent decision technologies: proceedings of the 13th KES-IDT 2021 conference*. Singapore: Springer; 2021. p. 71–81.
- [63] Pérez López C, Delgado Rodríguez MJ, de Lucas Santos S. Tax fraud detection through neural networks: an application using a sample of personal income taxpayers. *Future Internet* 2019;11(4):86.
- [64] Zhang L, Nan X, Huang E, Liu S. Detecting transaction-based tax evasion activities on social media platforms using multi-modal deep neural networks. 2020. arXiv:2007.13525.
- [65] Chen H, Gong L, Cheng L, You Z. Tax risk assessment model of large enterprises based on multilayer perceptron. *Appl Res Comput* 2020;37(S2):41–3+6. Chinese.
- [66] Zhang L, Nan X, Huang E, Liu S. Social e-commerce tax evasion detection using multi-modal deep neural networks. In: *Proceedings of the 2021 Digital Image Computing: Techniques and Applications (DICTA)*; 2021 Nov 29–Dec 1; Gold Coast, QLD, Australia. New York City: IEEE; 2021. p. 1–6.
- [67] Murorunkwere BF, Tuyishimire O, Haughton D, Nzabanita J. Fraud detection using neural networks: a case study of income tax. *Future Internet* 2022; 14(6):168.
- [68] Mojahedi H, Babazadeh Sangar A, Masdari M. Towards tax evasion detection using improved particle swarm optimization algorithm. *Math Probl Eng* 2022; 2022:1027518.
- [69] Alsadhan NA. Value-added tax fraud detection and anomaly feature selection using sectorial autoencoders. In: *Proceedings of the Data Analytics and Management (ICDAM 2022)*; 2022 Jun 25–26; Jelenia Góra, Poland. Singapore: Springer; 2022. p. 323–31.
- [70] Fan FL, Xiong J, Li M, Wang G. On interpretability of artificial neural networks: a survey. *IEEE Trans Radiat Plasma Med Sci* 2021;5(6):741–60.
- [71] Kar K, Kornblith S, Fedorenko E. Interpretability of artificial neural network models in artificial intelligence versus neuroscience. *Nat Mach Intell* 2022; 4(12):1–3.
- [72] Buda M, Maki A, Mazurowski MA. A systematic study of the class imbalance problem in convolutional neural networks. *Neural Netw* 2018;106:249–59.
- [73] Trentin E, Gori M. A survey of hybrid ANN/HMM models for automatic speech recognition. *Neurocomputing* 2001;37(1–4):91–126.
- [74] Ravisankar P, Ravi V, Rao GR, Bose I. Detection of financial statement fraud and feature selection using data mining techniques. *Decis Support Syst* 2011; 50(2):491–500.
- [75] Zheng M. Research on tax data mining based on SAS system [dissertation]. Zhengzhou: Zhengzhou University; 2012. Chinese.
- [76] González PC, Velásquez JD. Characterization and detection of taxpayers with false invoices using data mining techniques. *Expert Syst Appl* 2013; 40(5): 1427–36.
- [77] Song XP, Hu ZH, Du JG, Sheng ZH. Application of machine learning methods to risk assessment of financial statement fraud: evidence from China. *J Forecast* 2014;33(8):611–26.
- [78] Rahimikia E, Mohammadi S, Rahmani T, Ghazanfari M. Detecting corporate tax evasion using a hybrid intelligent system: a case study of Iran. *Int J Account Inf Syst* 2017;25:1–17.
- [79] Wu Y, Zheng Q, Gao Y, Dong B, Wei R, Zhang F, et al. TEDM-PU: a tax evasion detection method based on positive and unlabeled learning. In: *Proceedings of the 2019 IEEE International Conference on Big Data (Big Data)*; 2019 Dec 9–12; AngelesLos, CA, USA. New York City: IEEE; 2019. p. 1681–6.
- [80] Javadian KA, Poor ASAA, Hosseini SM. A model for identification tax fraud based on improved ID3 decision tree algorithm and multilayer perceptron neural network. *Manag Account* 2020;13(46):53–70.
- [81] Rahman RA, Masrom S, Omar N, Zakaria M. An application of machine learning on corporate tax avoidance detection model. *IAES Int J Artif Intell*

- 2020;9(4):721.
- [82] Mekonnen E. Data mining for detection of tax evasion: the case of tax payers in Addis Ababa [dissertation]. London: St. Mary's University; 2021.
- [83] Savić M, Atanasijević J, Jakovetić D, Krejić N. Tax evasion risk management using a hybrid unsupervised outlier detection method. *Expert Syst Appl* 2022; 193:116409.
- [84] Baghdasaryan V, Davtyan H, Sarikyan A, Navasardyan Z. Improving tax audit efficiency using machine learning: the role of taxpayer's network data in fraud detection. *Appl Artif Intell* 2022;36(1):2012002.
- [85] Schunck R. Within and between estimates in random-effects models: advantages and drawbacks of correlated random effects and hybrid models. *Stata J* 2013; 13(1):65–76.
- [86] Zhu X, Yan Z, Ruan J, Zheng Q, Dong B. IRTEd-TL: an inter-region tax evasion detection method based on transfer learning. In: Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE); 2018 Aug 1–3; New York City, NY, USA. New York City: IEEE; 2018. p. 1224–35.
- [87] Wei R, Dong B, Zheng Q, Zhu X, Ruan J, He H. Unsupervised conditional adversarial networks for tax evasion detection. In: Proceedings of the 2019 IEEE International Conference on Big Data (Big Data); 2019 Dec 9–12; AngelesLos, CA, USA. New York City: IEEE; 2019. p. 1675–80.
- [88] Zhang F, Shi B, Dong B, Zheng Q, Ji X. TTED-PU: a transferable tax evasion detection method based on positive and unlabeled learning. In: Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC); 2020 Jul 13–17; Madrid, Spain. New York City: IEEE; 2020. p. 207–16.
- [89] Wang J, Chen Y. Safe and robust transfer learning. Singapore: Springer; 2022.
- [90] Nam J, Pan SJ, Kim S. Transfer defect learning. In: Proceedings of the 2013 35th International Conference on Software Engineering (ICSE); 2013 May 18–26; FranciscoSan, CA, USA. New York City: IEEE; 2013. p. 382–91.
- [91] Li Y. Deep reinforcement learning: an overview. 2017. arXiv:1701.07274.
- [92] Sutton RS, Barto AG. Reinforcement learning: an introduction. Cambridge: MIT Press; 2018.
- [93] François-Lavet V, Henderson P, Islam R, Bellemare MG, Pineau J. An introduction to deep reinforcement learning. *Found Trends Mach Learn* 2018; 11:219–354.
- [94] Abe N, Melville P, Pendus C, Reddy C, Jensen D, Thomas V. Optimizing debt collections using constrained reinforcement learning. In: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; 2010 Jul 25–28; Washington, DC, USA. New York City: Association for Computing Machinery (ACM); 2010. p. 75–84.
- [95] Goumagias ND, Hristu-Varsakelis D, Assael YM. Using deep Q-learning to understand the tax evasion behavior of risk-averse firms. *Expert Syst Appl* 2018;101:258–70.
- [96] Bonnet C, Caron P, Barrett T, Davies I, Laterre A. One step at a time: pros and cons of multi-step meta-gradient reinforcement learning. 2021. arXiv: 2111.00206.
- [97] Jitani A, Mahajan A, Zhu Z, Abou-Zeid H, Fapi ET, Purnehdi H. Structure-aware reinforcement learning for node-overload protection in mobile edge computing. *IEEE Trans Cogn Commun Netw* 2022;8(4):1881–97.
- [98] Bäck T, Schwefel HP. An overview of evolutionary algorithms for parameter optimization. *Evol Comput* 1993;1(1):1–23.
- [99] Bartz-Beielstein T, Branke J, Mehnen J, Mersmann O. Evolutionary algorithms. *Wiley Interdiscip Rev Data Min Knowl Discov* 2014;4(3):178–95.
- [100] Alden ME, Bryan DM, Lessley BJ, Tripathy A. Detection of financial statement fraud using evolutionary algorithms. *J Emerg Technol Account* 2012; 9(1): 71–94.
- [101] Warner G, Wijesinghe S, Marques U, Badar O, Rosen J, Hemberg E, et al. Modeling tax evasion with genetic algorithms. *Econ Gov* 2015;16(2):165–78.
- [102] Hemberg E, Rosen J, Warner G, Wijesinghe S, O'Reilly UM. Tax noncompliance detection using co-evolution of tax evasion risk and audit likelihood. In: Proceedings of the 15th International Conference on Artificial Intelligence and Law; 2015 Jun 8–12; DiegoSan, CA, USA. New York City: Association for Computing Machinery (ACM); 2015. p. 79–88.
- [103] Hemberg E, Rosen J, Warner G, Wijesinghe S, O'Reilly UM. Detecting tax evasion: a co-evolutionary approach. *Artif Intell Law* 2016;24(2):149–82.
- [104] Karafotias G, Hoogendoorn M, Eiben ÁE. Parameter control in evolutionary algorithms: trends and challenges. *IEEE Trans Evol Comput* 2014; 19(2): 167–87.
- [105] Lobo FG, Lima C, Michalewicz Z. Parameter setting in evolutionary algorithms. Berlin: Springer Science & Business Media; 2007.
- [106] Sipper M, Fu W, Ahuja K, Moore JH. Investigating the parameter space of evolutionary algorithms. *BioData Min* 2018;11(1):2.
- [107] Gilbert N, Terna P. How to build and use agent-based models in social science. *Mind Soc* 2000;1:57–72.
- [108] Samanidou E, Zschischang E, Stauffer D, Lux T. Agent-based models of financial markets. *Rep Prog Phys* 2007;70(3):409–50.
- [109] Gilbert N. Agent-based models. Newbury Park: SAGE Publications; 2019.
- [110] Antunes L, Balsa J, Coelho H. Agents that collude to evade taxes. In: Proceedings of the 6th International Joint Conference on Autonomous Agents and Multiagent Systems; 2007 May 14–18; Honolulu, HI, USA. New York City: Association for Computing Machinery (ACM); 2007. p. 1–3.
- [111] Lima FWS. Tax evasion and nonequilibrium model on apollonian networks. *Int J Mod Phys C* 2012;23(11):1250079.
- [112] Llacer T, Miguel FJ, Noguera JA, Tapia E. An agent-based model of tax compliance: an application to the Spanish case. *Adv Complex Syst* 2013; 16(04n05):1350007.
- [113] Noguera JA, Quesada FJM, Tapia E, Llàcer T. Tax compliance, rational choice, and social influence: an agent-based model. *Rev Fr Sociol* 2014;55(4):765–804.
- [114] Andrei AL, Comer K, Koehler M. An agent-based model of network effects on tax compliance and evasion. *J Econ Psychol* 2014;40:119–33.
- [115] Bloomquist KM. A comparison of agent-based models of income tax evasion. *Soc Sci Comput Rev* 2006;24(4):411–25.
- [116] Manzo G, Matthews T. Potentialities and limitations of agent-based simulations. *Rev Fr Sociol* 2014;55(4):653–88.
- [117] McDonald GW, Osgood ND. Agent-based modeling and its tradeoffs: an introduction & examples. 2023. arXiv:2304.08497.
- [118] Fan W. Graph pattern matching revised for social network analysis. In: Proceedings of the 15th International Conference on Database Theory; 2012 Mar 26–29; Berlin, Germany. New York City: Association for Computing Machinery (ACM); 2012. p. 8–21.
- [119] Ma S, Cao Y, Fan W, Huai JP, Wo T. Strong simulation: capturing topology in graph pattern matching. *ACM Trans Database Syst* 2014;39(1):1–46.
- [120] Tian F, Lan T, Chao KM, Godwin N, Zheng Q, Shah N, et al. Mining suspicious tax evasion groups in big data. *IEEE Trans Knowl Data Eng* 2016; 28(10):2651–64.
- [121] Wei W, Yan Z, Ruan J, Zheng Q, Dong B. Mining suspicious tax evasion groups in a corporate governance network. In: Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing; 2017 Aug 21–23; Helsinki, Finland. Berlin: Springer; 2017. p. 465–75.
- [122] Liu L. Methods of detect falsely making out specialized invoices behavior based on directed graph [dissertation]. Xi'an: Xi'an University of Science and Technology; 2017. Chinese.
- [123] Ruan J, Yan Z, Dong B, Zheng Q, Qian B. Identifying suspicious groups of affiliated-transaction-based tax evasion in big data. *Inf Sci* 2019;477:508–32.
- [124] Mathews J, Mehta P, Babu S. Link prediction techniques to handle tax evasion. In: Proceedings of the 3rd ACM India Joint International Conference on Data Science & Management of Data (8th ACM IKDD CODS & 26th COMAD); 2021 Jan 2–4; online. New York City: Association for Computing Machinery (ACM); 2021. p. 307–15.
- [125] Rocha-Salazar JJ, Segovia-Vargas MJ, Camacho-Miñano MM. Detection of shell companies in financial institutions using dynamic social network. *Expert Syst Appl* 2022;207:117981.
- [126] Chen T, Tsourakakis C. Antibenford subgraphs: unsupervised anomaly detection in financial networks. In: Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining; 2022 Aug 14–18; Washington, DC, USA. New York City: Association for Computing Machinery (ACM); 2022. p. 2762–70.
- [127] Fan W, Li J, Ma S, Tang N, Wu Y, Wu Y. Graph pattern matching: from intractable to polynomial time. *Proc VLDB Endowment* 2010;3(1–2):264–75.
- [128] Ma S, Cao Y, Huai J, Wu T. Distributed graph pattern matching. In: Proceedings of the 21st International Conference on World Wide Web Conference; 2012 Apr 16–20; Lyon, France. New York City: Association for Computing Machinery (ACM); 2012. p. 949–58.
- [129] Bouhenni S, Yahiaoui S, Nouali-Taboudjemat N, Kheddouci H. A survey on distributed graph pattern matching in massive graphs. *ACM Comput Surv* 2021; 54(2):1–35.
- [130] Chen F, Wang YC, Wang B, Kuo CCJ. Graph representation learning: a survey. *APSIPA Trans Signal Inf Process* 2020;9(1):e15.
- [131] Khoshraftar S, An A. A survey on graph representation learning methods. 2022. arXiv:2204.01855.
- [132] Matos T, de Macêdo JAF, Monteiro JM, Lettich F. An accurate tax fraud classifier with feature selection based on complex network node centrality

- measure. In: Proceedings of the 19th International Conference on Enterprise Information Systems; 2017 Apr 26–29; Porto, Portugal. Berlin: Springer; 2017. p. 145–51.
- [133] Wu Y, Dong B, Zheng Q, Wei R, Wang Z, Li X. A novel tax evasion detection framework via fused transaction network representation. In: Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC); 2020 Jul 13–17; Madrid, Spain. New York City: IEEE; 2020. p. 235–44.
- [134] Mi L, Dong B, Shi B, Zheng Q. A tax evasion detection method based on positive and unlabeled learning with network embedding features. In: Proceedings of the International Conference on Neural Information Processing; 2020 Nov 18–22; Bangkok, Thailand. Berlin: Springer; 2020. p. 140–51.
- [135] An J, Zheng Q, Wei R, Dong B, Li X. NEUD-TRI: network embedding based on upstream and downstream for transaction risk identification. In: Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC); 2020 Jul 13–17; Madrid, Spain. New York City: IEEE; 2020. p. 277–86.
- [136] Wang Y, Zheng Q, Ruan J, Gao Y, Chen Y, Li X, et al. T-EGAT: a temporal edge enhanced graph attention network for tax evasion detection. In: Proceedings of the 2020 IEEE International Conference on Big Data (Big Data); 2020 Dec 10–13; Atlanta, GA, USA. New York City: IEEE; 2020. p. 1410–5.
- [137] Gao Y, Shi B, Dong B, Wang Y, Mi L, Zheng Q. Tax evasion detection with FBNE-PU algorithm based on PnCGCN and PU learning. *IEEE Trans Knowl Data Eng* 2021;35(1):931–44.
- [138] Shi B, Dong B, Xu Y, Wang J, Wang Y, Zheng Q. An edge feature aware heterogeneous graph neural network model to support tax evasion detection. *Expert Syst Appl* 2023;213:118903.
- [139] Gogoglou A, Bruss CB, Hines KE. On the interpretability and evaluation of graph representation learning. 2019. arXiv:1910.03081.
- [140] Leite RA, Gschwandtner T, Miksch S, Gstrein E, Kuntner J. Visual analytics for event detection: focusing on fraud. *Vis Inform* 2018;2(4):198–212.
- [141] Yuan J, Chen C, Yang W, Liu M, Xia J, Liu S. A survey of visual analytics techniques for machine learning. *Comput Vis Media* 2021;7(1):3–36.
- [142] Liu D, Alnegheimish S, Zytok A, Veeramachaneni K. MTV: visual analytics for detecting, investigating, and annotating anomalies in multivariate time series. *Proc ACM Hum Comput Interact* 2022;6(CSCW1):103.
- [143] Didimo W, Liotta G, Montecchiani F, Palladino P. An advanced network visualization system for financial crime detection. In: Proceedings of the 2011 IEEE Pacific Visualization Symposium; 2011 Mar 1–4; Hong Kong, China. New York City: IEEE; 2011. p. 203–10.
- [144] Tselykh A, Knyazeva M, Popkova E, Durfee A, Tselykh A. An attributed graph mining approach to detect transfer pricing fraud. In: Proceedings of the 9th International Conference on Security of Information and Networks; 2016 Jul 20–22; Newark, NJ, USA. New York City: Association for Computing Machinery (ACM); 2016. p. 72–5.
- [145] Didimo W, Giamminonni L, Liotta G, Montecchiani F, Pagliuca D. A visual analytics system to support tax evasion discovery. *Decis Support Syst* 2018;110:71–83.
- [146] Zheng Q, Lin Y, He H, Ruan J, Dong B. ATTENet: detecting and explaining suspicious tax evasion groups. In: Proceedings of the 28th International Joint Conference on Artificial Intelligence; 2019 Aug 10–16; Macao, China. Washington, DC: AAAI Press; 2019. p. 6584–6.
- [147] Dai H, Dai B, Song L. Discriminative embeddings of latent variable models for structured data. In: Proceedings of the International Conference on Machine Learning; 2016 Jun 19–24; New York City, NY, USA. New York City: Association for Computing Machinery (ACM); 2016. p. 2702–11.
- [148] Yu H, He H, Zheng Q, Dong B. TaxVis: a visual system for detecting tax evasion group. In: Proceedings of the World Wide Web Conference; 2019 May 13–17; FranciscoSan, CA, USA. New York City: Association for Computing Machinery (ACM); 2019. p. 3610–4.
- [149] Grover A, Leskovec J. Node2vec: scalable feature learning for networks. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; 2016 Aug 6–11; FranciscoSan, CA, USA. New York City: Association for Computing Machinery (ACM); 2016. p. 855–64.
- [150] Didimo W, Grilli L, Liotta G, Menconi L, Montecchiani F, Pagliuca D. Combining network visualization and data mining for tax risk assessment. *IEEE Access* 2020;8:16073–86.
- [151] Zha Z. TaxAA: a reliable tax auditor assistant for exploring suspicious transactions. In: Proceedings of the Web Conference 2020; 2020 Apr 20–24; Taipei, China. New York City: Association for Computing Machinery (ACM); 2020. p. 240–4.
- [152] Lin Y, Wong K, Wang Y, Zhang R, Dong B, Qu H, et al. TaxThemis: interactive mining and exploration of suspicious tax evasion groups. *IEEE Trans Vis Comput Graph* 2021;27(2):849–59.
- [153] Nussbaumer A, Verbert K, Hillemann EC, Bedek MA, Albert D. A framework for cognitive bias detection and feedback in a visual analytics environment. In: Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC 2016); 2016 Aug 16–19; Uppsala, Sweden. New York City: IEEE; 2016. p. 148–51.
- [154] Wall E, Blaha LM, Franklin L, WarningEnder A., bias may occur: a proposed approach to detecting cognitive bias in interactive visual analytics. In: Proceedings of the 2017 IEEE Conference on Visual Analytics Science and Technology (VAST 2017); 2017 Oct 3–6; Phoenix, AZ, USA. New York City: IEEE; 2017. p. 104–15.
- [155] Wall E. Detecting and mitigating human bias in visual analytics [dissertation]. Atlanta: Georgia Institute of Technology; 2020.
- [156] Zheng Q. 2019 big data knowledge engineering and application. *J Comput Res Dev* 2019;56(12):2519–20.
- [157] Wu F, Han Y, Li X, Zheng QH. Chen XL Reasoning in artificial intelligence: advances and challenges. *Bull Natl Nat Sci Found Chin* 2018; 32(3):262–5. Chinese.
- [158] Zhuang Y, Wu F, Chen C, Pan Y. Challenges and opportunities: from big data to knowledge in AI 2.0. *Front Inf Technol Electron Eng* 2017;18(1):3–14.
- [159] Yang Y, Zhuang Y, Pan Y. Multiple knowledge representation for big data artificial intelligence: framework, applications, and case studies. *Front Inf Technol Electron Eng* 2021;22(12):1551–8.
- [160] Zheng Q, Liu J, Zeng H, Guo Z, Wu B, Wei B. Knowledge forest: a novel model to organize knowledge fragments. *Sci China Inf Sci* 2021;64(7):179103.